IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand Oktober 2023

GRS - 757

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand Okober 2023

Robert Arians
Laura Kleinert
Christian Korn
Claudia Quester
Oliver Rest
Alexander Schug

Februar 2024

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4721R01610 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUV übereinstimmen.

GRS - 757
ISBN 978-3-910548-48-0

Deskriptoren

Advanced Persistent Threats, Critical Infrastructures, ICS, industrielle Steuerungssysteme, IT-Angriffe, IT-Angriffswerkzeuge, IT-Bedrohungslage, IT-Sicherheitsvorfälle, kerntechnische Anlagen, Schadsoftware kritische Infrastrukturen, Nuclear Facilities, Schadsoftware

Kurzfassung

Die IT-Bedrohungslage in Bezug auf kritische Infrastrukturen und industrielle Steuerungssysteme wird von der GRS kontinuierlich verfolgt, ausgewertet und in einem jährlichen Bericht dargestellt. Hierbei werden insbesondere Cyberangriffe mit Bezug zu kerntechnischen Anlagen und Anlagen im Umgang mit radioaktiven Stoffen sowie Cyberangriffe auf den Energiesektor in den Fokus genommen. Für das Jahr 2023 wurden darüber hinaus sieben weitere Themenschwerpunkte identifiziert, die in den vergangenen Monaten die IT-Bedrohungslage signifikant geprägt haben. Hierzu zählen neben Cyberangriffen in Zusammenhang mit dem Krieg in der Ukraine und weiteren geopolitischen Spannungsfeldern auch schadsoftwarefreie Cyberangriffe, Social Engineering, Ransomware-Angriffe und Supply-Chain-Angriffe. Zusätzlich werden Schwachstellen in industriellen Steuerungssystemen als Angriffsvektor für Cyberangriffe betrachtet. Der Bericht beschäftigt sich zudem mit den Aktivitäten von relevanten Advanced Persistent Threats. In den Anhängen befinden sich Informationen zu relevanten Schwachstellen, Angriffswerkzeugen, IT-Sicherheitsvorfällen und Cyberangriffen. Da es sich dabei um von Bericht zu Bericht weitergeführte und ergänzte Anhänge handelt, umfassen sie im Gegensatz zum Hauptteil des Berichtes einen deutlich längeren Betrachtungszeitraum als nur das Jahr 2023.

Abstract

GRS continuously screens and analyses the cyber threat landscape, focusing on industrial control systems and critical infrastructures. Special attention is paid to cyberattacks targeting the nuclear or energy sector. Additionally, this summary report for 2023 comprises seven main topics including cyber attacks connected to the war in Ukraine and geopolitically motivated cyberattacks in other parts of the world. Other main topics cover software free cyberattacks, social engineering, ransomware attacks and supply chain attacks. Emphasis is also placed on ICS vulnerabilities as attack vector. Moreover, this report includes an overview concerning relevant advanced persistent threat activities. The appendices summarize relevant vulnerabilities, cyber-attack tools, incidents and cyberattacks. As living appendices, they cover a much longer period than 2023 alone.

Inhaltsverzeichnis

1 Einleitung

Für kerntechnische Anlagen und Einrichtungen ist der Schutz gegen Störmaßnahmen und sonstige Einwirkungen Dritter essenziell, unabhängig davon ob potenzielle Angriffe als physische Angriffe, Cyberangriffe oder kombinierte Angriffe ausgeführt werden. Bei der Auswahl und Auslegung von Sicherungsmaßnahmen zur Sicherstellung des erforderlichen Schutzes sind sowohl die aktuelle Bedrohungslage als auch die tatsächliche Angriffsoberfläche zu berücksichtigen.

Die Angriffsoberfläche ist dabei die Summe aller potenziellen Angriffsvektoren. Sie beschreibt daher, wo überall ein Angreifer ansetzen könnte, um z. B. in das interne Netzwerk einzudringen, Manipulationen vorzunehmen, Auswirkungen hervorzurufen oder Inhalte zu exfiltrieren.

Die Angriffsoberfläche wird durch verschiedene Faktoren beeinflusst. Dazu zählen beispielsweise:

- Grad der Digitalisierung in allen Bereichen.
- Einsatz programmierbarer und rechnerbasierter industrieller Steuerungssysteme sowie anderer IT-Systeme.
- Einsatz von Remote-Verbindungen für z. B. Bedienung, Wartung, Inspektion.
- Ausgliederung sensibler Dienstleistungen.
- Beteiligte Lieferketten.
- Softwarebedingte Alterungseffekte.

Die Angriffsoberfläche ist individuell für eine konkrete Anlage oder Einrichtung. Dennoch lassen sich für die letzten Monate und Jahre generelle Entwicklungen ausmachen, die auch kerntechnische Anlagen und Einrichtungen in Deutschland betreffen. So wurden und werden viele ursprünglich festverdrahtet ausgeführte leittechnische Einrichtungen, Systeme und Komponenten in kerntechnischen Anlagen durch programmierbare oder rechnerbasierte Einrichtungen ersetzt. Darüber hinaus ist auch im Entwicklungs- und Herstellungsprozess sowie bei der Wartung dieser industriellen Steuerungssysteme ein immer stärkerer Einsatz von rechnerbasierten und programmierbaren Werkzeugen festzustellen. Gleichzeitig ist auch im Bereich aller weiteren IT-Systeme eine fortschreitende Digitalisierung und die stetige Erweiterung von Funktionalitäten zu verzeichnen.

Auch wächst die Zahl der IT-Systeme, die prinzipiell von außen erreichbar sind, konstant an. Spätestens seit den Jahren der COVID-19-Pandemie kommt zusätzlich eine Erweiterung der Möglichkeiten für Remote-Zugriffe hinzu. Dies umfasst auch Möglichkeiten für Remote-Bedienung, -Wartung und -Instandhaltung. Ein weiterer Trend ist die zunehmende Auslagerung sensibler Informationen und Dienstleistungen, beispielsweise zu Software-as-a-Service-Anbietern, Cloud-Anbietern oder Security Operation Centres. Darüber hinaus spielen softwarebedingte Alterungseffekte eine immer größere Rolle. Hierzu zählen beispielsweise die Unverfügbarkeit von erwünschten Updates und Patches für Legacy Systeme, Kompatibilitätsverluste oder vom Kunden nicht beeinflussbare Wartungslücken von Legacy Systemen. Hinzu kommt, dass sich die Gestalt der Angriffsoberfläche durch die immense Supply-Chain-Abhängigkeit und die immer stärkere Verzweigung der beteiligten Lieferketten von IT-Systemen, IT-Dienstleistungen und relevanter Hardware signifikant verändert. Klare Abgrenzungen werden immer stärker durch diffuse, häufig nicht vollständig erfassbare Bereiche ersetzt. All diese Veränderungen führen zu einer Vergrößerung der Angriffsoberfläche und damit zu immer neuen Möglichkeiten und Potenzialen im Bereich der Einflussnahme durch Dritte.

Die aktuelle IT-Bedrohungslage spiegelt wider, wozu potenzielle Angreifer derzeit in der Lage sind und was sie antreibt. Zentrale Punkte sind dabei die Fähigkeiten, Kenntnisse und Ressourcen potenzieller Angreifer sowie ihre Motivation. Im Gegensatz zur Angriffsoberfläche kann die IT-Bedrohungslage daher nicht direkt, sondern nur indirekt ermittelt werden. Relevante Aspekte beinhalten unter anderem:

- beobachtete Cyberangriffe und IT-Sicherheitsvorfälle.
- Bekanntwerden von Schadsoftwarekomponenten.
- Bekanntwerden oder sogar Ausnutzung neu erkannter oder bisher nicht geschlossener Schwachstellen in industriellen Steuerungssystemen bzw. in für kritische Infrastrukturen relevanten IT-Systemen.
- Eingesetzte Angriffstechniken.
- Verfügbarkeit von Angriffswerkzeugen und entsprechenden Dienstleistungen.
- Aktivitäten von Angreifergruppierungen.

Sekundäre Aspekte betreffen die Rückschlüsse, die sich hieraus ergeben, vor allem in Bezug auf:

- Motivation der Angreifer.
- Zweck der Angriffe.
- Fähigkeiten, Kenntnisse und Ressourcen der Angreifer.
- Kreis der potenziellen Angreifer.

Die IT-Bedrohungslage entwickelt sich sehr dynamisch. Es werden zunehmen Cyberangriffe beobachtet, wobei industrielle Steuerungssysteme immer stärker in den Fokus der Angreifer rücken. Die Bandbreite bei den eingesetzten Schadsoftwarekomponenten reicht von einfachen, aber bei erfolgreichem Einsatz häufig dennoch sehr effektiven Schadsoftwarekomponenten bis hin zu ausgefeilten Schadsoftwarekomponenten für mehrstufige, komplexe Cyberangriffe. Hierbei ist allerdings zu bemerken, dass ausgefeilte Schadsoftwarekomponenten bei ihrem Einsatz häufig unentdeckt bleiben, weil die Angreifer auf persistenten, langfristigen Zugriff auf Systeme und Informationen großen Wert legen und daher erheblichen Aufwand im Bereich Detektionsevasion betreiben. Dies stellt einen erheblichen Unterschied zu Angriffen beispielsweise mit Ransomware dar, bei denen eine zeitnahe Entdeckung des Angriffs von den Angreifern nicht nur einkalkuliert wird, sondern erwünscht ist. Die bei den beobachteten Cyberangriffen beobachteten Angriffstechniken sind sehr vielfältig. In den vergangenen Monaten ist ein Trend hin zu schwer detektierbaren Angriffstechniken sowie zu schadsoftwarefreien Angriffen festzustellen. In diesem Zusammenhang sind vor allem Living-off-the-Land-Techniken und Social Engineering zu nennen. Schwachstellen in industriellen Steuerungssystemen werden ebenfalls zunehmend beobachtet, was auch auf den deutlich erhöhten Aufwand zurückzuführen ist, mit dem von verschiedensten Seiten nach solchen Schwachstellen gesucht wird. Relevant ist hier vor allem, dass ein deutlicher Anteil der bekanntwerdenden Schwachstellen einen als hoch oder kritisch eingestuften Schweregrad besitzen und weder die Bereitstellung noch das Einspielen von entsprechenden Patches oder Updates als gesichert betrachtet werden kann. Daher prägen solche Schwachstellen häufig auch langfristig Teile der Angriffsoberfläche.

Bei den hier beobachteten Angreifergruppierungen wurden vielfältige Aktivitäten und häufig eine breite Streuung bei den Angriffszielen festgestellt. Insgesamt ist von einem breiter werdenden Feld an Angreifern auszugehen, da viele der beobachteten Angreifergruppierungen bereits seit Jahren aktiv sind und immer wieder neue Angreifergruppierungen hinzukommen. Eine bereits im vergangenen Jahr deutlich gewordene Entwicklung betrifft APT-for-hire, wobei etablierte, befähigte Angreifer ihre Fähigkeiten und Kenntnisse gegen Bezahlung zur Verfügung stellen.

Hinzu kommt, dass auch viele Angriffswerkzeuge nicht mehr nur ihren Entwicklern, sondern einem deutlich größeren Angreiferkreis zur Verfügung stehen, der häufig selbst nicht in der Lage gewesen wäre, diese Werkzeuge in Anbetracht ihrer stetig zunehmenden Komplexität zu entwickeln.

Bei den in den vergangenen Monaten beobachteten Angriffen und Angreiferaktivitäten wird deutlich, dass nach wie vor viele Angriffe aus finanzieller Motivation durchgeführt werden. Eine deutliche Zunahme ist hingegen bei Angriffen aus politischen oder ideologischen Motiven festzustellen. In Bezug auf die Motivation von Angreifern ist es wichtig, ihre Volatilität zu berücksichtigen. Während der Aufbau von Fähigkeiten, Kenntnissen und Ressourcen einige Zeit in Anspruch nimmt, kann sich die Motivation potenzieller Angreifer in beliebig kurzer Zeit ändern. Wie interessant ein potenzielles Angriffsziel für eine Angreifergruppierung ist, hängt neben ihrer Motivation auch stark davon ab, was sie mit dem Angriff bezweckt. In Bezug auf den Zweck der durchgeführten Cyberangriffe hat sich bei den beobachteten Angreiferaktivitäten eine Verschiebung von rein disruptiven hin zu destruktiven Angriffen ergeben. Auffällig ist auch die Zunahme von Cyberangriffen, die offenbar zu Aufklärungs- und Spionagezwecken sowie mit dem Ziel der Informationsbeschaffung durchgeführt wurden. Auch werden mit Cyberangriffen zunehmend strategische Interessen verfolgt. Insgesamt ist von einer Zunahme an Fähigkeiten, Kenntnissen und Ressourcen auf Angreiferseite bei gleichzeitig wachsendem Kreis an potenziellen Angreifern auszugehen.

Angesichts der sich dynamisch verändernden IT-Bedrohungslage werden international die bestehenden Regelwerke und Richtlinien zur IT-Sicherheit (insbesondere von IAEA, IEC und ISO) und damit die Anforderungen an Sicherungsmaßnahmen ständig weiterentwickelt und erweitert. Auch nationale Vorgaben zur IT-Sicherheit in Deutschland (BSI-Grundschutz, IT-SIG) und anderen Ländern (z. B. in GB, SF, USA) wurden in den letzten Jahren überarbeitet oder befinden sich wie das deutsche SEWD-Regelwerk IT aktuell in Überarbeitung.

Für die IT-Sicherheit kommt damit der regelmäßigen Analyse der Bedrohungslage, aber auch der Bewertung des Standes von Wissenschaft, Technik und Erkenntnis zur Prävention, Detektion sowie zur Reaktion auf Cyberangriffe, eine besondere Bedeutung zu. Die GRS verfolgt daher die Entwicklung der IT-Bedrohungslage für industrielle Steuerungssysteme und kritische Infrastrukturen, relevante IT-Sicherheitsvorfälle, Cyberangriffe, Schwachstellen, Angriffswerkzeuge, Schadsoftwarekomponenten sowie APTs kontinuierlich.

Aufbauend auf diesem kontinuierlichen Screening der IT-Bedrohungslage, werden die wichtigsten Vorkommnisse in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen ausgewählt und vor dem Hintergrund der IT-Bedrohungslage ausgewertet. Eine kurze Beschreibung der betrachteten Vorkommnisse findet sich im Anhang dieses Berichtes.

Typischerweise werden die Auswertungen der relevanten Vorkommnisse bereits kurz nach Bekanntwerden der zugrunde liegenden Vorfälle oder Angriffe erstellt, um möglichst zeitnah ihre Relevanz für die IT-Sicherheit deutscher kerntechnischer Anlagen abzuschätzen, d. h. die erste Auswertung erfolgt häufig zu einem Zeitpunkt, an dem die forensischen Analysen der IT-Sicherheitsvorfälle oder sogar die entsprechenden Angriffswellen selbst, noch andauern. Die forensische Analyse eines IT-Sicherheitsvorfalls kann sich hierbei ebenso hinziehen, wie die Untersuchung der von den Angreifern eingesetzten Schadsoftwarekomponenten und Angriffswerkzeuge. Gleiches gilt bei Schwachstellen in industriellen Steuerungssystemen und weiteren relevanten IT-Systemen, und zwar sowohl für deren Ausnutzung und das Bekanntwerden entsprechender Exploits als auch für Patches und Updates zum Schließen oder Mitigieren der Schwachstellen. Dabei bedeutet die Entdeckung eines Cyberangriffs häufig nicht dessen Ende, sondern bietet den Angreifern lediglich Anlass, zunächst auf einzelne Angriffswege und Angriffswerkzeuge zu verzichten und diese im weiteren Verlauf anzupassen. So können sich – auch Jahre nach dem ersten Bekanntwerden – noch relevante, zusätzliche Aspekte ergeben, aufgrund derer Ersteinschätzungen immer wieder ergänzt, angepasst oder vollständig überarbeitet werden müssen. Um dieser Dynamik gerecht zu werden, handelt es sich bei den im vorliegenden Bericht wiedergegebenen Beschreibungen (siehe Anhang) daher nicht um abschließende Bewertungen der jeweiligen Vorkommnisse, sondern um eine Momentaufnahme. Aufgrund dieser sich unter Umständen auch noch Jahre nach dem ersten Bekanntwerden ändernden Informationslage zu IT-Sicherheitsvorfällen, Angriffen und Schwachstellen müssen auch bisherige Auswertungen immer wieder auf ihre Aktualität geprüft und ggf. angepasst werden.

Für Ereignisse mit besonderer Relevanz für kerntechnische Anlagen und Einrichtungen, werden bei Bedarf noch vertiefte Auswertungen durchgeführt und detailliertere Einschätzungen abgegeben. Je nach Dringlichkeit oder Bedeutung kann es sich dabei um kurzfristige Ersteinschätzungen oder bzw. und um ausführliche Stellungnahmen handeln.

Zusätzlich zu den jeweils aktuell bekannt gewordenen IT-Sicherheitsvorfällen, Cyberangriffskampagnen und Schwachstellen in industriellen Steuerungssystemen, werden

Stück für Stück auch frühere, herausragende Vorfälle, Angriffe und Schwachstellen ausgewertet, um ein möglichst vollständiges Bild der relevanten IT-Bedrohungslage zu erhalten. Neben bekanntwerdenden IT-Sicherheitsvorfällen, Schwachstellen in industriellen Steuerungssystemen und Cyberangriffswerkzeugen, werden auch Informationen zu den in diesem Zusammenhang aktuell relevantesten APT-Gruppierungen und deren Aktivitäten kontinuierlich verfolgt und zusammengetragen.

2 IT-Bedrohungslage

Die IT-Bedrohungslage für kritische Infrastrukturen und insbesondere kerntechnische Anlagen und Einrichtungen und ihre dynamische Entwicklung werden von der GRS fortlaufend verfolgt, erfasst und ausgewertet. Als Grundlage zieht die GRS hierbei insbesondere Informationen zu folgenden Aspekten heran:

- Schwachstellen in industriellen Steuerungssystemen und in für kritische Infrastrukturen relevanten IT-Systemen (siehe Kapitel A im Anhang),
- Angriffswerkzeuge, die unabhängig von Cyberangriffen bekannt werden (siehe Kapitel A im Anhang)
- IT-Sicherheitsvorfälle und Cyberangriffe einschließlich der dabei eingesetzten Angriffswerkzeuge und Schadsoftwarekomponenten (siehe Kapitel B im Anhang) sowie
- APT-Gruppierungen (Advanced Persistent Threat – fortgeschrittene andauernde Bedrohung) und ihre Aktivitäten (siehe Abschnitt 2.10).

Basierend auf den Erkenntnissen zu diesen Aspekten wurden für den vorliegenden Bericht elf für die aktuelle IT-Bedrohungslage relevante Themenschwerpunkte ausgewählt:

- **Ransomware** – Ransomware-Angriffe nehmen einen erheblichen Teil der beobachteten Cyberangriffe insgesamt ein. Gleichzeitig kommt es auch immer häufiger zu Schein-Ransomware-Angriffen, die nur vorgeblich auf Erpressung ausgerichtet sind, in der Realität aber auf die Zerstörung von Daten setzen. Auch setzen die Angreifer hierbei immer stärkere Druckmittel wie beispielsweise die Androhung der Veröffentlichung von im Rahmen des Angriffs ausgeschleusten Daten ein.
- **Social Engineering** – Social Engineering ist mit Abstand der häufigste erste Angriffsschritt bei Cyberangriffen. Die dabei eingesetzten Techniken werden immer ausgefeilter, so dass sie häufig auch für sensibilisierte und trainierte Personen schwer zu erkennen sind. Social Engineering zielt darauf ab, Personen mit für sie interessanten Informationen oder Kenntnissen so zu manipulieren, dass sie als unwissentliche Innentäter im Rahmen des Angriffs agieren.
- **Schadsoftwarefreie Cyberangriffe und Living-off-the-Land** – Bei schadsoftwarefreien Cyberangriffen handelt es sich um Cyberangriffe, die ohne den Einsatz von Schadsoftwarekomponenten erfolgen. Neben vielen Social Engineering Techniken spielt hier vermehrt Living-off-the-Land eine Rolle, wobei die Angreifer bereits auf

den angegriffenen IT-Systemen vorhandene Programme oder Dienste für ihre eigenen Zwecke missbrauchen.

- **Cyberangriffe über die Lieferkette** – Supply-Chain-Angriffen kommt eine immer größere Bedeutung zu. Vor allem bei gut geschützten Angriffszielen wählen Angreifer diesen zwar aufwändiger erscheinenden, aber gleichzeitig komfortableren Weg, um Sicherheitsmaßnahmen und Barrieren zu umgehen. Dabei wird das eigentliche Angriffsziel nicht direkt angegriffen, sondern zunächst ein Zwischenziel in der Lieferkette kompromittiert.

- **Schwachstellen in industriellen Steuerungssystemen als Angriffsvektor** – Industrielle Steuerungssysteme haben häufig einen sehr langen Lebenszyklus, insbesondere was die Zeitspanne von ihrer ersten Inbetriebnahme bis zu ihrer Entsorgung anbelangt. Viele der aktuell eingesetzten industriellen Steuerungssysteme wurden zu einer Zeit entwickelt, in der das Thema Cybersicherheit für industrielle Steuerungssysteme noch nicht die heutige Bedeutung hatte. Daher ist die Betrachtung von Schwachstellen solcher Systeme als Angriffsvektor von besonderer Bedeutung.

- **IT-Sicherheitsvorfälle im Energiesektor** – Die Energieversorgung ist in vielerlei Hinsicht die Achillesferse der modernen Gesellschaft. Eine Unterbrechung der Energieversorgung ist mit Rückwirkungen auf eine Vielzahl von Anlagen und Tätigkeiten verbunden. Daher kommt IT-Sicherheitsvorfällen im Energiesektor generell, aber auch mit besonderem Blick auf kerntechnische Anlagen und Einrichtungen, eine besondere Bedeutung zu.

- **IT-Sicherheitsvorfälle mit Bezug zu kerntechnischen Anlagen und Anlagen im Umgang mit radioaktiven Stoffen** – Auch kerntechnische Anlagen und Anlagen im Umgang mit radioaktiven Stoffen sind immer wieder direkt oder indirekt von Cyberangriffen betroffen. Ihnen kommt im Kontext dieses Berichts sowie hinsichtlich der potenziellen Auswirkungen eines erfolgreichen Angriffs eine besondere Bedeutung zu.

- **Cyberangriffe in Zusammenhang mit dem Krieg in der Ukraine** – Bereits vor dem Hintergrund der wachsenden Spannungen und noch einmal seit Kriegsausbruch ist es zu einem starken Anstieg der politisch und strategisch motivierten Cyberangriffe nicht nur in der Ukraine, sondern auch darüber hinausgekommen.

  Dabei stehen im diesjährigen Bericht insbesondere Cyberangriffe auf NATO-Staaten im Vordergrund.

- **Cyberangriffe in Zusammenhang mit weiteren politischen Spannungsfeldern –** Cyberangriffe kommen heute in praktisch allen politischen Spannungsfeldern zum Einsatz. Beispielhaft werden hier die Konflikte zwischen Iran und Israel, zwischen China und Japan sowie zwischen Nordkorea und Südkorea beleuchtet.

Diese Themenschwerpunkte werden in den folgenden Abschnitten 2.1 bis 2.9 vorgestellt. Die Aktivitäten von insgesamt 15, im Kontext dieses Berichts relevanten APT-Gruppierungen werden in Abschnitt 2.10 näher beschrieben.

2.1 Ransomware

Bei Ransomware handelt es sich um Schadsoftwarekomponenten, welche von Angreifern zu Zwecken der Lösegelderpressung eingesetzt werden. Die Ransomware verschlüsselt die Dateien des Opfers. Anschließend stellen die Angreifer eine Lösegeldforderung mit dem Versprechen, dass sie bei Zahlung des Lösegeldes ein Software-Werkzeug zur Verfügung stellen, mit dessen Hilfe das Opfer seine Dateien wieder entschlüsseln kann. Darüber hinaus setzen die Angreifer häufig weitere Schadsoftwarekomponenten zur Spionage und zum Datendiebstahl ein, um Daten zu exfiltrieren, bevor deren Verschlüsselung durch die Ransomware im System des Opfers erfolgt. In diesem Fall versehen sie ihre Lösegeldforderung mit der Drohung, gestohlene, sensible Daten zu veröffentlichen, sollte das Lösegeld nicht gezahlt werden. Dabei handelt es sich also um eine doppelte Erpressungsstrategie. Die Motivation der Angreifer ist hierbei eindeutig finanzieller Natur: Zahlung des Lösegeldes. Ist diese erfolgt, kommt es häufig vor, dass entgegen der ursprünglichen Angaben im Anschluss keine Entschlüsselung der Daten stattfindet. Oftmals verfügen die Angreifer gar nicht über die Software-Werkzeuge, um die Verschlüsselung wieder rückgängig zu machen. Eine Entschlüsselung der Daten nach Zahlung des Lösegeldes liegt in vielen Fällen von vornherein nicht in der Absicht der Angreifer. Auch IT-Dienstleistern und -Sicherheitsunternehmen gelingt dies nur, wenn sie an Informationen gelangen, auf welche Weise die Datenverschlüsselung durchgeführt wurde. Ransomware-Angriffe sind daher äußerst destruktiv und enden nicht selten mit der unwiderruflichen Zerstörung der schadhaft verschlüsselten Daten des Opfers.

Mittlerweile müssen Cyberkriminelle nicht mehr über Programmierkenntnisse verfügen, um Ransomware-Angriffe durchzuführen. APT-Gruppierungen (siehe Abschnitt 2.10) wie z. B. REvil oder auch BlackMatter bieten Ransomware-as-a-Service

(RaaS)-Lösungen an. Das bedeutet, dass sie eine für den jeweils beabsichtigten Angriff maßgeschneiderte Ransomware anderen Cyberkriminellen zum Kauf anbieten oder diese gegen eine Gewinnbeteiligung bei der Lösegelderpressung zur Verfügung stellen. Häufig streicht die APT-Gruppierung, welche die RaaS-Lösung bereitstellt, den Hauptteil des Lösegeldes ein. Da es sich bei den Lösegeldforderungen je nach Opfer, Art und Umfang des Angriffes um Beträge im fünf- bis achtstelligen US-Dollar-Bereich handelt, ist die Inanspruchnahme dieser Dienste für Cyberkriminelle dennoch äußerst lukrativ.

Nicht zuletzt aufgrund der erzielbaren hohen Lösegeldbeträge und der Möglichkeit, RaaS-Dienste in Anspruch nehmen zu können, nimmt die Zahl der Ransomware-Angriffe stetig zu. Laut /SEC23w03/ waren die Mehrheit der Cyberangriffe im Jahr 2022 finanziell motivierte Ransomware-Angriffe mit einem Anteil von 74 %.

In den letzten Monaten haben vor allem folgende Gruppierungen durch Ransomware-Angriffe auf sich aufmerksam gemacht:

- Bei REvil handelt es sich um eine vermutlich aus Russland heraus agierende APT-Gruppierung (siehe Abschnitt 2.10.10), welche weltweit Ransomware und RaaS sehr profitabel einsetzt und seit 2019 aktiv ist. Die von der Gruppierung bislang eingesetzte Schadsoftware fragt die Spracheinstellungen des infizierten Systems ab und wird bei Benutzern mit russischer Spracheinstellung nicht aktiv. Nach Verschlüsselung der Daten des angegriffenen Unternehmens durch die Schadsoftware wird von der Gruppierung eine entsprechende Lösegeldforderung gestellt mit der Drohung, während des Angriffs erbeutete, sensible Informationen bei Nichtzahlung zu veröffentlichen. Die jährlichen Umsätze von REvil durch Lösegeldzahlungen liegen im Bereich von 100 Millionen US-Dollar. Wenn das betroffene Unternehmen das Lösegeld nicht zahlt, führen die Angreifer einen Distributed-Denial-of-Service-Angriff (DDoS[1]) auf die Kunden und Geschäftspartner des Unternehmens durch. Zu den Angriffszielen von REvil gehören verschiedene Industriebereiche, u. a. im Bereich der Fertigung und Dienstleistung oder beispielsweise IT-Dienstleister oder das Gesundheitswesen, vor allem aber Unternehmen, von denen sich die APT-Gruppierung hohe Lösegelderträge verspricht.

[1] Bei einem DDoS-Angriff werden Internetseiten mit einer Flut von Datenanfragen überrollt, um die Systeme zu überlasten und damit zu einer vorübergehenden Unterbrechung der Möglichkeit des Zugriffs auf diese Seiten zu führen. Dabei stammt der eingehende Datenverkehr aus verschiedenen Quellen.

- Bei BlackCat handelt es sich um eine Ransomware-Gruppierung (siehe Abschnitt B.14.19), welche weltweit Ransomware und RaaS einsetzt und seit Ende des Jahres 2021 aktiv ist. Zu den Angriffszielen von BlackCat gehören Unternehmen in Europa, Afrika, Asien und den USA, wobei oftmals kritische Infrastrukturen (z. B. Energieversorger, Firmen im Bereich Ölproduktion) aber auch staatliche Institutionen (z. B. österreichisches Bundesland Kärnten, ecuadorianische Hauptstadt Quito) Ziel der Angriffe waren. Nach dem Zugriff auf das Zielsystem erfolgt die Exfiltration von Daten des Opfers und die anschließende Verschlüsselung der Daten auf dem System des Opfers. Es erfolgt eine Lösegeldforderung mit der Drohung, die gestohlenen Daten zu veröffentlichen. Die von der Gruppierung BlackCat eingesetzte Schadsoftware ist die erste professionell genutzte Ransomware, die in der Programmiersprache Rust geschrieben wurde. Rust bietet die Möglichkeit, relativ einfach auf mehrere Plattformen übersetzt zu werden, was es leichter macht, die Schadsoftware auf mehrere Betriebssysteme und Prozessarchitekturen anzupassen.

- Black Basta ist eine Ransomware-Gruppierung (siehe Abschnitt B.14.18), die seit April 2022 bekannt ist. Weltweit kam es zu Angriffen von Black Basta auf Unternehmen aus diversen Branchen, wie beispielsweise Fertigungsindustrie, Baugewerbe, Transportwesen, Telekommunikationsunternehmen, pharmazeutische Industrie oder Unternehmen der Energietechnik. Auch Black Basta nutzt die übliche Taktik der doppelten Erpressungsstrategie, bei welcher die Daten vor deren Verschlüsselung extrahiert werden. Wird kein Lösegeld für das Entschlüsseln der Daten gezahlt, werden die exfiltrierten Daten veröffentlicht. Es gibt Hinweise, die darauf hindeuten, dass es sich bei Black Basta um eine russische Gruppierung handelt. Aufgrund der Vielzahl erfolgreich durchgeführter Angriffe in kurzer Zeit und die routinierte Verhandlungsweise mit den Opfern handelt es sich bei Black Basta vermutlich nicht um eine neue Gruppierung, sondern um die Neuauflage einer früheren Ransomware-Gruppierung.

- Die Ransomware-Gruppierung Hive (siehe Abschnitt B.14.31) ist seit Juni 2021 aktiv und hat bis November 2022 weltweit über 1300 Unternehmen angegriffen und rund 100 Millionen US-Dollar an Lösegeldzahlungen erhalten. Die Gruppierung Hive bietet ihre Dienste ebenfalls als RaaS in Form einer maßgeschneiderten Version zum Kauf an. Angriffe erfolgten auf ein breites Spektrum an Unternehmen in über 80 Ländern weltweit.

So wurden Regierungseinrichtungen, Kommunikationseinrichtungen, Produktionsanlagen und Einrichtungen im Gesundheits- und Sozialwesen angegriffen. Neben einer Lösegeldforderung zur Entschlüsselung der bei dem Angriff verschlüsselten Dateien wird ebenfalls damit gedroht, die exfiltrierten Dateien bei einer Nichtzahlung des Lösegeldes zu veröffentlichen. Es ist bekannt, dass Hive die Netzwerke von angegriffenen Organisationen, die ihre Netzwerke ohne die Zahlung von Lösegeld wiederhergestellt haben, erneut angreift. Laut Berichten aus dem Jahr 2023 ist es gelungen, die Gruppierung Hive durch eine gemeinsame Aktion von Ermittlungsbehörden diverser Länder auszuschalten.

- BlackMatter ist eine weitere APT-Gruppierung mit mutmaßlich russischem Hintergrund, welche mit Ransomware-Angriffen erstmals im Juli 2021 in Erscheinung trat. Die BlackMatter Gruppierung bietet ebenfalls RaaS-Dienste an (siehe Abschnitt B.13.7). Die Gruppierung verwendet für ihre Angriffe die gleichnamige Schadsoftware BlackMatter, die von ihr auch als RaaS in Form einer maßgeschneiderten Version zum Kauf angeboten wird. Die Schadsoftware verschlüsselt die Dateien der Opfer, woraufhin die Angreifer (entweder BlackMatter selbst oder deren RaaS-Kunden) eine Lösegeldforderung für die Entschlüsselung der Daten stellen. Dabei wird mit der Veröffentlichung der gestohlenen Daten gedroht. Zu den Angriffsopfern von BlackMatter zählen auch Unternehmen aus dem Bereich der kritischen Infrastruktur, darunter zwei Organisationen des US-amerikanischen Lebensmittel- und Landwirtschaftssektors.

Sensible Daten von Unternehmen, die im Zuge von Ransomware-Angriffen gestohlen wurden, werden bei Zahlungsunwilligkeit der Angriffsopfer häufig auf Leak-Webseiten veröffentlicht. Diese Informationen können dann wiederum von anderen Cyberkriminellen genutzt werden, um weitere Angriffe zu planen. Befinden sich unter den gestohlenen Daten Informationen zu Lieferkettenstrukturen, sind, zusätzlich zu den bereits attackierten Opfern, alle Lieferanten und Kunden des betroffenen Unternehmens potenzielle Opfer von Datenlecks und somit das Ziel von Cyberangriffen. Die Veröffentlichung sensibler Daten auf Leak-Webseiten gewinnt bei den Ransomware-Angriffen immer mehr an Bedeutung. Mit BianLian (siehe Abschnitt B.15.6) ist eine erste Gruppierung dazu übergegangen, hauptsächlich durch Exfiltration zu erpressen. Die IT-Systeme der Opfer bleiben hierbei intakt, es findet keine Verschlüsselung von Daten statt. Es werden aber Daten, bevorzugt von Unternehmen, die häufig mit sensiblen Daten arbeiten, exfiltriert. Die Lösegeldforderung basiert auf der Drohung, die gestohlenen, sensiblen Daten zu veröffentlichen.

Die Gruppierung CL0P Ransomware Gang hat ebenfalls auf eine Verschlüsselung von Daten bei ihrem Cyberangriff auf Nutzer der Software MoveIT Transfer verzichtet und ausschließlich auf die öffentlichkeitswirksame Erpressung nach erfolgreichem Datendiebstahl gesetzt (siehe Abschnitt B.15.35 im Anhang).

Generell sind Ransomware-Angriffe nicht immer auf Büro-IT beschränkt. Im schlimmsten Fall können sich Ransomware-Angriffe auch auf die OT-Netzwerke (Operational Technology), welche zur Verwaltung, Überwachung und Steuerung industrieller Abläufe dienen, und industrielle Steuerungssysteme auswirken (siehe Abschnitt B.15.4 im Anhang). Entweder müssen infolge der Angriffe Teile dieser Systeme vom Unternehmen abgeschaltet werden, um eine weitere Ausbreitung von Schadsoftware zu verhindern, oder diese sind selbst vom Datendiebstahl und der Datenverschlüsselung der Ransomware betroffen. Die Folge sind Produktionsausfälle und Lieferengpässe, was zusätzlich zu dem von den Angreifern geforderten Lösegeld für die Datenentschlüsselung zu einem finanziellen Schaden für das Unternehmen führt. Besonders schwerwiegend sind solche Auswirkungen von Ransomware-Angriffen auf Unternehmen und Organisationen im Bereich der kritischen Infrastrukturen, die z. B. auch die Bereiche der Wasserversorgung, Energieversorgung, Lieferung fossiler Brennstoffe und den Verteidigungssektor umfassen. Ausfälle von ICS-Systemen und Datendiebstahl können hier zu einer eingeschränkten Verfügbarkeit oder sogar zum Ausfall der betroffenen kritischen Infrastruktur führen. Die in diesem Absatz beschriebene Problematik wird durch die im Folgenden behandelten Ransomware-Angriffe verdeutlicht:

- Eine mutmaßlich russische Gruppierung (Beendigung und Löschung der Ransomware bei russischer Systemsprache, Angriffe auf westliche Ziele ausgerichtet) kompromittierte mit Hilfe der Cuba-Ransomware Einrichtungen im Bereich der kritischen Infrastrukturen und erbeutete dabei Lösegeld für die angebliche Wiederherstellung der von ihnen verschlüsselten Daten (siehe Abschnitte B.13.14 und B.14.32 im Anhang). Bei den Angriffen wurde eine Vielzahl von Schadsoftware-Komponenten und Angriffstechniken eingesetzt. Die Cuba-Ransomware erhielt ihren Namen dadurch, dass sie die Endung der von ihr verschlüsselten Dateien in *.cuba* umbenannte. Seit Beginn des Jahres 2021 betreibt die Gruppierung eine Leak-Webseite, auf der sie gestohlene Daten veröffentlicht, sollte das Lösegeld nicht gezahlt werden. Einige der gestohlenen Daten wurden von den Angreifern verkauft. Zu den Angriffszielen gehören der Finanzsektor, Behörden und Regierungen, Gesundheitsorganisationen sowie Produktions- und Informationstechnikunternehmen in den USA, Südamerika und Europa.

- Am 29.01.2022 erfolgte ein Ransomware-Angriff auf Oiltanking, ein Tanklagerlogistikunternehmen und Betreiber diverser Tanklager in Deutschland und weltweit (siehe Abschnitt B.14.16 im Anhang). Der Cyberangriff wurde von der Gruppierung BlackCat ausgeführt und führte dazu, dass in Deutschland alle Be- und Entladesysteme von Oiltanking betroffen waren und Tankwagen nicht mehr beladen werden konnten. Insgesamt waren 233 Tankstellen betroffen, wobei die Versorgungslage in Deutschland nicht gefährdet war, da andere Unternehmen die ausgefallenen Kapazitäten kompensieren konnten.

- Im August 2022 kam es zu einem Ransomware-Angriff auf Nexeya (siehe Abschnitt B.14.27 im Anhang), einem französischen Tochterunternehmen des Rüstungsunternehmers Hensoldt, welches auf den Entwurf und die Entwicklung von elektronischen Geräten für die Luftfahrt, Verteidigungs-, Energie-, Bahn- und Raumfahrtbranche spezialisiert ist. Durch den Angriff, der der Gruppierung REvil zugeschrieben wird, kam es zu Beeinträchtigungen des laufenden operativen Betriebs und zu einer Unerreichbarkeit der Webseite von Nexeya.

- Die Friedrich Vorwerk Gruppe, ein deutsches Unternehmen u. a. zum Bau von Pipelines zur Gasversorgung im Rahmen des Baus von Flüssiggas-Terminals, wurde im November 2022 Opfer eines Ransomware-Angriffs (siehe Abschnitt B.14.28 im Anhang). Der Cyberangriff führte zum Ausfall weiter Teile der IT-Infrastruktur des Unternehmens, was sich nicht nur auf die IT und die Mitarbeiter, sondern auch auf das Unternehmensergebnis ausgewirkt hat, da durch den Angriff die Profitabilität belastet und die Visibilität eingeschränkt wurde. Es dauerte etwa vier Wochen, bis die IT-Infrastruktur nach dem Angriff wieder instandgesetzt war.

- Im Mai 2023 kam es zu einem Ransomware-Angriff auf Asea Brown Boveri (ABB), einem international operierenden Unternehmen der Energie- und Automatisierungstechnik (siehe Abschnitt B.15.1 im Anhang). Der Cyberangriff wurde von der Gruppierung Black Basta ausgeführt und führte dazu, dass ABB vorsorglich diverse IT-Systeme abgeschaltet und VPN-Verbindungen zu Kunden beendet hat, um eine Ausbreitung der Schadsoftware zu verhindern. Durch den Angriff kam es zu Verzögerungen bei der Abwicklung von Projekten und Störungen im Tagesgeschäft und in der Produktion. Zwei Wochen nach dem Angriff waren trotz sofort eingeleiteter Maßnahmen noch nicht alle Systeme wieder in Betrieb.

- CloudNordic und AzeroCloud, dänische Cloud- und Hosting-Anbieter, wurden im August 2023 Opfer eines Ransomware-Angriffs (siehe Abschnitt B.15.3 im Anhang).

Da der Cyberangriff zum Zeitpunkt der Migration von Servern in ein neues Rechenzentrum erfolgte, schaffte dies für die Angreifer die Möglichkeit, auf die zentralen Verwaltungssysteme und die Backup-Systeme zuzugreifen. Durch den Angriff kam es zur Verschlüsselung aller Kundendaten und zur Abschaltung aller Systeme (Webseiten, E-Mail-Systeme, Kundensysteme, Webseiten der Kunden, usw.), wodurch alle Daten, Systeme, Server sowie die Kommunikation verloren gingen. Es kam zur Verschlüsselung sowohl aller Server-Laufwerke als auch der primären und sekundären Backup-Systeme. Da sich die Wiederherstellung der Daten als unmöglich erwiesen hat und eine Lösegeldzahlung nicht erfolgt, sind somit alle Kundendaten unwiederbringlich verloren. Somit sind von diesem Cyberangriff neben CloudNordic und AzeroCloud auch alle Kunden betroffen, deren Daten in der Cloud der Unternehmen gespeichert waren. Dies umfasst mehrere hundert dänische Unternehmen. Dieser Cyberangriff ist somit sowohl für CloudNordic und AzeroCloud als auch die betroffenen Kunden potenziell existenzbedrohend.

- Die Gruppierung BlackCat führte im Februar 2023 einen Ransomware-Angriff auf die Albert Ziegler GmbH (siehe Abschnitt B.15.7 im Anhang) aus, einem deutschen Hersteller von Feuerwehrbedarf und Einsatzfahrzeugen mit Kunden in über 100 Ländern weltweit. Aufgrund des Cyberangriffs wurden sicherheitshalber standortübergreifend alle IT-Systeme abgeschaltet, wodurch die Arbeitsfähigkeit und die Erreichbarkeit stark eingeschränkt wurden. Alle IT-Systeme mussten nach dem Angriff neu aufgesetzt werden, was auch zwei Wochen nach dem Angriff noch nicht vollständig umgesetzt war. Da vermutlich kein Lösegeld gezahlt wurde, kam es im April 2023 zur Veröffentlichung mehrerer gestohlener Daten der Albert Ziegler GmbH auf der Leak-Webseite der Gruppierung BlackCat.

Weitere Ransomware-Angriffe werden im Anhang beschrieben (siehe beispielsweise Abschnitte B.13.5, B.13.6, B.13.10, B.13.11, B.13.13, B.14.7, B.14.8, B.14.14, B.14.17, B.14.29, B.15.2 und B.15.5 im Anhang).

Zusammenfassend ist festzuhalten, dass Ransomware-Angriffe aufgrund der finanziellen Motivation durch die zu erzielenden hohen Lösegeldbeträge und der gleichzeitig immer einfacheren Möglichkeit, dies durch Inanspruchnahme von RaaS-Lösungen auch ohne eigene Fachkenntnisse zu erreichen, eine stetig wachsende Bedrohung darstellen. Dabei steht inzwischen nicht mehr nur die zeitweise Verschlüsselung der Daten des Opfers im Vordergrund, sondern vermehrt auch der Einsatz von Schadsoftwarekomponenten, die nur vorgeblich Ransomwarekomponenten sind, aber keine Funktionalität für die

Entschlüsselung der Daten besitzen und so betroffene Daten dauerhaft zerstören. Auch ist eine Beschränkung der Verschlüsselung auf reine Büro-IT, wie zu Beginn der Ransomware-Angriffe üblich, nicht mehr gegeben. Im Zuge der bei den Angriffen erfolgenden Datenverschlüsselung werden auch immer häufiger ICS-Systeme in Mitleidenschaft gezogen. Dies führt zu Produktionsausfällen, Lieferengpässen und in Verbindung mit der Lösegeldforderung der Angreifer für die Datenentschlüsselung zu einem immensen finanziellen Schaden. Auch ist die Wiedererlangung der verschlüsselten Daten längst nicht mehr der einzig maßgebliche Aspekt der Erpressung. Die Angreifer drohen neben dem Datenverlust zumeist auch mit der Veröffentlichung von im Zuge des Angriffs gestohlenen, sensiblen Daten. Auch geben die Angreifer in manchen Fällen durch eine Ausweitung der Drohungen und mögliche Angriffe auf den Kundenstamm eines Unternehmens ihren Forderungen noch stärkeres Gewicht. Ein in letzter Zeit verstärkt beobachteter Trend zeigt zudem, dass Angreifergruppierungen mehr und mehr auch durch die Hervorrufung von Ausfällen bei verfahrenstechnischen Prozessen den Druck auf die betroffenen Unternehmen noch deutlich erhöhen. Dieser Aspekt wiegt insbesondere bei Ransomware-Angriffen auf Organisationen im Bereich der kritischen Infrastrukturen besonders schwer.

2.2 Social Engineering

Die wesentlichen Aspekte im Zusammenhang mit Cybersicherheit sind nicht nur technischer Natur, sondern umfassen auch alle Bereiche, die den Faktor Mensch und dessen Interaktion mit IT- und OT-Systemen betreffen. Der wichtigste Angriffsvektor ist dabei das „Social Engineering“, bei dem Angreifer Menschen derartig manipulieren und ausnutzen, dass sie freiwillig bzw. nicht wissentlich die Ziele der Angreifer durch eigene Handlungen unterstützen. Die Angreifer sehen somit den Menschen als Schwachstelle und oftmals leichter zu überwindendes Hindernis als beispielsweise technische Sicherheitsvorkehrungen. Hierbei zielen Angreifer direkt auf die Unwissenheit, Arglosigkeit oder Nachlässigkeit des Opfers ab. Allgemein ist das Ziel der Angreifer dabei im Wesentlichen, das Opfer zur Installation von Schadsoftware, zur Preisgabe sensibler Informationen oder zur Durchführung bestimmter Handlungen zu bewegen. Oftmals bezwecken die Angreifer, sich damit temporär oder dauerhaft Zugriff auf Systeme bzw. das Netzwerk der Opfer zu verschaffen. Ein zentrales Merkmal von Angriffen mit Hilfe von Social Engineering ist die Täuschung der Opfer hinsichtlich der Identität und Absicht des Angreifers.

Nach wie vor stellt Social Engineering einen der erfolgreichsten und am häufigsten angewandten Angriffsvektor im Bereich der Cybersicherheit dar, der weiterhin sehr erfolgsversprechend für Angreifer ist und in verschiedenen Formen im Rahmen von einzelnen Cyberangriffen oder Angriffskampagnen realisiert werden kann. Die Opfer von Social Engineering werden hierbei zu unwissentlichen Innentätern.

Generell gilt es zwischen gezielten und ungezielten Angriffen im Zusammenhang mit Social Engineering zu unterscheiden. Ungezielte Angriffe sind mittlerweile allgegenwärtig und haben das Ziel, möglichst viele Personen zu erreichen und somit die Chance für die Angreifer, ein unvorsichtiges Opfer anzusprechen, zu erhöhen. Überwiegend werden dazu entsprechend präparierte Spam-Mails eingesetzt, deren Täuschungsfähigkeit und Professionalität abhängig vom Aufwand und den Fähigkeiten der Angreifer ist. Bei gezielten Angriffen haben die Angreifer klare Absichten für ein bestimmtes Ziel (beispielsweise eine Person oder ein Unternehmen) und versuchen typischerweise möglichst lange unentdeckt zu bleiben. Dazu gehen die Angreifer oftmals mit hohem Aufwand und hoher Professionalität vor, um das potenzielle Opfer zu täuschen. Die ersten Schritte des gezielten Social-Engineering-Angriffs umfassen typischerweise die Beschaffung frei verfügbarer oder einfach zu erlangender Informationen über das Ziel. Dabei kann es sich um Unternehmen und Organisationen handeln, über deren Organisationsstruktur und interne Abläufe der Angreifer Informationen sammelt, sowie um Einzelpersonen bzw. Personen mit einem entsprechenden Bezug zum Unternehmen. Die anschließende Kontaktaufnahme durch die Angreifer kann über verschiedene Wege wie beispielsweise die persönliche Ansprache, über das Telefon/Videotelefonie, postalisch oder am häufigsten digital per E-Mail bzw. Messenger, Social Media oder allgemein über den Browser stattfinden. Mit fortschreitenden technischen Möglichkeiten und unter Verwendung von künstlicher Intelligenz werden dabei die Vorgehensweisen und Täuschungsmöglichkeiten der Angreifer mitunter immer ausgereifter und schwerer zu erkennen. Textnachrichten lassen sich relativ einfach mit herkömmlichen Mitteln fälschen. Die heutige Technik erlaubt es Angreifern darüber hinaus jedoch beispielsweise Stimmen oder auch Videoübertragungen derartig zu manipulieren, dass dem Opfer glaubhaft ein anderer, typischerweise dem Opfer bekannter Gesprächspartner vorgetäuscht wird.

Im Folgenden werden exemplarisch einige der gängigen Techniken im Zusammenhang mit Social-Engineering-Angriffen kurz erläutert:

- Phishing: Im einfachsten Fall werden E-Mails ungezielt an eine Vielzahl Personen versendet mit schadsoftwarebehafteten Anhängen oder Links zu präparierten Internetadressen, wobei sich das Opfer durch das Aufrufen entsprechender Seiten unwissentlich entweder Schadsoftware herunterlädt oder zur Eingabe vertraulicher Informationen aufgefordert wird. In der Regel verwenden die Angreifer Verschleierungstaktiken bzgl. des Absenders wie beispielsweise Identitätsdiebstahl einzelner Personen oder die Vorgabe, es handele sich um eine legitime E-Mail wirtschaftlicher, privater oder öffentlicher Institutionen. Dieser Angriffsvektor ist sehr weit verbreitet, da er mit einfachen Mitteln zu realisieren ist (im einfachsten Fall genügt die Kenntnis einer E-Mail-Adresse bzw. einer Liste von E-Mail-Adressen zur Durchführung). Angriffe über diesen Angriffsvektor lassen sich zudem sehr leicht durch die Angreifer automatisieren.
- Spear-Phishing: Die Vorgehensweise ist ähnlich wie beim Phishing, mit dem Unterschied, dass der Angriff gezielt spezifisch auf eine oder wenige Personen zugeschnitten ist.
- Whaling: Auch hier ist die Vorgehensweise im Wesentlichen wie beim Phishing bzw. Spear-Phishing, wobei die Angriffe spezifisch auf hochrangige Zielpersonen wie CEOs oder CFOs angelegt sind.
- Watering Hole: Hierbei versuchen Angreifer über die Kompromittierung spezifischer Websites, von denen dem Angreifer bekannt ist, dass das Opfer diese besucht, Zugriffsmöglichkeiten auf das Opfersystem/-netzwerk zu verschaffen. Der Angriffsvektor setzt somit bei den Angewohnheiten, Interessen und dem Verhalten von potenziellen Zielen beim Surfen im Internet an. Dabei können die entsprechenden Websites auf unterschiedliche Weise manipuliert werden, beispielsweise über bekannte, aber nicht gepatchte Sicherheitslücken.
- Baiting: Der Angreifer platziert ein mit Schadsoftware präpariertes physisches Gerät (zum Beispiel ein USB-Stick) an einem gezielt ausgewählten Ort, bei dem davon auszugehen ist, dass es vom Ziel gefunden wird bzw. verschickt dieses gezielt an das Opfer. Wenn das Opfer das Gerät dann an einen Computer anschließt, wird die Schadsoftware (ggf. unbemerkt) installiert.
- Scareware: Hierbei versuchen Angreifer ihre Opfer unter Druck zu setzen, indem sie eine angebliche Schadsoftwareinfektion bzw. das Herunterladen angeblich illegaler Inhalte vortäuschen und dem Opfer eine „Lösung“ für diese Problematik anbieten. Die vermeintliche Lösung zur Behebung des vorgetäuschten Problems verleitet das Opfer dann dazu, unwissentlich Schadsoftware des Angreifers herunterzuladen oder sensible Informationen preiszugeben.

- Pretexting: Beim Pretexting täuschen Angreifer falsche Tatsachen vor bzw. ihr Wissen über bestimmte Sachverhalte geschickt ein, um die Opfer dazu zu bringen sensible Informationen preiszugeben oder gegenüber dem Angreifer nützliche Handlungen auszuführen. Die Angreifer erfinden dabei ein fiktives Szenario, um die Opfer zu überlisten. Oftmals nimmt ein Angreifer dazu die Rolle einer Autoritätsperson an, die das Opfer vermeintlich unterstützen will.
- Dumpster Diving: Diese Technik umfasst die Beschaffung von Informationen durch die Angreifer über den vermeintlichen Abfall/Müll des Opfers (digital oder analog). Dazu zählen sowohl Notizen über Passwörter oder andere sensible Informationen wie auch vermeintlich nicht sensible Informationen, die Angreifern jedoch Anhaltspunkte beispielsweise über Gewohnheiten oder Verhaltensweisen des Opfers liefern. Über das Dumpster Diving hinaus gelingt es Angreifern in der heutigen Zeit oftmals durch die Aggregation von freiwillig in Social Media Accounts preisgegebenen Informationen wertvolle Erkenntnisse für ihre Angriffe zu erlangen.

Insgesamt gab es in den vergangenen Jahren eine Vielzahl von Cyberangriffen, bei denen die oben genannten bzw. darüberhinausgehende Social-Engineering-Techniken eingesetzt wurden und typischerweise als Einfallstor zur Erlangung des initialen Zugriffs auf die Systeme und Netzwerke der Opfer für die Angreifer dienten – oftmals auch auf sicherheitskritische Einrichtungen. In Anbetracht dessen sind für die Gewährleistung der Cybersicherheit Sicherungsmaßnahmen, die den Anwender und Mitarbeiter als menschlichen Faktor berücksichtigen, essenziell für kritische Infrastrukturen, insbesondere für Kernkraftwerke sowie sonstige kerntechnische Anlagen und Einrichtungen. Die Etablierung und Aufrechterhaltung einer entsprechenden Sicherungskultur einschließlich regelmäßiger Trainings, Sensibilisierungsmaßnahmen und Maßnahmen in Bezug auf die Awareness der Mitarbeiter liegt mittlerweile im Fokus nationaler und internationaler Organisationen und Behörden weltweit. Social-Engineering-Angriffe sind dabei nicht nur für global agierende Unternehmen oder staatliche Behörden relevant, obgleich erfolgreiche Angriffe, bei denen derartige Techniken eingesetzt werden, in diesem Fall weitreichende und kritische Auswirkungen haben können. Auch kleinere Unternehmen und Institutionen sind oftmals lohnende Ziele für Angreifer, insbesondere wenn sie Verbindungen zu größeren Unternehmen und Behörden haben (siehe Abschnitt 2.4). Nachfolgend werden einige bedeutende IT-Sicherheitsvorfälle im Zusammenhang mit Social Engineering kurz exemplarisch beschrieben.

Die im Folgenden kurz beschriebenen IT-Sicherheitsvorfälle in Zusammenhang mit Social Engineering sind hierbei nur ausgewählte Beispiele aus der großen Menge an Cyberangriffen, bei denen Social-Engineering-Techniken eingesetzt werden.

- Social-Engineering-Techniken werden häufig von APT-Gruppierungen (siehe Abschnitt 2.10) eingesetzt, beispielsweise durch die mutmaßlich nordkoreanische Gruppierung APT38/Lazarus (siehe Abschnitt 2.10.3), welche zur Erlangung des initialen Zugriffs auf Zielsysteme und -netzwerke Spear-Phishing- und Watering Hole-Techniken einsetzt. Auch die ebenfalls nordkoreanische Gruppierung Kimsuky (siehe Abschnitt APT 2.10.8) setzt zur Erlangung des initialen Zugriffs überwiegend auf Phishing, Spear-Phishing und Watering Hole Angriffe, beispielsweise im Rahmen einer Angriffskampagne 2020 auf Vertreter des Sicherheitsrats der Vereinten Nationen und im letzten Jahr im Rahmen einer Spionagekampagne im Zusammenhang mit einer jährlich stattfindenden gemeinsamen Militärübung der USA und Südkorea (siehe Abschnitt B.15.33 im Anhang).
  Die dem russischen Militärgeheimdienst zugeordnete Gruppierung APT28/Fancy Bear (siehe Abschnitt 2.10.1) führte im Jahr 2021 eine Spear-Phishing-Kampagne auf die E-Mail-Postfächer von Googlemail-Nutzern durch mit dem Ziel, Passwörter zu stehlen, Zugriff auf die Postfächer und die darin enthaltenen Informationen zu erlangen und dadurch weitere Angriffe überwiegend auf ausgewählte Aktivisten, Journalisten, Regierungsmitarbeiter, Menschenrechtler, Rechtsanwälten und Angestellte im Bereich der Nationalen Sicherheit ausführen zu können. Auch die mutmaßlich ebenfalls russischen Gruppierungen Sandworm (siehe Abschnitt 2.10.11) und Turla (siehe Abschnitt 2.10.13) sowie die chinesische Gruppierung Tonto Team (siehe Abschnitt APT 2.10.12) setzten in der Vergangenheit bereits Social-Engineering-Techniken im Rahmen ihrer Angriffskampagnen ein.
- Bei einem Cyberangriff auf einen deutschen KRITIS Betreiber setzten unbekannte Angreifer im Jahr 2023 unter anderem Videomaterial des Geschäftsführers ein (siehe Abschnitt B.15.24 im Anhang). Dabei wurden Mitarbeiter mit Freigabeberechtigungen für Zahlungen gezielt zu einer manipulierten Videokonferenz eingeladen, bei der in einem anderen Zusammenhang erstelltes, authentisches Videomaterial des Geschäftsführers gezeigt und anschließend aufgrund vermeintlicher technischer Probleme auf einen Messenger-Dienst zur weiteren Besprechung verwiesen wurde.

Die Angreifer hatten sich im Vorfeld (ggf. über Social-Engineering-Techniken) mutmaßlich Informationen über Positionen und Freigabeberechtigungen im Unternehmen verschafft und versuchten unter der Vortäuschung falscher Tatsachen und mit Hilfe der illegitimen Verwendung entsprechenden Videomaterials die Opfer zur Ausführung bestimmter Handlungen zu bewegen.

- Social-Engineering-Techniken werden und wurden häufig auch in Zusammenhang mit dem Krieg in der Ukraine (siehe Abschnitt 2.8) sowie mit weiteren politischen Spannungsfeldern (siehe Abschnitt 2.9) eingesetzt. Hierbei sind einerseits Social-Engineering-Angriffe im Zusammenhang mit russischen Cyberangriffen auf ukrainische und osteuropäische Ziele zu nennen. Dabei wurden beispielsweise im Juni 2023 E-Mail-Server ukrainischer Behörden und Regierungsstellen mit Hilfe einer Phishing-Kampagne kompromittiert (siehe Abschnitt B.15.16 im Anhang) und im Frühjahr 2023 wurden verschiedene diplomatische Einrichtungen in Osteuropa mit einer Phishing-Kampagne angegriffen (siehe Abschnitt B.15.10 im Anhang). Zudem verüben mutmaßlich der islamischen Republik Iran zugehörige Gruppierungen seit mehr als zehn Jahren Cyberangriffe in einem weiten Umfeld, bei denen Social-Engineering-Techniken und insbesondere Phishing eingesetzt wird (siehe Abschnitt B.14.36 im Anhang).
- Ein Beispiel für die Social-Engineering-Technik Baiting stellt eine Angriffskampagne einer Angreifergruppierung auf US-Unternehmen, insbesondere aus der Transport-, Versicherungs- und Rüstungsbranche im Jahr 2021 dar, bei der Angreifer USB-Sticks an die Opfer verschickt haben (siehe Abschnitt B.14.15 im Anhang). Diese wurden beispielsweise als Geschenkbox bzw. vermeintliche Covid-19-Informationsdatenträger ausgegeben und enthielten Ransomware (siehe Abschnitt 2.1). Als vermeintliche Absender wurden das US Department of Health and Human Services bzw. das Unternehmen Amazon angegeben und die Pakete wurden über den US Postal Service oder den Transportdienstleister UPS versendet. Die Opfer sollten somit getäuscht und dazu gebracht werden, den USB-Stick anzuschließen, wodurch sie Opfer der Ransomware geworden wären.
- Auch im Zusammenhang mit IT-Sicherheitsvorfällen mit nukleartechnischem Bezug (siehe Abschnitt 2.7) wurden in der Vergangenheit bereits Social-Engineering-Techniken eingesetzt. Beispielsweise wurden mutmaßlich ab 2010 Spear-Phishing-Angriffe durch einen ehemaligen U.S. NRC-Mitarbeiter auf Mitarbeiter des U.S. Department of Energy durchgeführt (siehe Abschnitt B.5.3 im Anhang). Das Ziel war dabei unter anderem die Informationsbeschaffung zum Nuklearsektor, beispielsweise über Nuklearwaffen. Außerdem wurden beim Cyberangriff auf

den französischen Baudienstleisters Ingérop, der für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo arbeitet, Social-Engineering-Techniken in Form von Phishing eingesetzt (siehe Abschnitt B.10.2 im Anhang).

Zusammenfassend ist festzuhalten, dass Social Engineering, eine Gruppierung von Angriffstechniken für Cyberangriffe bei denen Angreifer vorwiegend auf den Menschen als Schwachstelle für den Bereich Cybersicherheit abzielen, seit vielen Jahren eingesetzt wird und auch heute noch einen überaus erfolgversprechenden Angriffsvektor darstellt, der in nahezu allen Bereichen zahlreich angewandt wird. Typischerweise nutzen Angreifer und insbesondere APT-Gruppierungen Social Engineering dabei zur Erlangung des initialen Zugriffs auf die Systeme und Netzwerke ihrer Opfer, d. h. als einen der ersten von mehreren Angriffsschritten. Diesbezüglich gibt es viele unterschiedliche Angriffstechniken, von denen insbesondere das Phishing, bei dem Angreifer ihren Zielen Täuschungsnachrichten mit dem Ziel der Verteilung von Schadsoftware oder zur Informationsgewinnung zusenden, weitläufig – gezielt und ungezielt - eingesetzt wird. Sicherungsmaßnahmen, die den Anwender und Mitarbeiter als menschlichen Faktor berücksichtigen und die Etablierung einer entsprechenden Sicherungskultur sind daher essenziell.

2.3 Schadsoftwarefreie Angriffe und Living-off-the-Land

In den vergangenen Jahren ist die Bedrohung durch Cyberangriffe nicht nur deutlich gewachsen, ihr wird heutzutage auch von Seiten vieler Unternehmen, Behörden und Einrichtungen mit entsprechenden Sicherungsmaßnahmen begegnet. Diese Sicherungsmaßnahmen dienen häufig dem Schutz von IT-Systemen vor Cyberangriffen, zunehmend aber auch der Detektion potenzieller Angriffshandlungen, sollte es den Angreifern gelingen, die präventiven Maßnahmen zu überwinden. Diese detektiven Sicherungsmaßnahmen sind vor allem relevant für Angreifer, die langfristig Angriffshandlungen ausführen und daher einen persistenten Zugriff auf ein kompromittiertes System herstellen wollen. Daher verschiebt sich der Fokus insbesondere bei komplexen Cyberangriffen und Cyberangriffen, bei denen verdeckt ablaufende Angriffsschritte wesentlich sind, immer stärker in Richtung Detektionsevasion. Die Vergrößerung der Chancen, dass der Cyberangriff nicht detektiert wird, ist ein Grund für die deutliche Zunahme an schadsoftwarefreien Angriffen und dem vermehrten Einsatz von Living-off-the-Land, der im vergangenen Jahr deutlich zu beobachten war.

Bei Living-off-the-Land nutzen die Angreifer bereits auf dem angegriffenen System vorhandene, legitime Programme, Funktionen oder Dienste missbräuchlich für ihre Zwecke. Da auf diese Art und Weise keine Schadsoftware eingebracht werden muss und die Kommunikation mit oder von den missbräuchlich eingesetzten Programmen zudem häufig wie legitime Kommunikation wirkt, ist dies mit einem deutlich geringeren „Fußabdruck" verbunden als die Einbringung einer Schadsoftware, welche dieselben Zwecke erfüllt. Somit ist die Gefahr einer Detektion deutlich geringer. Der Einsatz von Living-off-the-Land ist inzwischen bei vielen Angreifergruppierungen, insbesondere bei APT-Gruppierungen zu beobachten. So setzte beispielsweise die russische Gruppierung Sandworm, die sich bis dahin stark auf schadsoftwarebasierte Angriffe konzentriert hatte, auch Living-off-the-Land-Techniken ein, als sie im Oktober 2022 Angriffe auf die Energieversorgung in der Ukraine durchführte (diese Angriffe wurden erst im November 2023 bekannt und sind daher noch nicht im Anhang dieses Berichtes beschrieben). Es gibt darüber hinaus aber auch Angreifergruppierungen wie beispielsweise die dem chinesischen Nexus zugerechnete Gruppierung Volt Typhoon, die bei ihren Angriffen zur Detektionsevasion nahezu ausschließlich auf Living-off-the-Land-Techniken zurückgreift (siehe Abschnitt B.15.26). Hierbei ist anzumerken, dass ein schadsoftwarefreies Vorgehen, das sich hauptsächlich auf Living-off-the-Land stützt, häufig einen Hands-on-keyboard Zugriff für die Angreifer erfordert, d. h. einen Zugriff von außen, mit dem ein Angreifer unmittelbar auf das kompromittierte System zugreifen kann (sofern die Angreifer sich keinen physischen Zugang zu diesem System verschafft haben).

Eine sehr gängige Technik für einen schadsoftwarefreien Erstzugriff ist die Nutzung legitimer Zugangsdaten. Es gibt für Angreifer zahlreiche Möglichkeiten, an legitime Zugangsdaten zu gelangen. Beispiele hierfür sind im Abschnitt Social Engineering (siehe Abschnitt 2.2) beschrieben. Hierbei ist zu beachten, dass bereits viele der dort beschriebenen Techniken schadsoftwarefrei ablaufen können und daher die Detektion schwieriger ist.

Insgesamt ist sowohl die Zahl schadsoftwarefreier Cyberangriffe als auch die Zahl an Cyberangriffen, bei denen die Angreifer teilweise auf schadsoftwarefreie Techniken wie die Nutzung legitimer Zugangsdaten oder Living-off-the-Land zurückgreifen, in den vergangenen Monaten deutlich gestiegen. Es ist zu erwarten, dass sich dieser Trend in den kommenden Monaten und Jahren weiter verstärken wird.

2.4 Supply-Chain-Angriffe

Supply-Chain-Angriffe bleiben in Anbetracht der fortschreitenden Digitalisierung und Globalisierung weltweit in nahezu sämtlichen Bereichen inklusive der Lieferketten von IT-Systemen und industriellen Steuerungssystemen hochgradig relevant. Die steigende Komplexität von Software, Hardware und IT-Dienstleistungen in diesem Zusammenhang bietet Angreifern vielfältige Möglichkeiten, insbesondere innerhalb der Lieferkette von Komponenten oder Diensten. IT-Sicherheitsvorfälle der jüngeren Vergangenheit wie die Supply-Chain-Angriffe auf international aufgestellte Unternehmen bzw. Produkte, die weltweit große Aufmerksamkeit erfuhren, verdeutlichen die potenziell verheerenden Folgen derartiger Angriffe.

Grundsätzlich betrifft die Frage der IT-Sicherheit in der Lieferkette alle IT-Systeme, die in kritischen Infrastrukturen und kerntechnischen Anlagen und Einrichtungen eingesetzt werden. Dies beinhaltet sowohl Software- als auch Hardwarebestandteile. In der heutigen Zeit werden die Bestandteile der Software und Hardware in der Regel nicht vollständig von einzelnen Herstellern oder Unternehmen alleinig erzeugt bzw. hergestellt, sondern durch verschiedene und häufig mehrere Zulieferer bereitgestellt. Zudem sind nicht zwangsläufig alle Softwarebestandteile, die für ein IT-System erforderlich sind, lokal auf dem betreffenden IT-System vorhanden, sodass externe Softwarebestandteile erforderlich sind, die über entsprechende Abhängigkeiten eingebunden werden. Bei der Lieferkette eines IT-Systems kann es sich prinzipiell um eine einzelne, unverzweigte Verbindung zwischen einem Betreiber und einem beauftragten Unternehmen handeln. Sehr viel wahrscheinlicher ist in der heutigen Zeit jedoch, dass die Lieferkette eines IT-Systems von einer ganzen Reihe von Lieferketten und darin enthaltenen Hard- und Softwarebestandteilen abhängt, von denen jedes einzelne für sich allein genommen als Zwischenziel eines potenziellen Cyberangriffs dienen kann. Zudem sind Angriffe auf die Lieferkette eines IT-Systems nicht auf die „erste Lieferung“ eines IT-Systems bzw. seiner Komponenten beschränkt, sondern umfassen den gesamten Lebenszyklus. Dies beinhaltet u. a. neben der Konzeptions-, Entwurfs- und Entwicklungsphase auch die generelle Nutzung, Wartung und Pflege nach der Auslieferung sowie die Ausmusterung und Entsorgung. Somit umfasst das Thema IT-Sicherheit in der Lieferkette auch auf jegliche Art im weiteren Verlauf nach der ursprünglichen Auslieferung erfolgte Hardware- und Software-Lieferung, -Aktualisierung oder -Modifizierung beispielsweise im Rahmen von Wartung, Instandhaltung oder zu Update-, Konfigurations- und Parametrierzwecken. Cyberangriffe über die Lieferkette unterscheiden sich dementsprechend grundsätzlich dadurch, an welcher Stelle der Lieferkette, d. h. in welcher Phase des Software- bzw.

Hardwarelebenszyklus ein Angriff erfolgt, wobei ein Angriff prinzipiell in jeder Phase erfolgen kann und nicht auf eine Phase beschränkt sein muss.

Durch die Abhängigkeiten und Wechselwirkungen der einzelnen Schritte im Lebenszyklus eines IT-Systems, der Involvierung von in der Regel mehreren Zulieferern und der sich dadurch bietenden unterschiedlichen Angriffsmöglichkeiten, liegen bei Supply-Chain-Angriffen die Möglichkeiten zur Verhinderung, Abwehr oder Unterbrechung der Angriffe nur bis zu einem gewissen Grad im Einflussbereich des potenziellen Angriffsziels. Beispielsweise können Betreiber kritischer Infrastrukturen indirekt von Cyberangriffen über die Lieferkette betroffen sein, wenn mit den Betreibern in Verbindung stehende IT-Dienstleister Ziele solcher Angriffe sind. Zudem pflegen Hersteller bzw. IT-Dienstleister unter Umständen einen unterschiedlichen Umgang mit Cyberangriffen und Schwachstellen, wobei insbesondere die Kommunikation infolge solcher IT-Sicherheitsvorfälle oftmals nicht optimal ist und Informationen nur verspätet, nicht vollständig oder gar nicht weitergegeben werden. Für Betroffene ist eine gesicherte und stets aktuelle Informationslage essenziell, um Risiken für die eigene Organisation einschätzen und ggf. frühzeitig Maßnahmen ergreifen zu können, da auf Schwachstellen oder Sicherheitsrisiken nur reagiert werden kann, wenn diese bekannt sind. Insgesamt sind somit zur Vermeidung von IT-Sicherheitsvorfällen für Betreiber kritischer Infrastrukturen nicht nur das Sicherheitsmanagement und entsprechende Sicherheitsmaßnahmen vor Ort, sondern auch darüberhinausgehende organisatorische Maßnahmen relevant, die den gesamten Lebenszyklus von Hard- und Softwarekomponenten eingesetzter IT-Systeme einschließen und permanent aktualisiert und an neue Erkenntnisse angepasst werden müssen.

Wie bereits diskutiert, kommt IT-Dienstleistern im Zusammenhang mit Supply-Chain-Angriffen eine besondere Bedeutung zu. Dies ist im Wesentlichen darin begründet, dass Cyberangriffe auf derartige Unternehmen Angreifern potenziell eine Vielzahl möglicher Opfer bieten und somit die Auswirkungen eines einzelnen erfolgreichen Angriffs sich möglicherweise auf eine große Zahl mit dem IT-Dienstleister in Verbindung stehender Unternehmen erstrecken. Außerdem werden in der heutigen Zeit immer mehr Dienste und Dienstleistungen durch externe Unternehmen und Dienstleister bereitgestellt, wodurch sich die potenzielle Angriffsoberfläche fortwährend vergrößert. Sowohl für finanziell motivierte Angreifer wie auch für Angreifer, deren Ziel die Einschränkung der Verfügbarkeit von Diensten und Dienstleistungen ist, bieten derartige Angriffe somit ein erstrebenswertes Kosten-Nutzen-Verhältnis. Zudem stellt für Angreifer, deren Motive

Informationsdiebstahl und Spionage sind, ein Cyberangriff auf zentrale Dienstleister, die ggf. für mehrere Behörden oder Unternehmen tätig sind, ein lohnendes Ziel dar. Dies gilt sowohl für gezielte Cyberangriffe wie auch für Cyberangriffe, bei denen Angreifer kein spezifisches Angriffsziel im Auge haben (den IT-Dienstleister selbst oder ein damit in Verbindung stehendes Unternehmen). Zudem sind bei derartigen Cyberangriffen auf IT-Dienstleister nicht nur deren direkte Kunden betroffen, sondern potenziell auch Unternehmen und Einrichtungen, die selbst keine Beziehung zum angegriffenen Dienstleister haben, deren Zulieferer und IT-Dienstleister jedoch eine entsprechende Verbindung zum Angriffsziel haben (siehe Abschnitt B.13.4). Ansonsten gelten für Supply-Chain-Angriffe über bzw. auf IT-Dienstleister die gleichen oben genannten Aspekte, insbesondere hinsichtlich der potenziellen Umgehung von Sicherheits- und Sicherungsmaßnahmen sowie der Komplexität und Vielschichtigkeit der Lieferketten im Allgemeinen.

Generell gab es in den vergangenen Jahren wiederholt Cyberangriffe auf sicherheitskritische Einrichtungen, die mit der Lieferkette von IT-Systemen zusammenhängen. In Anbetracht dessen ist die Gewährleistung der Cybersicherheit in der gesamten Lieferkette eine wesentliche und herausfordernde Aufgabe für kritische Infrastrukturen, insbesondere für Kernkraftwerke sowie sonstige kerntechnische Anlagen und Einrichtungen. Die hohe Relevanz dieser Thematik für den Bereich der Cybersicherheit wird auch international zunehmend diskutiert und liegt im Fokus nationaler und internationaler Behörden und Organisationen weltweit. Zahlreiche Angreifer haben in den vergangenen Jahren für ihre Cyberangriffe explizit auf bekannte bzw. zum Angriffszeitpunkt unbekannte Schwachstellen in der Lieferkette von IT-Systemen gesetzt, um ihre Ziele zu erreichen. Insbesondere kleinere oder mittelständische Hersteller oder IT-Dienstleister, die bezüglich IT-Sicherheitsmaßnahmen verglichen mit internationalen Großunternehmen lediglich eingeschränktere Möglichkeiten haben, stellen sich so oftmals als schwächstes Glied in der Lieferkette heraus, welches sich Angreifer gezielt auswählen, um darüber Zugriff auf andere Unternehmen, Organisationen oder Betreiber kritischer Infrastrukturen zu erhalten, die besser geschützt sind. Aber auch global agierende Unternehmen mit hohen Sicherheitsstandards können Opfer von Cyberangriffen über die Lieferkette werden, wobei dies oft Folgen erheblichen Ausmaßes hat. Nachfolgend werden bedeutende IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette von IT-Systemen kurz exemplarisch beschrieben:

- Im Jahr 2021 wurden Informationen über schwerwiegende Sicherheitslücken bei Microsoft bekannt, welche von Angreifern dazu ausgenutzt werden können, um Microsoft Exchange Server, welche unter anderem für das weltweit verbreitete

E-Mail und Organisations-Programm Outlook genutzt werden, vollständig zu kontrollieren (siehe Abschnitt A.5.1 im Anhang). Zum Zeitpunkt des Bekanntwerdens wurde die Schwachstelle bereits aktiv von Angreifern ausgenutzt, wodurch potenziell eine hohe Anzahl von Unternehmen, Behörden und Betreibern kritischer Infrastruktur betroffen war. Die Schwachstellen ermöglichen neben der Übernahme des gesamten Systems aus der Ferne durch Angreifer auch Datendiebstahl und die Installation von Schadsoftware. In Deutschland waren Anfang 2021 von den Schwachstellen zehntausende Server potenziell betroffen.

- Potenzielle Angreifer können wie oben beschrieben, bereits im Entwicklungs- oder Updateprozess eingreifen und entsprechende Angriffe vorbereiten. Im Juli 2021 ereignete sich zum Beispiel ein Cyberangriff auf Server verschiedener weltweit verbreiteter Unternehmen über die Software VSA des amerikanischen IT-Dienstleisters Kaseya (s. Abschnitt B.13.4 im Anhang). Die betroffene Software, ein Remote-Monitoring und -Management-Tool, mit dem Dienstleistungen wie beispielsweise Fernwartung o. Ä. durchgeführt werden können, wird von über 1.000 Firmen verwendet. Die Angreifer nutzten dabei mehrere Sicherheitslücken und Zero-Day-Exploits aus, um die VSA-Server zu manipulieren und so ein vorher präpariertes, schadsoftwarebehaftetes Update zu platzieren, welches entsprechend durch die Server an die Clients weitergegeben wurde und zur Verschlüsselung der betroffenen Systeme führte. Neben den direkt betroffenen Unternehmen, die mit Kaseya in Verbindung standen, waren auch Firmen betroffen, die selbst keinen direkten Bezug zu Kaseya hatten, sondern lediglich deren IT-Dienstleister oder Zulieferer VSA nutzten.

- Bezüglich manipulierter, schadsoftwarebehafteter Solar-Winds-Produkte und Updates wurde im Dezember 2020 eine Angriffswelle von Cyberangriffen über die Lieferkette entdeckt (siehe Abschnitt B.12.4 im Anhang). Betroffen hiervon war die Software-Plattform SolarWinds Orion, die unter anderem Monitoring und Management von IT-Netzwerken, -Systemen und -Anwendungen ermöglicht und von 33.000 SolarWinds Kunden genutzt wird. Bei diesem IT-Sicherheitsvorfall gelang es den Angreifern, unbemerkt eine Reihe von SolarWinds Orion Versionen mit einer Schadsoftwarekomponente zu infizieren, welche dann digital signiert und somit für Endkunden vom Hersteller zertifiziert ab März 2020 über den offiziellen Update-Server von SolarWinds verteilt wurden. Der Cyberangriff war insbesondere für die Endkunden sehr schwer detektierbar und blieb über ein halbes Jahr lang unbemerkt. Von den Cyberangriffen betroffen waren unter anderem eine Reihe von US-Ministerien

und Behörden (bspw. die US-Departments of Homeland Security, Justice, Energy, Commerce und Treasury ebenso wie das US Department of State und die National Institutes of Health) sowie große, private IT-Unternehmen wie Microsoft oder Cisco und auf Analysen von Cyberangriffen spezialisierte Firmen wie FireEye.

- Neben IT-Sicherheitsvorfällen im Zusammenhang mit globalen Unternehmen, weitreichenden Auswirkungen und einer über die IT-Sicherheitsbranche hinausgehende Berichterstattung, gab es in den letzten Jahren wiederholt Cyberangriffe auf kleinere, mittelständische und lokal agierende Dienstleister, die verschiedene IT-Dienstleistungen für Unternehmen, Behörden und Institutionen anbieten. Die Auswirkungen dieser Supply-Chain-Angriffe betrafen neben den Dienstleistern selbst oftmals direkt deren Kunden und resultierten beispielsweise in Informationsdiebstahl oder dem Ausfall von Diensten und IT-Dienstleistungen. Neben internationalen Fällen, wie beispielsweise im Zusammenhang mit Cellcom in Israel (siehe Abschnitt B.14.9 im Anhang) oder Okta in den USA (siehe Abschnitt B.14.11 im Anhang), gab es in den letzten Jahren auch IT-Sicherheitsvorfälle im Zusammenhang mit IT-Dienstleistern in Deutschland. Im November 2021 wurde beispielsweise die Kisters AG, ein IT-Dienstleister unter anderem tätig im Bereich der kritischen Infrastrukturen, der beispielsweise Energieerzeuger, Netzbetreiber und Messstellenbetreiber mit Softwareprodukten versorgt, Opfer eines Ransomware-Angriffs, bei dem auch Daten gestohlen wurden (siehe Abschnitt B.13.6 im Anhang). Neben dem Informationsdiebstahl gab es darüber hinaus keine bekannten Auswirkungen für die Kunden des Unternehmens. Zu einem weiteren Fall von Informationsdiebstahl im Zusammenhang mit einem IT-Dienstleister kam es im vergangenen Jahr, als das Unternehmen Adesso, zu dessen Kundenkreis neben Behörden der Bundes-, Landes- und Kommunalverwaltung auch Betreiber kritischer Infrastrukturen gehören. Dabei verschafften sich die Angreifer, mutmaßlich über Monate hinweg, unbemerkt Informationen über Adesso und dessen Kunden (siehe Abschnitt B.15.30 im Anhang). Der deutsche IT-Dienstleister Bitmarck, der mit diversen Krankenkassen in Deutschland zusammenarbeitet und beispielsweise Dienstleistungen im Zusammenhang mit der elektronischen Krankenkassenkarte und elektronischen Patientenakte anbietet, wurde im Jahr 2023 Opfer von Cyberangriffen. Neben dem Abfluss von Informationen kam es dabei temporär unter anderem zu technischen Störungen und Einschränkungen im Tagesgeschäft mehrerer gesetzlicher Krankenversicherungen in Deutschland (siehe Abschnitt B.15.38 im Anhang).

- Weitere Cyberangriffe im Zusammenhang mit der Lieferkette erfolgten auf die Software- bzw. IT-Dienstleistungsunternehmen Centreon (siehe Abschnitt B.13.2), CodeCov (siehe Abschnitt B.13.3), und Ivanti (siehe Abschnitt B.14.12). Obwohl Cyberangriffe über die Lieferkette nicht grundsätzlich auf Schwachstellen in der entsprechenden Software angewiesen sind, sind die potenziellen Folgen, wenn entsprechende Schwachstellen oder Zero-Day-Exploits vorliegen, oftmals verheerend. In diesem Zusammenhang verursachte das Bekanntwerden einer Schwachstelle in der Java Programmierbibliothek Log4j des amerikanischen Herstellers Apache im Dezember 2021 weltweit großes Aufsehen (siehe Abschnitt A.4.12). Log4j ist Teil diverser Open-Source- und kommerzieller Softwareprodukte und hat sich zu einem De-Facto-Standard im Bereich des Loggings in Java entwickelt, der entsprechend weit verbreitet ist. Die Log4Shell genannte Schwachstelle ermöglicht es Angreifern bei einem Cyberangriff über Abhängigkeiten bzw. das Einbinden externer Java-Bibliotheken beliebigen Code auf dem angegriffenen System auszuführen und beispielsweise die vollständige Systemkontrolle zu übernehmen. Die Schwachstelle kann vollautomatisiert direkt über das Internet ausgenutzt werden. Weltweit wurden zahlreiche Cyberangriffe über die Schwachstelle registriert.

Insgesamt gilt weiterhin, dass Supply-Chain-Angriffen im Kontext der IT-Bedrohungslage eine große Bedeutung zukommt. Dies gilt insbesondere für kritische Infrastrukturen und industrielle Steuerungssysteme. Zum einen stellt die Lieferkette gerade bei Anlagen mit ausgefeilten, sorgfältig umgesetzten IT-Sicherheitskonzepten und durch zahlreiche Sicherungsmaßnahmen und Barrieren geschützten IT-Systemen einen wesentlichen Angriffspfad in Bezug auf Cyberangriffe dar. Zum anderen reduzieren sich die Möglichkeiten, die der Endkunde zur Detektion von schadsoftwarebehafteten Produkten hat, je früher im Entwicklungsprozess der Soft- oder Hardware die Angreifer ihre Manipulationen vorgenommen haben. Auch sind die Detektionschancen für eine vorliegende Infektion mit Schadsoftware typischerweise geringer, wenn die Schadsoftware über die Lieferkette eingebracht wurde, da so der Footprint beim eigentlichen Angriffsziel kleiner bleibt. Daher sind die Erfolgsaussichten bei Supply-Chain-Angriffen auf gut geschützte Ziele meist deutlich höher als bei direkten Cyberangriffen von außen. In der jüngeren Vergangenheit kam es zudem vermehrt zu Cyberangriffen auf IT-Dienstleister, denen eine besondere Bedeutung im Zusammenhang mit Supply-Chain-Angriffen zukommt, insbesondere, da Angreifer durch Cyberangriffe auf einzelne derartige Unternehmen potenziell eine Vielzahl damit in Verbindung stehender Ziele Treffen können.

2.5 Schwachstellen in ICS als Angriffsvektor für Cyberangriffe

Industrielle Steuerungssysteme (ICS) werden zur Regelung, Steuerung und Überwachung von industriellen und verfahrenstechnischen Prozessen eingesetzt. Die zugrundeliegenden Systeme werden in diversen industriellen Umgebungen und unter anderem auch in kritischen Infrastrukturen, beispielsweise im Bereich Energieerzeugung einschließlich in Kernkraftwerken bzw. anderen kerntechnischen Anlagen und Einrichtungen eingesetzt. Die im Rahmen der industriellen Steuerungssysteme eingesetzte Technologie basiert dabei auf verschiedensten Einzelkomponenten und Systemen unterschiedlicher Anbieter, Dienstleister und Hersteller. Cyberangriffe auf industrielle Steuerungssysteme werden als hochgradig problematisch angesehen, da hierbei u. a. physische Prozessabläufe gestört, manipuliert oder unterbrochen und so industrielle Abläufe, ganze Produktionsketten oder darüber hinaus kritische Infrastrukturen beeinträchtigt werden können.

Befinden sich im Programmcode einer Software eines Gerätes Inkonsistenzen oder Fehler, die vom Hersteller nicht erkannt und deshalb nicht abgefangen wurden und ermöglichen diese, die üblichen Softwarefunktionen bzw. deren sicherheitstechnischen Einschränkungen zu umgehen, dann spricht man im Allgemeinen von einer Schwachstelle. Je nach technischer Ausprägung, ergeben sich verschiedene Angriffsmöglichkeiten auf betroffene Geräte. Manche Schwachstellen versetzen einen Angreifer in die Lage Konfigurationsdaten sowie Passwörter oder Schlüssel, unter Umständen sogar als Klartext, auszulesen. Mit diesen Informationen können z. B. neue Benutzer mit Administratorrechten eingerichtet, der Datenverkehr des Netzwerks ausspioniert oder Aktivitäten eines Angreifers verschleiert werden. Oftmals verschafft die Ausnutzung derartiger Schwachstellen Angreifern überhaupt erst den initialen Zugriff auf IT-Netzwerke und die Möglichkeit, sich innerhalb der Netzwerke lateral zu bewegen. Ähnliche Schwachstellen in der Software von ICS-Geräten dienen entsprechend als Angriffsvektor auf diese und die mit ihnen verbundenen Geräte. Bietet eine Schwachstelle Angreifern die Möglichkeit Einfluss auf den Datenverkehr zu nehmen, so können sie diesen manipulieren und Man-in-the-Middle-Angriffe durchführen. Über andere Schwachstellen kann eigener Programmcode auf Geräten platziert und/oder ausgeführt werden. Auf diese Weise können Angreifer ICS unter Umständen vollständig übernehmen, deren Zustand verändern und immense, zum Teil physische Schäden herbeiführen. Manche Schwachstellen ermöglichen zudem Denial-of-Service-Angriffe (DoS). Dabei wird ein bestimmtes Gerät innerhalb kurzer Zeit mit Kommunikationsanfragen bombardiert oder es wird ein bestimmter Befehl gesendet, so dass das Gerät nicht mehr reagieren kann.

Es geht entsprechend in den Stand-By-Modus über oder schaltet sich ganz ab. Besonders fatal ist dies, wenn das Gerät sicherheitstechnisch relevante Aufgaben übernimmt.

Wird eine Schwachstelle entdeckt, dann sollte der Hersteller des Geräts umgehend informiert werden, damit dieser einen Patch bzw. ein Softwareupdate entwickeln kann, um die Schwachstelle zu schließen. Oftmals werden Schwachstellen von IT-Sicherheitsunternehmen aufgedeckt, die dann zusammen mit dem Hersteller an einer Lösung arbeiten. In keinem Fall sollten Informationen zu der Schwachstelle veröffentlicht werden, bevor der Patch/das Update zur Verfügung steht. Ansonsten werden ebenfalls potenzielle Angreifer über die Schwachstelle informiert und können diese bei Netzwerkzugriff ungehindert ausnutzen. Wird von einem Hersteller ein Patch/Update zu einer Schwachstelle veröffentlicht, dann ist dieses in der Regel umgehend zu installieren, da mit der Veröffentlichung auch Angreifer auf die Schwachstelle aufmerksam gemacht werden und in der Folgezeit mit Versuchen zur Ausnutzung der Schwachstelle zu rechnen ist. Insbesondere bei isolierten Systemen sind dabei jedoch Kosten und Nutzen abzuwägen, da ein Zugriff auf das System, zwecks Installation des Patches/Updates, Angreifern auch immer eine potenzielle Zugriffsmöglichkeit liefert (siehe Abschnitt 2.4). Entsprechende Patches bzw. Updates sollten nur von vertrauenswürdigen Quellen bezogen werden. Viele Angreifergruppierungen untersuchen aber auch Softwareprodukte gezielt, um eine mögliche Schwachstelle ausfindig zu machen und nutzen zu können. In diesem Fall erfolgen Cyberangriffe unter Verwendung der Schwachstelle, bevor diese öffentlich bekannt wurde und man spricht von einer Zero-Day-Schwachstelle. Allgemein handelt es sich bei Schwachstellen um eines der am häufigsten genutzten Einfallstore über ungepatchte Systeme in IT-Netzwerke und ICS.

Nachfolgend werden einige ausgewählte bekannt gewordene Schwachstellen in ICS beschrieben:

- Verschiedene Schwachstellen betreffen ICS-Komponenten und -Systeme von Siemens. Zwei Schwachstellen gefährden beispielsweise Siemens SIPROTEC 4-Schutzrelais. Diese Geräte werden häufig in Umspannwerken eingesetzt (siehe Abschnitt A.4.8 im Anhang). Über die DIGSI4- und EN100-Ethernet-Kommunikationsmodule können unter Ausnutzung der Schwachstellen Autorisierungspasswörter rekonstruiert oder überschrieben werden. Siemens berichtete erstmals am 08.03.2018 in seinem Sicherheits-Advisory SSA-203306 über die Schwachstellen, welches am 13.07.2021 zuletzt aktualisiert wurde. Das Unternehmen hat zudem entsprechende Firmware-Updates veröffentlicht.

Eine weitere kritische Schwachstelle betrifft die SIMATIC S7-1200 und S7-1500 CPU-Produkte von Siemens, für die das Unternehmen am 11.10.2022 ein Security Advisory (SSA-568427: Weak Key Protection Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families) veröffentlicht hat (siehe Abschnitt A.6.5 im Anhang). Die Schwachstelle besteht durch die Verwendung eines veralteten kryptographischen Schlüssels, der zum Schutz von vertraulichen Konfigurationsdaten und älteren Kommunikationsverbindungen eingesetzt wird. Bei erfolgreicher Ausnutzung der Schwachstelle könnten Angreifer, die Zugriff auf ein betroffenes Gerät haben, den Schlüssel extrahieren und ihn verwenden, um an vertrauliche Konfigurationsdaten wie kryptografische Schlüssel oder Passwörter zu gelangen. Darüber hinaus können Man-in-the-Middle-Angriffe durchgeführt werden, bei denen Angreifer den Datenaustausch zwischen speicherprogrammierbaren Steuerungen (SPS) und Human-Machine-Interfaces/Engineering-Stations lesen, modifizieren oder blockieren können. Eine Ausnutzung der Schwachstelle erfordert somit eine geringe Angriffskomplexität bei hohem Schadenspotential. Siemens hat ein Update veröffentlicht, das die Schwachstelle beseitigt. Die SIMATIC S7-1200 und S7-1500 CPU-Produkte sind u. a. von zwei zusätzlichen Schwachstellen betroffen (siehe Abschnitt A.2.2 im Anhang). Eine ermöglicht den Zugriff auf das System und das unerkannte Platzieren eigener Software. Die andere bietet die Möglichkeit, dass der angezeigte Code und der tatsächlich ausgeführte Code nicht identisch sind. Siemens veröffentlichte entsprechende Sicherheitshinweise und bietet Softwareupdates zur Behebung der Schwachstellen an. Im Dezember 2019 wurden zahlreiche Schwachstellen im Leittechniksystem SPPA-T3000 von Siemens entdeckt (siehe Abschnitt A.2.1 im Anhang). Bei SPPA-T3000 handelt es sich um ein weltweit eingesetztes Distributed Control System (DCS), welches insbesondere in konventionellen Kraftwerken und Turbinensteuerungssystemen eingesetzt wird, wobei SPPA-T3000 keine Sicherheitsleittechnik direkt integriert unterstützt. Die Schwachstellen sind als äußerst schwerwiegend eingeschätzt worden und ermöglichen Angreifern umfassende Kontrollübernahme über das betroffene Leittechniksystem. Ende 2019 veröffentlichte Siemens einen CERT-Report zu den bekannt gewordenen Schwachstellen, verfügbaren Updates und Mitigationsmöglichkeiten. Im Februar 2020 veröffentlichte Siemens IT-Sicherheitshinweise zu Schwachstellen in der Profinet-Kommunikation und generelle in der Ethernet-Kommunikation von Siemens Leittechniksystemen (siehe Abschnitt A.3.1 im Anhang). Bei Profinet handelt es sich um einen für die in der Leittechnik notwendige Echtzeitkommunikation entwickelten Kommunikationsstandard, welcher auf der Ethernet-Technik basiert.

Bei Netzwerkzugriff auf die Kommunikation mittels Profinet bzw. auf die generelle Ethernetkommunikation können Angreifer unter Ausnutzung der Schwachstellen ohne Authentifizierung spezielle Nachrichten an die mit Profinet bzw. Ethernet kommunizierenden Leittechniksysteme versenden, wodurch es bei den betroffenen Leittechniksystemen zu einem Denial-of-Service Zustand kommt, sodass die leittechnischen Funktionen der Systeme nicht mehr ausgeführt werden.

- Im März 2020 veröffentlichte das Unternehmen ABB, ein international tätiger Hersteller für Leittechnik- und Sicherheitsleittechniklösungen, mehrere IT-Sicherheitshinweise zu teilweise schwerwiegenden bekanntgewordenen Schwachstellen im Leittechniksystem ABB 800xA (siehe Abschnitt A.3.2 im Anhang). Mit ABB 800xA ist ein weltweit eingesetztes DCS mit Sicherheitsleittechnikunterstützung von Schwachstellen betroffen, die potenziell Angreifern die Möglichkeit bieten, die Integrität und Verfügbarkeit des gesamten Systems zu beeinflussen. Das 800xA-System von ABB wird in einer Vielzahl von Industrie- und Kraftwerksanlagen in Deutschland und Europa verwendet.

- Zwei Schwachstellen betreffen die M1-Hardware-Controller von Bachmann (siehe Abschnitt A.4.3 im Anhang). Diese werden in den Bereichen erneuerbare Energien (z. B. Windkraft, Energieverteilung) und Automatisierung (Maschinenbau und Anlagenbau) eingesetzt. Über eine Schwachstelle kann ein nicht authentifizierter Angreifer per Fernzugriff die Hashwerte der Passwörter auslesen und entschlüsseln. Die andere Schwachstelle ermöglicht Denial-of-Service-Angriffe, wodurch der Controller zum Absturz gebracht wird. Die Schwachstellen werden mit dem am 11.01.2021 veröffentlichen Patch M-Base V4.49-P1 bzw. dem am 18.01.2021 veröffentlichten Patch M-Base V3.95R-P8 behoben.

- Im Jahr 2021 wurde bekannt, dass das industrielle Energiemanagementsystem (EMS) DIAEnergie des Herstellers Delta Electronics etwa 30 Sicherheitslücken aufweist (siehe Abschnitt A.4.10 im Anhang). DIAEnergie ermöglicht Unternehmen unter anderem die Visualisierung von elektrischen und energetischen Systemen sowie die Überwachung und Steuerung durch manuelle und automatisierte Systeme. Die sich aus den Sicherheitslücken ergebenden Angriffsmöglichkeiten umfassen das Abfangen von Passwörtern im Klartext, das Hinzufügen neuer Benutzer mit Administrator-Rechten und das Ausführen beliebigen Codes auf Basis von SQL-Injections bzw. Dateiupload-Möglichkeiten. Eine Ausnutzung der Schwachstellen erfordert keine Authentifizierung und ermöglicht es einem Angreifer unter Umständen die

vollständige Kontrolle über DIAEnergie und die Systeme zu übernehmen. Mittlerweile konnten mit Hilfe von Softwareupdates einige Sicherheitslücken behoben werden.

- Zwei schwerwiegende Schwachstellen betreffen Bibliotheken der Programmiersprache Java, die auf Milliarden von IT-Systemen installiert ist. Dazu gehören neben Bürosystemen auch insbesondere Linux-basierte Industrielle PCs (IPCs), Internet of Things (IoT/IIoT) Anwendungen und leittechnische Systeme. Am 09. Dezember 2021 wurden auf der Code-Sharing Plattform GitHub Informationen zur Schwachstelle Log4Shell für die Java Logging-Bibliothek Log4j veröffentlicht (siehe Abschnitt A.4.12 im Anhang). Da die Programmiersprache Java keine eigenen Logging-Funktionen besitzt und Log4j sich in der Vergangenheit als die zentrale Logging-Bibliothek für Java etablierte, besitzt Log4j eine sehr hohe Verbreitung bei Java-basierten Softwaren sowie Systemen. Log4j ermöglicht die Einbeziehung von Java-Variablen. Durch die Schwachstelle Log4Shell kann diese Einbeziehung praktisch unbegrenzt und ohne Rechteabfrage genutzt werden, sodass auch externe Java-Bibliotheken über Log4j aufgerufen werden können. In diesen Bibliotheken kann sogenannter Shell-Code integriert werden, welcher dann zur Ausführung beliebigen Codes auf dem betroffenen System führen kann, woher der Name der Schwachstelle Log4Shell stammt. Betroffen sind die Log4j Versionen 2.0 bis 2.14 mit Ausnahme der Version 2.12.2. Mit dem Update auf Log4j 2.15 wurde am 06. Dezember 2021 die Möglichkeit zur Deaktivierung der der Schwachstelle Log4Shell zugrunde liegenden Befehlsreihen etabliert. Die Schwachstelle wurde bereits bei Cyberangriffen ausgenutzt (siehe Abschnitt B.14.35 im Anhang). Die ersten Angriffe über die Schwachstelle begannen ab dem 01. Dezember 2021. Am 31. März 2022 wurde durch VMware die kritische Schwachstelle SpringShell (aufgrund der Analogie zu Log4Shell häufig auch Spring4Shell genannt) in den Java Bibliotheken Spring MVC und Spring WebFlux öffentlich gemacht (siehe Abschnitt A.5.3 im Anhang). Die Schwachstelle betrifft analog zu Log4Shell eine weit verbreitete Bibliothek der Programmiersprache Java. Das Spring Framework ist eine umfassende unterstützende Bibliothek, um grundlegende programmiertechnische Infrastruktur in Java-Applikationen zu integrieren, wodurch Java-Programmierer Zeit und Aufwand im Rahmen der Programmierung sparen können. Von SpringShell betroffen sind die Spring-Versionen 5.3.0 bis 5.3.17, 5.2.0 bis 5.2.19 sowie ältere Versionen. Unter bestimmten Umständen kann SpringShell auf betroffenen Systemen insoweit ausgenutzt werden, dass beliebiger Code in Form von Shellcode ausgeführt werden kann und damit Vertraulichkeit, Verfügbarkeit und Integrität der Systeme beeinflusst werden kann.

Mit den Spring Versionen 5.3.18 sowie 5.2.20 stehen seit dem 31. März 2022 aktualisierte Versionen von Spring zur Verfügung, in denen die Schwachstelle behoben wurde. Bisher sind keine umfassenden Angriffsserien auf Java Systeme mit Spring Bibliothek bekannt geworden.

- Im Januar 2022 informierte Schneider Electric seine Kunden über vier Schwachstellen mit potenziell hohem Bedrohungsgrad in seinen Mittelspannungsschutzrelais Easergy P3 und P5, die in Kraftwerken und im elektrischen Stromnetz eingesetzt werden (siehe Abschnitt A.5.4 im Anhang). Erhalten Angreifer Zugriff auf den fest codierten SSH-Schlüssel eines betroffenen Geräts, können sie auf das mit dem Gerät verbundene ICS-Netzwerk zugreifen und unter Ausnutzung der Schwachstellen dessen Datenverkehr beobachten sowie Schadsoftware in das Netzwerk laden. Es existieren Firmwareupdates, mit denen die Schwachstellen behoben werden. Um das geeignete Firmwareupdate zu erhalten, ist eine Anfrage bei Schneider Electric erforderlich.

- Cyberangriffe können auf Geräte für die unterbrechungsfreie Stromversorgung (Uninterruptible Power Supply UPS) abzielen, welche zwecks Energieüberwachung und routinemäßiger Wartung mit dem Internet verbunden sind. Ermöglicht wird dies durch die Ausnutzung von Schwachstellen, darunter drei Schwachstellen in smarten UPS-Geräten des Herstellers APC, die als TLStorm bezeichnet werden (siehe Abschnitt A.5.9 im Anhang). APC ist ein Tochterunternehmen von Schneider Electric. UPS-Geräte werden auch in kritischen Infrastrukturen eingesetzt. Zwei der drei Schwachstellen können Angreifer ausnutzen, um nicht authentifizierte Netzwerkpakete an die Geräte zu senden. Angreifer können die dritte Schwachstelle ausnutzen, um eine eigens erstellte, bösartige Firmware auf den Geräten zu installieren. Dadurch hätten Angreifer die Möglichkeit sich dauerhaft auf den UPS-Geräten einzunisten und von diesen ausgehend weitere Cyberangriffe auf das Netzwerk durchzuführen, auch um Daten zu stehlen. Schneider Electric hat seine Kunden über die Schwachstellen informiert und stellt entsprechende Patches bereit, um die Sicherheitslücken zu schließen.

- Unter dem Namen BadAlloc werden eine Serie von mehr als 25 Schwachstellen in Echtzeitbetriebssystemen und Software Development Kits (SDKs) für OT-, IoT- und IIoT-Systemen zusammengefasst (siehe Abschnitt A.4.7 im Anhang). Der Name leitet sich daraus ab, dass die Schwachstellen verschiedene Speicherfunktionen ausnutzen, welche als „Bad Allocation of Memory“ (kurz BadAlloc) bezeichnet werden. Werden die Schwachstellen ausgenutzt, können Angreifer zum einen

Denial-of-Service-Zustände bei betroffenen Geräten auslösen, zum anderen ermöglichen ein Teil der BadAlloc Schwachstellen das Ausführen beliebigen Codes durch Angreifer. Zu den betroffenen Echtzeitbetriebssystemen und SDKs gehören sowohl freie als auch kommerzielle Versionen namhafter Anbieter wie Amazon, ARM, BlackBerry, Samsung, Tencent, Texas Instruments, Windriver und viele weitere. Für die meisten betroffenen Betriebssysteme und SDKs stehen Updates bereit, welche die Schwachstellen beheben.

- Über acht Schwachstellen in der Open Automation Software (OAS) des gleichnamigen Herstellers OAS können sich Angreifer Zugriff auf Netzwerke verschaffen und beliebigen Code ausführen (siehe Abschnitt A.5.11 im Anhang). Die Schwachstelle CVE-2022-26082 ist besonders schwerwiegend, da sie einem Angreifer die Ausführung von beliebigem Programmcode auf dem kompromittierten Gerät ermöglicht. Da die Softwareplattform OAS häufig in industriellen Steuersystemen ICS Anwendung findet, werden diese durch die Schwachstellen gefährdet. Die Software ist eine universelle Lösung zur Vereinfachung der Datenkonnektivität, welche den Datentransfer und die Datenumwandlung zwischen Geräten und Anwendungen, sowohl bezogen auf Software als auch auf Hardware betrifft. Sie wird in den Bereichen Maschinelles Lernen, Data Mining, Berichterstellung und Datenvisualisierung eingesetzt und häufig in ICS verwendet, um industrielle und IoT-Geräte, SCADA-Systeme (darunter OPC Modbus SCADA-Systeme), SPS, Datenbanken, Netzwerkpunkte und APIS in einem ganzheitlichen Netzwerksystem miteinander zu verbinden. Updates zur Behebung der Schwachstellen stehen seit dem 22. Mai 2022 zur Verfügung.

- Unter der Bezeichnung OT:ICEFALL veröffentlichten Forscher im Juni 2022 einen Bericht über 56 Schwachstellen verschiedener Geräte von zehn Anbietern, die Operational Technology (OT) betreffen (siehe Abschnitt A.5.2 im Anhang). Die betroffenen Geräte von Herstellern wie Honeywell, Omron, Motorola und Siemens sind für ihren Einsatz in industriellen Anlagen, insbesondere auch in kritischen Infrastrukturen wie der Öl-, Gas-, Chemie- und Nuklearindustrie bekannt. Im Bericht wird die bisher im Bereich OT weniger ausgeprägte Sicherheitskultur thematisiert, die dazu führt, dass Geräte in diesem Bereich oftmals eine schlechte Allgemeinsicherheit bezogen auf IT- bzw. ICS-spezifische Angriffe aufweisen. Die im Bericht aufgeführten Angriffsmöglichkeiten hängen von den genauen anlagenspezifischen Umständen ab und umfassen unter anderem die Ausführung beliebigen Codes auf betroffen Geräten sowie Denial-of-Service-Angriffe, bei denen Angreifer zum Beispiel die Verfügbarkeit betroffener Geräte einschränken können.

- Im März 2023 wurden zwei kritische Schwachstellen in der Netzwerküberwachungslösung MXsecurity Series des taiwanesischen Unternehmens Moxa Inc., welche weltweit auch in kritischen Infrastrukturen eingesetzt wird, entdeckt (siehe Abschnitt A.6.2 im Anhang). Weitere fünf Schwachstellen wurden am 01.09.2023 bekannt. Über die Schwachstellen können sich Angreifer aus der Ferne Zugriff auf IT-Systeme verschaffen und dort Schadcode ausführen. Unter Umständen können Angreifer auf diese Weise Instanzen vollständig übernehmen. In einem Advisory gibt der Hersteller Moxa Inc. an, dass alle bisher entdeckten Schwachstellen in der Version 1.1.0 von MXsecurity Series beseitigt wurden.

- Das Unternehmen CODESYS Group ist der Hersteller der hardwareunabhängigen Automatisierungssoftware CODESYS. Es wurden 15 schwerwiegende Schwachstellen mit dem Bedrohungsgrad „hoch“ in einem Software Development Kit (SDK) des Herstellers mit der Bezeichnung CODESYS V3 SDK 15 entdeckt (siehe Abschnitt A.5.10 im Anhang). Mit dem SDK werden Programmable Logic Controllers (PLCs) programmiert, die vor allem in Europa in kritischen Infrastrukturen eingesetzt werden. Über die Schwachstellen können DoS-Angriffe durchgeführt und Schadcode ausgeführt werden. Sie ermöglichen es einem Angreifer Kraftwerke außer Betrieb zu nehmen und sich über eine Backdoor dauerhaft Zugriff auf Systeme zu verschaffen, um Informationen abzugreifen. Seit März 2023 ist ein Sicherheitspatch in Form der gegen die Schwachstellen abgesicherten Version V3.5.19.0 des SDK verfügbar, welches von der Webseite des Herstellers heruntergeladen werden kann. Darüber hinaus hat das Unternehmen CODESYS Group ein entsprechendes Advisory mit Informationen zu den Schwachstellen veröffentlicht.

Industrielle Steuerungssysteme geraten immer stärker in den Fokus von Angreifern. Dieser Fokus ist vielschichtig. Zum einen bieten potenzielle Produktionsausfälle und mögliche Schäden an verfahrenstechnischen Komponenten ein starkes Druckmittel im Rahmen von Ransomware-Angriffen (siehe Abschnitt 2.1). Zum anderen lassen sich mit Cyberangriffen auf industrielle Steuerungssysteme Auswirkungen in der physischen Welt erreichen. Schwachstellen in ICS spielen als möglicher Angriffsvektor daher eine Schlüsselrolle, da sie Angreifern den Zugriff auf diese Systeme erleichtern. Darüber hinaus werden die meisten schadhaften Einwirkungen auf und Manipulationen von ICS überhaupt erst durch entsprechende Schwachstellen ermöglicht.

2.6 Cyberangriffe auf den Energiesektor

Cyberangriffe auf den Energiesektor können zu Stromausfällen führen und regionale bis hin zu länderübergreifende Auswirkungen haben. In diesem Zusammenhang muss nicht der Energieversorger zwingend das eigentliche Ziel des Angriffs sein. Es genügt bereits, wenn Geräte eines Herstellers, die von einem Angriff betroffen sind, in ICS-Systemen von Energieanlagen eingesetzt werden und zusätzlich eine unzureichende Trennung zwischen Büro-Netzwerken und ICS-Systemen vorliegt. Über die Verbindungen der Büro-Netzwerke mit dem Internet eingeschleuste Schadsoftware, kann sich dann auf die ICS-Systeme ausbreiten und den Anlagenbetrieb stören und im schlimmsten Fall zum Ausfall der Anlage führen. Darüber hinaus gibt es weitere Möglichkeiten Schadsoftware in ICS-Systemen einzuschleusen, z. B. über einen Innentäter, der ein kompromittiertes Gerät über eine Schnittstelle mit dem ICS-System verbindet. Seit dem russischen Cyberangriff mit der Schadsoftware BlackEnergy3 auf das ukrainische Stromnetz im Jahr 2015 (siehe Abschnitt B.7.1 im Anhang), sind verstärkt gezielte Angriffe auf den Energiesektor zu beobachten. Vor allem mutmaßlich russischen APT-Gruppierungen hat die Ukraine dabei regelrecht als Versuchslabor gedient. Bereits ein Jahr nach dem Angriff mit BlackEnergy3 kam es im Jahr 2016 zu einem Stromausfall, nachdem ein Umspannwerk in Kiew mit der Schadsoftware Crashoverride/Industroyer angegriffen worden war (siehe Abschnitt B.8.1 im Anhang). Bei Crashoverride/Industroyer handelt es sich um die erste Schadsoftware, mit der ICS-Systeme von Umspannwerken und anderen elektrischen Einrichtungen gezielt manipuliert werden können. Darüber hinaus gibt es eine Vielzahl weiterer Cyberangriffe auf den Energiesektor, bei denen die ICS-Systeme und deren Manipulation, bis hin zu physischen Schäden, nicht im Vordergrund stehen. Im März 2019 kam es zum ersten dokumentierten Cyberangriff auf einen Betreiber von Windkraft- und Solaranlagen in den USA, der daraufhin die datentechnische Verbindung zu seinen energieerzeugenden Anlagen verlor (siehe Abschnitt B.11.7 im Anhang). Es werden vermehrt Cyberangriffe, darunter Ransomware-Angriffe (siehe Abschnitt 2.1), beobachtet, bei denen sensible Daten entwendet und unter Umständen im Darknet zum Verkauf angeboten werden. Diese Daten können dann für die Planung und Vorbereitung späterer Angriffe auf den Energiesektor genutzt werden. Als Beispiel ist hier die seit 2015 andauernde Angriffswelle der APT-Gruppierung Dragonfly (siehe Abschnitt 2.10.5) gegen Unternehmen des Energiesektors zu nennen (siehe Abschnitt B.9.3 im Anhang). Dabei sammeln die Angreifer gezielt Informationen zu industriellen Steuerungssystemen und deren Bedienung. Auch Cyberangriffe, die nicht primär auf den Energiesektor abzielen, können sich indirekt auf diesen auswirken.

Beim russischen Einmarsch in die Ukraine im Februar 2022 erfolgte ein Cyberangriff auf den Kommunikationssatelliten KA-SAT, woraufhin dieser ausfiel (siehe Abschnitt B.14.2 im Anhang). Dies hatte Auswirkungen auf Windkraftanlagen des deutschen Energieanbieters Euroskypark. Im Falle eines Fehlers war eine Entstörung aus der Ferne durch den Ausfall der Kommunikationsverbindung nicht mehr möglich.

Diese sowie weitere Cyberangriffe auf Anlagen und Einrichtungen zur Stromerzeugung und Stromübertragung werden im Folgenden kurz beschrieben:

- Am 23.12.2015 ereignete sich ein Cyberangriff der russischen APT-Gruppierung Sandworm (siehe Abschnitt 2.10.11) mit der Schadsoftware BlackEnergy3, auch als BlackEnergy Lite bezeichnet, auf das ukrainische Stromnetz (siehe Abschnitt B.7.1 im Anhang). Es wurden insgesamt drei Energieversorgungsunternehmen erfolgreich angegriffen, was zu einem mehrstündigen Stromausfall führte, von dem etwa 225.000 Kunden betroffen waren. Drei weitere Unternehmen wurden ebenfalls angegriffen, ihr Betrieb konnte aber aufrechterhalten werden. Die Schadsoftware BlackEnergy3 beinhaltet Plugins und Funktionen, die im Wesentlichen auf die Auskundschaftung von Netzwerken ausgerichtet sind, sowie zusätzlich eine KillDisk-Komponente zur Datenlöschung. Eine spätere, abgewandelte Version der Schadsoftware bietet zusätzlich die Möglichkeit, ICS-Systeme zu manipulieren. Die Angreifer erhielten über Remote-Zugänge Zugriff auf die Büro-IT und die Leittechniksysteme. Über die KillDisk-Komponente wurden anschließend für den Betrieb erforderliche Daten gelöscht. Darüber hinaus wurde die unterbrechungsfreie Stromversorgung für die Server angegriffen. Es wird davon ausgegangen, dass BlackEnergy3 bei dem Angriff hauptsächlich eine unterstützende Rolle spielte, um Zugriff auf die IT-Netzwerke der Anlagen zu erhalten.

- Ende des Jahres 2015 erfolgte ein Cyberangriff mit der Schadsoftware GreyEnergy auf ein Energieversorgungsunternehmen in Polen (siehe Abschnitt B.7.2 im Anhang). Danach fanden weitere Cyberangriffe mit der Schadsoftware gegen Ziele aus dem Bereich der kritischen Infrastrukturen in Zentral- und Osteuropa statt. Der Schwerpunkt lag dabei auf Organisationen in der Ukraine. Die Schadsoftware ist modular aufgebaut und dient im Wesentlichen dazu Netzwerke auszukundschaften und Zugangsrechte zu erhalten. Sie ist nicht in der Lage ICS-Systeme direkt zu beeinflussen. Die APT-Gruppierung, die die Schadsoftware entwickelt hat, wird ebenfalls al GreyEnergy bezeichnet.

- Ab 2015 führte die APT-Gruppierung Dragonfly (siehe Abschnitt 2.10.5) eine Angriffswelle gegen Unternehmen im Energiesektor einschließlich der kerntechnischen Industrie sowie der Öl- und Gasindustrie durch (siehe Abschnitt B.9.3 im Anhang). Die Angriffe erreichten im Jahr 2017 einen vorläufigen Höhepunkt, dauern aber nach wie vor an und konzentrieren sich auf Unternehmen in Europa, darunter auch Unternehmen in Deutschland, sowie auf Unternehmen in den USA und in einigen asiatische Ländern. Häufig greifen die Angreifer die anvisierten Ziele nicht direkt an, sondern kompromittieren zunächst geeignete Zwischenziele in der Lieferkette. Endgültig ins Zielnetzwerk eingedrungen, sammeln sie Informationen zu den industriellen Steuerungssystemen wie Konfigurations- und Zugriffsinformationen sowie Informationen zu deren Bedienung einschließlich der Erfassung von Screenshots während des Betriebs. Mindestens ein Angriff erfolgte auf eine kerntechnische Anlage, das US-amerikanische Kernkraftwerk Woolf Creek. In einer ersten Reaktion gab die Anlage an, die möglichen Auswirkungen des Angriffs seien auf die administrativen und geschäftlichen Teile des Anlagennetzwerks beschränkt, die Untersuchungen seien aber noch nicht abgeschlossen.

- Am 17.12.2016 führte die russische APT-Gruppierung ELECTRUM (siehe Abschnitt 2.10.6), welche in direkter Verbindung zur Gruppierung Sandworm steht, einen weiteren Angriff auf das ukrainische Stromnetz aus (siehe Abschnitt B.8.1 im Anhang). Von dem Cyberangriff war ein Umspannwerk in Kiew betroffen, was zu einem Stromausfall führte, der über eine Stunde andauerte. Die Angreifer setzten dabei die Schadsoftware Crashoverride, auch Industroyer genannt, ein. Sie bietet die Möglichkeit die ICS-Systeme von Umspannwerken und anderen elektrischen Einrichtungen direkt zu manipulieren und Schalter zu kontrollieren. Die Schadsoftware Crashoverride/Industroyer ist modular aufgebaut und kann durch zusätzliche Module erweitert werden, so dass weitere Angriffsmöglichkeiten denkbar sind. Bei dem genannten Angriff wurden die Handlungsoptionen, die die Schadsoftware bietet, nicht voll ausgeschöpft. Daher handelte es sich bei diesem Vorfall vermutlich um einen Test der Schadsoftware. Hierfür spricht auch, dass der Angriff nach etwa einer Stunde von Angreiferseite beendet wurde.

- In der ersten Hälfte des Jahres 2019 wurde die Wiper-Schadsoftware ZeroCleare bei mehreren Angriffen auf den Energiesektor im Mittleren Osten eingesetzt (siehe Abschnitt B.11.4 im Anhang). IT-Sicherheitsanalysten von IBM Security haben die Schadsoftware entdeckt. Der Wiper versucht auf den infizierten Systemen so viele Daten wie möglich zu löschen.

Für Windows-basierte Systeme bedeutet das, dass ZeroCleare versucht den Master Boot Record (MBR) zu überschreiben und Partitionen zu beschädigen. Nach eingehender Untersuchung der Schadsoftware äußert IBM die Vermutung, dass die Angriffe von iranischen, staatlich geförderten Angreifern durchgeführt wurden. Die Rede ist hierbei von APT34, auch OilRig genannt, sowie von mindestens einer weiteren Gruppierung.

- Im März 2019 kam es zum ersten dokumentierten Fall eines Cyberangriffs auf einen Erzeuger erneuerbarer Energien in den USA (siehe Abschnitt B.11.7 im Anhang). Bei diesem Cyberangriff verlor der betroffene Energieversorger die datentechnische Verbindung zu seinen energieerzeugenden Windkraft- und Solaranlagen. Der Betreiber sPower wurde hierbei Opfer eines Cyberangriffes auf Firewalls des Herstellers Cisco. Der Angriff erfolgte über eine bekannte Schwachstelle in der Software der Cisco Firewalls. Die zugehörige Hardware der Firewall wurde durch den Vorfall überlastet, sodass der Netzwerkverkehr von sPower zu seinen Anlagen nicht mehr weitergeleitet wurde. Hierbei handelte es sich nach bisherigen Berichten nicht um einen zielgenauen Cyberangriff auf den Energieerzeuger, sondern um Flächenangriffe. Es kam zu keinen Folgeangriffen auf die technische Infrastruktur von sPower.

- Am 13. Oktober 2020 kam es in Mumbai zu einem Stromausfall, von dem 20 Millionen Menschen betroffen waren (siehe Abschnitt B.12.3 im Anhang). Vermutlich war der Stromausfall die Folge eines Cyberangriffs einer mutmaßlich chinesischen Angreifergruppierung auf ein nahe gelegenes Stromlastmanagementzentrum. Dem Ereignis waren politische Spannungen zwischen Indien und China vorrausgegangen. Bis heute ist nicht vollständig klar, ob es sich bei dem Stromausfall um einen Cyberangriff oder um technisches bzw. menschliches Versagen gehandelt hat. Analysten gehen von einem Cyberangriff aus, was von offizieller, indischer Seite aber bestritten wird.

- Im Februar 2021 kam es zu einem IT-Sicherheitsvorfall im brasilianischen Kernkraftwerk Angra (siehe Abschnitt B.13.2 im Anhang). Dabei wurde von den Angreifern die Ransomware Darkside eingesetzt. Neben dem Kernkraftwerk wurden auch dessen Betreiber Eletrobras und der Energiekonzern Copel mit der Schadsoftware angegriffen und Informationen von Copel wurden entwendet. Der IT-Sicherheitsvorfall hatte keinen Einfluss auf den Betrieb des Kernkraftwerks.

- Ab Februar 2022 kam es unter Ausnutzung der Schwachstelle Log4Shell in der Software VMWare Horizon zu Cyberangriffen durch die nordkoreanische

APT-Gruppierung APT 38 (siehe Abschnitt 2.10.3), auch Lazarus genannt, auf Energieunternehmen in den USA, Kanada und Japan (siehe Abschnitt B.14.35 im Anhang). Über die Schwachstelle erlangten die Angreifer Zugriff auf über das Internet erreichbare Server und über diese auch auf die Daten und Netzwerke der betroffenen Energieunternehmen. Sie nutzten drei unterschiedliche Schadsoftwaren für den Aufbau eines langfristigen Zugriffs und das Auslesen von Zugangsdaten und weiteren für die Angreifer relevanten Datensätzen. Das langfristige Ziel der Angriffe scheinen insbesondere das Auslesen von Zugriffsdaten, die Etablierung innerhalb des Netzwerks der angegriffenen Unternehmen und der allgemeine Abfluss von Daten gewesen zu sein.

- Am 24.02.2022 begann Russland mit der Invasion der Ukraine (siehe Abschnitt 2.8 sowie Abschnitt B.14.5 im Anhang). Parallel zu den physischen Kampfhandlungen wurden auch Cyberangriffe gegen die Ukraine durchgeführt. Am 08.04.2022 sollten offenbar durch den Einsatz der Schadsoftware Industroyer2 industrielle Steuerungssysteme in Hochspannungsumspannwerken sabotiert und so ein Blackout hervorgerufen werden, von dem etwa zwei Millionen Menschen betroffen gewesen wären. Der Angriff, der der APT-Gruppierung Sandworm (siehe Abschnitt 2.10.11) zugeschrieben wird, wurde jedoch rechtzeitig erkannt und ein Stromausfall konnte verhindert werden. Die Schadsoftware Industroyer2 basiert auf der Schadsoftware Industroyer bzw. Crashoverride, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert.

- Bei KA-SAT (KASAT Viasat) handelt es sich um einen Kommunikationssatelliten der US-amerikanischen Firma Viasat. Mit 82 Spotbeams erreicht er eine europaweite Abdeckung. Am Donnerstag, den 24.02.2022, um 4 Uhr UTC morgens (entspricht 6 Uhr ukrainischer Zeit) kam es in Folge eines Cyberangriffs mit der Wiper-Schadsoftware AcidRain zu einem Ausfall der Kommunikation über den KA-SAT-Satelliten (siehe Abschnitt B.14.2 im Anhang). Dieser erfolgte nahezu zeitgleich mit dem Angriff durch russische Streitkräfte auf die Ukraine. Hierbei wird ein Zusammenhang vermutet. Beweise hierzu liegen bisher allerdings nicht vor. Der Ausfall des Satelliten hatte auch Auswirkungen auf Windkraftanlagen des deutschen Energieanbieters Enercon. Zwar laufen die Anlagen autark weiter und ihre Steuerung ist weiterhin gewährleistet, aber eine Entstörung im Falle eines Fehlers ist aus der Ferne bei einem Ausfall der KA-SAT-Verbindung nicht möglich.

- Um den Schutz kritischer Infrastrukturen in den USA zu verbessern, hat das FBI im Jahr 1996 das InfraGard-Programm ins Leben gerufen. Angreifer, die sich selbst als

„USDoD“ bezeichnen und das Siegel des U.S. Department of Defense verwenden, haben sich im InfraGard-Programm angemeldet und konnten die Datenbank wichtiger Schlüsselpersonen aus dem Bereich kritischer Infrastrukturen kopieren (siehe Abschnitt B.14.33 im Anhang). Die Datenbank dient dazu die Schlüsselpersonen zu vernetzen. Die Angreifer haben die abgegriffenen Daten seit dem 10.12.2022 in einem Darknet-Forum zum Verkauf angeboten. Offenbar betrifft der Datendiebstahl die Informationen von mehreren zehntausend Menschen, zu denen auch Mitarbeiter von Energieversorgern und Kernenergieunternehmen gehören.

Darüber hinaus erfolgten Cyberangriffe mit Ransomware (siehe Abschnitt 2.1) auf den Energiesektor, die das Ziel hatten sensible Daten zu stehlen und/oder zu verschlüsseln, um anschließend eine Lösegeldforderung für die Nicht-Veröffentlichung und/oder die Entschlüsselung der Daten zu stellen. Am 19.11.2021 wurde ein Cyberangriff auf Vestas Wind Systems A/S, einem der weltweit größten Hersteller von Windenergieanlagen mit Hauptsitz in Dänemark, entdeckt (siehe Abschnitt B.13.17 im Anhang) und am 31.03.2022 wurde festgestellt, dass es zu einem Cyberangriff auf Nordex, einem der weltweit größten Hersteller und Service Provider von Windenergieanlagen mit Niederlassungen in mehr als 30 Ländern und Hauptsitz in Deutschland, gekommen ist (siehe Abschnitt B.14.17 im Anhang). Die APT-Gruppierung Black Basta führte am 11.04.2022 einen Cyberangriff auf die Deutsche Windtechnik durch (siehe Abschnitt B.14.18 im Anhang). Am 22. Juli 2022 erfolgte ein Cyberangriff der APT-Gruppierung BlackCat auf den luxemburgischen Netzbetreiber Creos und den luxemburgischen Energieversorger Enovos, die beide zur Encevo-Gruppierung gehören und eine Gaspipeline sowie die Stromversorgung in Luxemburg betreiben (siehe Abschnitt B.14.19 im Anhang). Am 19.08.2022 erfolgte ein Cyberangriff der APT-Gruppierung Ragnar Locker auf den griechischen Gasnetzbetreiber Desfa (siehe Abschnitt B.14.29 im Anhang). In allen Fällen waren die ICS-Systeme von den Angriffen nicht betroffen, da diese in der Regel vom Büro- IT-Netzwerk isoliert sind und nur letzteres eine Verbindung zum Internet besitzt. Aber da von den Unternehmen kein Lösegeld gezahlt wurde, wurden die gestohlenen sensiblen Daten veröffentlicht. Diese umfassen unter anderem personenbezogene Daten von Mitarbeitern (z. B. Ausweiskopien, E-Mails, Daten zu Bankkonten) und Vertragsdaten.

Cyberangriffe auf den Energie-Sektor stellen eine wachsende Bedrohung dar. Der Einsatz von speziell ausgelegter Schadsoftware wie Crashoverride/Industroyer zeigt, dass

eine Spezialisierung von APT-Gruppierungen auf ICS-Systeme erfolgt, die im Bereich der Energieversorgung eingesetzt werden.

Die Angreifer verfügen über das technische Verständnis, die Mittel und die Fähigkeiten, ICS-Systeme elektrischer Einrichtungen gezielt zu manipulieren. Um die Auswirkungen solcher Angriffe zu verhindern oder wenigstens zu minimieren, sind umfassende Sicherungsmaßnahmen u. a. zur rechtzeitigen Detektion eines Cyberangriffs auf die IT-Systeme in den elektrischen Einrichtungen und zur umgehenden Reaktion darauf, wie beispielsweise im Fall des Cyberangriffs mit Industroyer 2, ausschlaggebend.

2.7 Cyberangriffe mit Bezügen zu kerntechnischen Anlagen und Anlagen im Umgang mit radioaktiven Stoffen

Kerntechnische Anlagen sowie Anlagen mit radioaktiven Stoffen setzten seit über 20 Jahren auch IT-Systeme für die Durchführung ihrer betrieblichen Aufgaben ein. Weiterhin werden auch sicherungstechnisch relevante Systeme wie Einbruchmeldesysteme, Kameras und Zugangskontrollsysteme rechnerbasiert oder programmierbar ausgeführt, wodurch in den Anlagen eine Vielzahl potenzieller Ziele für Cyberangriffe besteht. Bereits vor dem Stuxnet Angriff wurden daher innerhalb und außerhalb Deutschlands IT-Sicherungsmaßnahmen in kerntechnischen Anlagen eingeführt. Diese Maßnahmen wurden nach Stuxnet intensiviert, sodass in Deutschland 2013 die „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter“ (SEWD-Richtlinie IT) /BMU13n01/ erlassen wurde. Später folgten entsprechende Richtlinien für kerntechnische Anlagen und Einrichtungen der Sicherungskategorie III und für den Umgang mit sonstigen radioaktiven Stoffen.

Kerntechnische Anlagen und Anlagen mit radioaktiven Stoffen sind aus gleich mehreren Perspektiven für Angreifende interessant. So sind Informationen über diese Anlagen und die darin eingesetzten verfahrenstechnischen Systeme und IT-Systeme sowie die Daten, die in diesen Anlagen erfasst, verarbeitet und ausgegeben werden, zum einen für Angreifergruppierungen, die staatlich beauftragt oder gefördert werden, im Rahmen der Spionage oder der potenziellen weiteren Angriffsvorbereitung direkt von Interesse. Ähnliches gilt auch für andere Gruppierungen, nicht zuletzt für politische Zwecke, wobei in diesen Fällen insbesondere die Aufmerksamkeitswirksamkeit der entsprechenden schadhaften Handlungen Ziel politisch motivierter Gruppierungen ist.

Diese Aufmerksamkeit ist aufgrund der großen ökonomischen und sicherheitstechnischen Bedeutung aber auch der politischen Diskussionslage bei kerntechnischen Einrichtungen deutlich höher als bei konventionellen Anlagen.

Im Rahmen der Analyse der Bedrohungslage wurden dabei insbesondere Cyberangriffe auf die verwaltenden IT-Systeme von kerntechnischen und radiologischen Anlagen selbst, aber auch auf deren Zulieferer oder andere, im kerntechnischen Sektor agierenden Unternehmen verzeichnet. Weiterhin wurden Cyberangriffe auf Behörden mit kerntechnischen Bezügen bekannt.

Grundsätzlich sind direkte Cyberangriffe auf kerntechnische Anlagen selten und werden darüber hinaus auch noch seltener berichtet, da Cyberangriffe auf kerntechnische Anlagen wie auch Einrichtungen mit sonstigen radioaktiven Stoffen politische Wirkung entfalten können. Weiterhin wurden weltweit für kerntechnische Anlagen eigene nationale Regelwerke und internationale Empfehlungswerke (z. B. unter dem Dach der IAEA) geschaffen, welche über typische Regelwerke zur Cyber-Sicherheit hinausgehende Maßnahmen für kerntechnische Anlagen aber auch Anlagen im Umgang mit sonstigen radioaktiven Stoffen hinausgehen.

Zu den bekanntesten Cyberangriffen auf kerntechnische Anlagen in den letzten Jahren zählen unter anderem die folgenden Cyberangriffe:

- Mit dem indischen Kernkraftwerk Kudankulam wurde im Jahr 2019 ein direkter Cyberangriff auf ein sich im Betrieb befindliches Kernkraftwerk bekannt. Nach bisherigen Erkenntnissen wurden hierbei über mehrere Jahre Informationen zu Personen im indischen zivilen nuklearen Sektor erforscht, um dann entsprechenden Personen und Unternehmen mit Schadcode behaftete Emails zu übersenden. Die Angreifenden gaben sich dabei als Mitarbeiter der indischen Regierung aus, was schließlich zur Infektion eines zentralen Servers des administrativen Netzwerks des Kernkraftwerks Kudankulam führte. Der Angriff wurde langfristig vorbereitet, erreichte tiefgehenden Systemzugriff im administrativen Teil, aber nicht im davon getrennten leittechnischen Teil des Anlagennetzes, und ermöglichte die Entwendung einer großen Menge an Daten. Der Angriff wird der APT-Gruppierung 38/Lazarus (siehe Abschnitt 2.12.3) zugeordnet und wird in Abschnitt B.11.2 im Anhang genauer beschrieben.
- Im Kernkraftwerk Südukraine kam es zu einem Zwischenfall durch die eigenen Mitarbeiter (siehe Abschnitt B.11.1 im Anhang). Hierbei führten im August 2019

Mitarbeiter eigene IT-Systeme in den Verwaltungsbereich des Kraftwerks ein, mit dem Ziel Kryptowährungen wie Bitcoins auf diesen zu generieren. Da die hierfür notwendigen Hochleistungsgrafikkarten einen hohen Energiebedarf besitzen, wurde der Strom des Kernkraftwerks genutzt. Um Kryptowährungen zu erzeugen, ist eine permanente Internetverbindung notwendig, sodass die Mitarbeiter Teile des internen Netzwerks des Verwaltungstraktes entgegen den Vorgaben an das Internet anschlossen. Auch in den militärischen Kasernen der Nationalgarde wurde entsprechende Technik auf dem Kraftwerksgelände gefunden.

- Im Februar 2021 kam es zu einem IT-Sicherheitsvorfall im brasilianischen Kernkraftwerk Angra, bei dem die Ransomware DarkSide eingesetzt wurde (siehe Abschnitt B.13.2 im Anhang). Allerdings wurde der Anlagenbetrieb davon nicht beeinflusst. Neben Angra wurden auch der Kernkraftwerksbetreiber Eletrobras selbst und der Energiekonzern Copel angegriffen. Dabei wurden Daten von Copel entwendet.

Häufiger werden kerntechnische Anlagen Opfer von Cyberangriffen, welche sich bei Zulieferern, Behörden und anderen Organisation, welche sich in wirtschaftlichen oder regulatorischen Beziehungen zu den Anlagen befinden, ereignen. Solche Organisationen können zum einen erhebliche Daten bezüglich der kerntechnischen Anlage und deren IT-Systeme speichern, z. B. im Rahmen von Ausschreibungen, im Rahmen von behördlichen Aufsichtsverfahren oder im Rahmen von Arbeitnehmerüberlassungen. In den vergangenen Jahren kam es mehrfach zu Fällen, in denen sich Angreifer durch Cyberangriffe auf andere Unternehmen Informationen von kerntechnischen Anlagen aneigneten. Je nach Motivationslage ist es zum Teil auch zu Veröffentlichungen dieser Daten gekommen:

- Das britische Unternehmen Zaun Ltd. wurde im August 2023 Opfer eines Ransomware-Angriffes, bei welchem zwar verhindert wurde, dass Daten des Unternehmens verschlüsselt wurden, jedoch über 10 GB an Unternehmensdaten von den Angreifern extrahiert wurden. Als britischer Spezialist für Hochsicherheitsumzäunungen sind Auftraggeber der Zaun Ltd. z. B. Gefängnisse, Militärbasen aber auch kerntechnischen Anlagen. Jedoch sollen laut Aussagen der Zaun Ltd. nur solche Daten entwendet worden sein, welche sich auch auf der Unternehmenswebseite hätten aufrufen lassen, sodass die Wahrscheinlichkeit des Abflusses relevanter Daten kerntechnischer Anlagen gering erscheint. (Anhang B.15.5)

- Als beim japanischen Kernkraftwerk Fukushima Daiichi im Jahr 2023 damit begonnen wurde, gefiltertes radioaktiv belastetes Kühlwasser in den pazifischen Ozean zu leiten, begann die Hacker- und Aktivistengruppierung Anonymous mit Cyberangriffen auf Webseiten japanischer Behörden und Unternehmen mit kerntechnischen Bezügen in Form von Distributed-Denial-of-Service-Angriffen, welche mit geringem Erfolg die Erreichbarkeit der Webseiten einschränkten. Die Cyberangriffe wurden von der Gruppierung bereits 2021 für den Fall einer Kühlwassermeeresverklappung angekündigt. (Anhang B.15.32)

- Im Mai 2023 wurde bekannt, dass die in Unternehmen und Behörden beliebte Datenmanagementsoftware MoveIT Transfer von einer Zero-Day Schwachstelle betroffen ist, welche durch die CL0P Ransomware Gang ausgenutzt wurde. Eine Ransomware wurde hierbei jedoch nicht eingesetzt, sondern es wurden große Datenmengen von CL0P extrahiert und anschließend die Eigentümer der Daten für eine Löschung dieser erpresst. Dies kumulierte in der Veröffentlichung großer Datenmengen im August 2023. Betroffen war nach Medienberichten das amerikanische Versuchsendlager des Department of Energy DoE Waste Isolation Pilot Plant in New Mexiko. (Anhang B.15.35)

- Sogin ist ein staatliches Unternehmen Italiens und ist für die Abwicklung des Rückbaus italienischer kerntechnischer Anlagen sowie die Entsorgung sonstiger radioaktiver Stoffe verantwortlich. Durch einen nicht näher dargestellten Cyberangriff wurden Ende 2020 umfassende Datensätze mit Informationen zu den Mitarbeitern, Passwörtern im Klartext, technischen Zeichnungen, Software- und Hardware-Updates, weitere betriebliche Informationen sowie auch private Informationen gestohlen und im Darknet zum Verkauf angeboten. Es besteht aufgrund des Vorhandenseins privater Informationen unter den angebotenen Daten die Vermutung, dass durch eine private Nutzung von IT-Systemen eine Angriffsoberfläche für den Angriff auf Sogin entstanden ist. (Anhang B.13.19)

- Ingérop ist ein französischer Baudienstleister, welcher unter anderem an verschiedenen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo beteiligt ist. Im November 2018 wurde bekannt, dass mehr als 11.000 gestohlene Datensätze des Unternehmens zum Verkauf angeboten wurden. Die Daten entstammen einem Phishing-Angriff mit unbekannter Schadsoftware. Die Daten betrafen neben Cigéo auch das Kernkraftwerk Fessenheim am Rhein. (Anhang B.10.2)

Weiterhin werden jedes Jahr mehr als 30.000 Schwachstellen von informationstechnischen Systemen öffentlich bekannt. Immer wieder sind hierbei auch solche Systeme betroffen, welche in IT- und OT-Anwendungen kerntechnischer Anlagen und Anlagen im Umgang mit sonstigen radioaktiven Stoffen vorkommen. Darüber hinaus sind vielfach weitere Gefahrenpotentiale gegeben, weil Systeme ähnlicher Funktion oder ähnlichen Typs in kerntechnischen Anlagen eingesetzt werden, ohne dass deren Nutzung bestätigt wurde. In den letzten Jahren sind z. B. die folgenden Schwachstellen bekannt geworden:

- Kritische Schwachstellen in SIMATIC S7-1200 und S7-1500 CPU-Systemen (Anhang A.6.6
- Kritische Schwachstellen in Codesys (Anhang A.5.10)
- Log4Shell und Spring4Shell (Anhang A.4.12 und Anhang A.5.3)
- ABB 800xA – Schwachstellen in ICS (Anhang A.3.2)

Kerntechnische Anlagen und Anlagen im Umgang mit sonstigen radioaktiven Stoffen waren in den vergangenen Jahren mehrfach Ziel von Cyberangriffen unterschiedlicher Motivation. Beispielsweise sind bekanntgewordene Einwirkungen auf kerntechnische bzw. radiologische Anlagen auf staatlich gestützte Spionage oder Schadwirkung im Rahmen von Konflikten, politischen Aktivismus sowie persönliche oder finanzielle Motive zurückzuführen. Die gleichzeitig bestehende hohe potenzielle Schadwirkung von tiefgreifenden Angriffen und das hohe Aufmerksamkeitspotenzial von solchen Angriffen lassen vor allem aufgrund der aktuell verschärften IT-Bedrohungslage für kritische Infrastrukturen annehmen, dass es auch in der Zukunft zu Cyberangriffen auf solche Anlagen und Systeme kommen wird.

2.8 Cyberangriffe in Zusammenhang mit dem Krieg in der Ukraine

Im Zusammenhang mit dem Krieg in der Ukraine ist es bislang zu zahlreichen Cyberangriffen gekommen. Dies schließt sowohl Cyberangriffe im Rahmen des seit Jahren schwelenden Konflikts seit spätestens 2014, kriegsvorbereitende Cyberangriffe seit spätestens 2021 und kriegsbegleitende Cyberangriffe seit Ende Februar 2022 mit ein.

Schon seit Jahren kommt es mutmaßlich von russischer Seite zu Cyberangriffen auf ukrainische Ziele. Mehrfach wurde beispielsweise die Energieversorgung über Cyberangriffe auf industrielle Steuerungssysteme in Umspannwerken angegriffen:

- So kam es bereits in den Jahren 2015 und 2016 zu gezielten Cyberangriffen auf das ukrainische Stromnetz. Im Dezember 2015 wurden mehrere ukrainische Energieversorgungsunternehmen unter Einsatz der Schadsoftware Black Energy 3 (siehe Abschnitt B.7.1) im Anhang) angegriffen. Einige der angegriffenen Unternehmen konnten den Betrieb aufrechterhalten, dennoch waren die physischen Auswirkungen so groß, dass es zu einem mehrstündigen Stromausfall für ca. 225.000 Kunden kam.
- Im Dezember 2016 wurde unter Einsatz der Schadsoftware Crashoverride/Industroyer (siehe Abschnitt B.8.1 im Anhang) ein Umspannwerk in Kiew angegriffen, wodurch es zu einem einstündigen Stromausfall im Großraum Kiew kam. Während beide Cyberangriffe von ihrem Effekt her der Demonstration von Fähigkeiten und dem Aufbau einer Drohkulisse zugeordnet werden können, erfüllte der Cyberangriff im Jahr 2016 offenbar noch einen weiteren Zweck. So wurde dieser Angriff nach etwa einer Stunde von den Angreifern selbst beendet, was stark für einen Testcharakter des Angriffs spricht.

In dem Jahr vor Beginn der Kriegshandlungen wurde ein Anstieg der Cyberangriffe festgestellt. So wurden ab März 2021 von ukrainischen Stellen zahlreiche Cyberangriffe registriert. Dabei handelte es sich häufig um Angriffe zu Spionagezwecken, insbesondere im Hinblick auf militärische Aufklärung. Beispielsweise wurde eine breit angelegte Phishing-Kampagne auf E-Mail-Konten der ukrainischen Armee durchgeführt. Ab Mitte 2021 kam es zusätzlich zur Etablierung von persistentem Zugriff auf für die Ukraine und die NATO wichtige Lieferketten. Weiter wurde Informationsdiebstahl bei außenpolitischen Einrichtungen festgestellt. Diese Aktivitäten beschränkten sich nicht auf die Ukraine, sondern wurden in vielen NATO-Mitgliedsstaaten beobachtet. In der zweiten Jahreshälfte 2021 wurden diese Aktivitäten durch Überwachung und Ausspähung von Organisationen ergänzt, die im Kriegsfall möglicherweise militärische, diplomatische oder humanitäre Unterstützung bereitstellen bzw. organisieren könnten. Ende 2021 waren vermehrt Cyberangriffe festzustellen, die auf die Etablierung von persistentem Zugriff und die strategisch günstige Positionierung in den Sektoren Energie und IT abzielten. Ab Anfang 2022 kam es über diese vorbereitenden Cyberangriffe hinaus auch zu Cyberangriffen mit Wipern und anderen destruktiven Schadsoftwarekomponenten auf ukrainische Regierungseinrichtungen und Einrichtungen im IT-, Energie- und Finanzsektor. Zusätzlich wurden auch DDoS-Angriffe in diesen Bereichen durchgeführt:

- Besonders hervorzuheben ist hierbei die Schadsoftware WhisperGate (siehe Abschnitt B.14.1 im Anhang), den Berichten /REC22w02/ zufolge vornehmlich gegen

Ziele in der Ukraine – darunter Regierungseinrichtungen, Non-profit-Organisationen und IT-Organisationen – eingesetzt wurde. Dabei handelt es sich um einen Wiper, der unter dem Deckmantel eines Ransomware-Angriffs den Master Boot Record des angegriffenen Systems zerstört.

Mit Kriegsbeginn hat sich die Situation weiter verschärft:

- Direkt mit Kriegsbeginn, nahezu zeitgleich mit dem Beginn des Angriffs russischer Streitkräfte auf die Ukraine, am Morgen des 24. Februar 2022, erfuhr die Kommunikation über den Kommunikationssatelliten KA-SAT eine Unterbrechung, welche einen teilweisen Ausfall der Dienste des KA-SAT Satellitennetzwerks über Europa nach sich zog. Über KA-SAT wurde zu diesem Zeitpunkt auch die Satellitenkommunikation für die ukrainische Polizei und das ukrainische Militär bereitgestellt, deren Störung das eigentliche Ziel des Cyberangriffs gewesen sein dürfte.

Seit Kriegsbeginn kam es zu einem weiteren Anstieg der Cyberangriffe in der Ukraine und bei westlichen Partnern. Dabei war auch immer wieder die elektrische Energieversorgung ein Angriffsziel:

- Unter anderem gab es einen versuchten Cyberangriff auf die ukrainische Stromversorgung mit der Schadsoftware Industroyer 2 in der ersten Aprilhälfte 2022, der ukrainischen Angaben zufolge rechtzeitig erkannt und vereitelt wurde (siehe hierzu Abschnitt B.14.5 im Anhang).

- Im Oktober 2022 wurden parallel zu den mit Raketenangriffen ausgeführten physischen Angriffen auf die Energieversorgung in weiten Teilen der Ukraine auch Cyberangriffe zu diesem Zweck erfolgreich ausgeführt. Diese offenbar von der russischen APT-Gruppierung Sandworm ausgeführten Angriffe wurden erst im November 2023 bekannt. Welche Ziele dabei genau angegriffen wurden, ist den bislang verfügbaren Informationen nicht zu entnehmen. Deutlich wird aus den vorliegenden Informationen allerdings, dass die Cyberangriffe zu den massiven Einschränkungen bei der Stromversorgung der Ukraine im Oktober 2022 beigetragen haben (siehe hierzu Abschnitt B.15.36 im Anhang).

Neben Cyberangriffen durch mutmaßlich von staatlichen russischen Stellen unterstützte Angreifergruppierungen ist seit Beginn des Krieges auch die Entfaltung zahlreicher weiterer, kriegsbegleitender Cyberangriffe festzustellen.

Dies gilt sowohl in Bezug auf Angreifer, welche mit ihren Aktivitäten die ukrainische Seite unterstützen wollen, als auch in Bezug auf Angreifer, die ihre Unterstützung für die russische Seite erklärt haben.

Bereits vor Ausbruch der physischen Kriegshandlungen, aber verstärkt seit dem russischen Angriff auf die Ukraine ist nicht nur die Ukraine das Ziel von Cyberangriffen von russischen Angreifergruppierungen, sondern vermehrt auch Länder die sich unterstützend gegenüber der Ukraine zeigen oder sich gegen den russischen Angriffskrieg aussprechen. Beispielsweise wurden nahezu alle Mitgliedsstaaten der NATO seit 2022 Opfer von Cyberangriffen, die in Zusammenhang mit dem Angriff auf die Ukraine stehen. Zudem ist zu erwähnen, dass auch weltweite Partner-Länder der NATO, Ziel solcher Cyberangriffe waren. Die beobachteten Cyberangriffe werden von verschiedenen Angreifergruppierungen wie beispielsweise Killnet oder NoName057 durchgeführt.

In den Jahren 2022 und 2023 wurden zahlreiche europäische NATO-Mitgliedsstaaten von politisch motivierten Cyberangriffen in Zusammenhang mit dem Krieg in der Ukrainebetroffen. Darunter befanden sich beispielsweise Belgien /CPO23w01, BLO23w01/, Bulgarien /UKR23w01/, Dänemark /REU23w02, DER23w01/, Deutschland /SPI23w01, BSI23r03, BSI23r07/, Finnland /DAI23w03/, Frankreich /REC23w01, SAK23w01/, Großbritannien /BSI23r03, COM23w01/, Italien /REC23w01/, Lettland /BIT23w01/, Luxemburg /LUX23w01/, Niederlande /REC23w01/, Norwegen /BSI23r03, COM23w01/, Polen /FOC23w01, BSI23r08/, Slowakei /UKR23w02/, Spanien /REC23w01/ und Tschechien /EXP23w01/, Albanien /FOR23w01/, Estland, Lettland, Rumänien /BSI22r17/, die Türkei /MIC22w01/, Portugal /EUR23w01/, Island /EUR23w02/, Litauen /LRT23w01/, Griechenland /MIM23w01/, Nord-Mazedonien /NAT23w01/.

Die Art der Cyberangriffe unterscheidet sich hierbei, häufig werden allerdings Phishing-Angriffe und DDoS-Angriffe beobachtet. Bei diesen Angriffen werden beispielsweise Webseiten lahmgelegt oder Daten gestohlen. Überwiegend werden dabei Regierungseinrichtungen oder andere Einrichtungen aus dem politischen Umfeld angegriffen, aber auch kritische Infrastrukturen, wie beispielsweise Finanzeinrichtungen, Transportunternehmen oder Krankenhäuser. Einige Cyberangriffe stehen im direkten Zusammenhang mit politischen Entscheidungen, wie die Unterstützung der Ukraine mit der Lieferung von Panzern /ZDF23w02, HAN23w01/ oder dem formalen Betritt von Finnland in die NATO /TAG23w01/, aber auch allein das Aussprechen einer Unterstützung der Ukraine oder Äußerungen gegen den russischen Angriffskrieg waren in der Vergangenheit ausreichend, um Ziel eines Cyberangriffes seitens prorussischer Angreifer zu werden.

Besonders hervorzuheben sind die folgenden Cyberangriffe auf einen europäischen NATO-Mitgliedsstaat:

- Im August 2023 kam es zu mehreren Cyberangriffen auf die polnische Bahn, bei dem es aufgrund eines unbefugten Sendes eines Nothalt-Signals zum Anhalten von Zügen kam. Diese Cyberangriffe ereigneten sich zweimal im August 2023. Hierbei wurde der Bahnverkehr in den nordwestlichen, südwestlichen und nördlichen Provinzen von Polen beeinflusst. Bei den Cyberangriffen wurde eine lang bekannte Schwachstelle des analogen Funksystems ausgenutzt. Beide Male kam es zu physischen Auswirkungen (siehe Anhang B.15.8) /BSI23r08, BSI23r10, WIN23w01, HEI23w01, WIR23w01/.
- Ebenfalls im August 2023 wurden mehrere deutsche Webseiten Ziel eines Cyberangriffs, darunter befanden sich deutsche Versicherungskonzerne und die Webseite des Bundesfinanzministeriums (BMF). Dieser Cyberangriff war Teil des DDoSia-Projektes, welches durch die Angreifergruppierung NoName057(16) ins Leben gerufen wurde. Jeder Hacker kann Teil dieses Projektes werden und Cyberangriffe auf vorzugsweise östliche und westliche NATO-Länder, wie Litauen, Polen, Italien, Frankreich oder Deutschland durchführen (siehe Anhang B.15.9) /BSI23w07, SAK23w01, GOL23w02, THN23w01/.
- Im Fokus einer Phishing-Kampagne, zwischen März und Mai 2023, standen auch zahlreiche osteuropäische Mitgliedsstaaten. Die Infizierung der Opfer wurde mit einer neuen Backdoor namens GraphicalProton versucht, ausgeführt von der Gruppierung APT29 (siehe Anhang B.15.10) /BSI23r11/.

Zur Veranschaulichung und Verdeutlichung, dass Russland sich im digitalen Krieg gegen die Ukraine nicht nur auf die Ukraine als Angriffsziel fokussiert, sondern zahlreiche europäische NATO-Mitgliedsstaaten als Ziel für Cyberangriffe wählt, ist in Abb. 2.1 eine Karte der EU gezeigt. Alle farblich markierten Länder sind europäische Mitgliedsstaaten der NATO. Die rot markierten NATO-Mitgliedsstaaten wurden seit Beginn des russischen Angriffskrieges im Februar 2022 Opfer eines Cyberangriffs von mutmaßlich russischen Angreifergruppierungen im Zusammenhang mit dem Krieg gegen die Ukraine. Die orange markierten NATO-Mitgliedsstaaten haben bislang keine Informationen zu einem solchen Angriff bekannt gegeben.

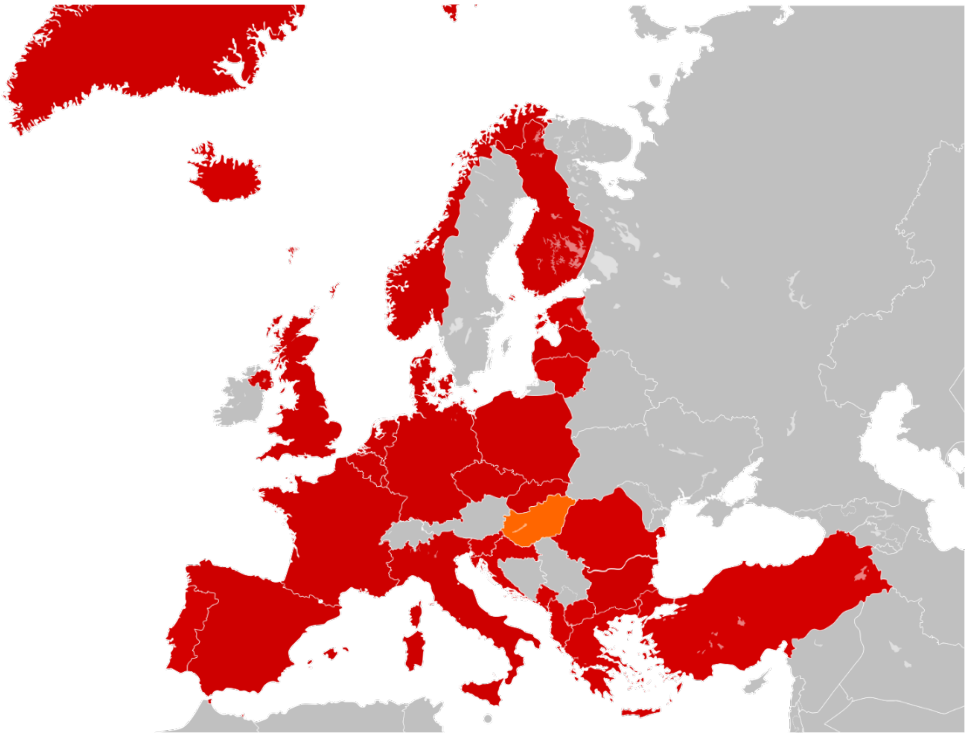

Abb. 2.1 Europäische NATO-Mitgliedsstaaten, die seit Ausbruch des Krieges in der Ukraine Opfer eines Cyberangriffs wurden

Europäische NATO-Mitgliedsstaaten, die seit Ausbruch des Krieges in der Ukraine Opfer mindestens eines politisch motivierten, mit dem Krieg in der Ukraine in Zusammenhang stehenden Cyberangriffs wurden in Rot, weitere NATO-Mitgliedsstaaten in orange. Nicht-NATO-Mitgliedsstaaten sind grau dargestellt, unabhängig davon, ob sie ebenfalls Opfer eines Cyberangriffs in Zusammenhang mit dem Krieg in der Ukraine wurden.

Anhand von Abb. 2.1 ist zu erkennen, dass sich derartige Cyberangriffe bereits gegen nahezu alle europäischen NATO-Mitgliedsstaaten gerichtet haben. Mutmaßliches Ziel ist die Beeinflussung der geleisteten Unterstützung für die Ukraine.

Es ist zudem anzumerken, dass nicht nur europäische Mitgliedsstaaten der NATO bereits das Ziel von Cyberangriffen von prorussischen Angreifergruppierungen geworden sind, sondern auch die nicht-europäischen NATO-Mitgliedsstaaten USA /BSI22r17/ und Kanada /REU23w03/, sowie NATO-Partnerstaaten, wie Schweden /MIC22w01/, Österreich /BLE22w09/, die Schweiz /SWI23w01/, Japan /TAS23w01/ und Australien /ABC23w01/.

Insgesamt ist im Zusammenhang mit dem Krieg in der Ukraine bereits vor Beginn der Kampfhandlungen eine deutliche Zunahme an Cyberangriffen bekannt geworden.

Seit Beginn der Kampfhandlungen wurde darüber hinaus ein deutlicher Anstieg bei den bekannt gewordenen Cyberangriffen festgestellt. Seit Kriegsausbruch haben insbesondere strategisch und politisch motivierte Cyberangriffe deutlich zugenommen. Grundsätzlich ist im Hinblick auf bekannt gewordene Cyberangriffe davon auszugehen, dass nur ein kleiner Teil der tatsächlich stattfindenden Angriffe publik gemacht wird. Dies gilt noch verstärkt im Umfeld der kriegerischen Auseinandersetzungen, da hier die Bekanntmachung erfolgreicher wie auch vereitelter Cyberangriffe, insbesondere auf kritische Infrastrukturen, eine verstärkte politische Dimension erhält. Daher ist vor dem Hintergrund des laufenden Angriffskrieges von einer stark verschärften IT-Bedrohungslage und einer Zunahme an Cyberangriffen bei gleichzeitig geringer werdender Informationslage auszugehen.

2.9 Cyberangriffe in Zusammenhang mit weiteren politischen Spannungsfeldern

Geht es um Cyberangriffe im Zusammenhang mit politischen Spannungsfeldern so fällt der mitteleuropäisch geschulte Blick häufig zuerst auf den nach wie vor andauernden Krieg in der Ukraine. Seit mehr als 10 Jahren kommt es dort vor allem von russischer Seite zu einer Vielzahl von Cyberangriffen, die kriegsvorbereitend und kriegsbegleitend eingesetzt wurden und werden. Häufig haben diese Cyberangriffe die Störung kritischer Infrastrukturen wie die Unterbrechung der Stromversorgung oder auch die Unterbrechung von Kommunikationsverbindungen zum Ziel. Viele dienen aber auch der Spionage, der militärischen Aufklärung, der Demonstration von Macht oder der Destabilisierung der etablierten Strukturen. Hinzu kommen Cyberangriffe mit dem Ziel der politischen Meinungsäußerung oder der Beeinflussung der für die Bevölkerung verfügbaren Informationen. Das Feld der Angreifer ist dabei breit und was Hintergrund und Fähigkeiten anbelangt sehr gemischt.

Das Spannungsfeld Russland-Ukraine bzw. Russland-NATO stellt im Moment zwar eines der sichtbarsten, aber bei Weitem nicht das einzige politische Spannungsfeld dar, in dem Cyberangriffe eine bedeutende Rolle spielen. Beispiele für weitere politische Spannungsfelder werden im Folgenden kurz umrissen. Ein zentraler Punkt hierbei ist, dass solche Spannungsfelder nicht losgelöst vom restlichen Weltgeschehen existieren, sondern sich häufig gegenseitig beeinflussen. So hat der Krieg in der Ukraine auch Auswirkungen auf Cyberangriffe und Angreiferaktivitäten in weiteren Spannungsfeldern. In den vergangenen Monaten nutzten beispielsweise eine Reihe von APTs, die dem

chinesischen, nordkoreanischen oder iranischen Nexus zugeordnet werden, die Situation in der Ukraine oder auch die EU-Sanktionen gegen Russland für ihre Zwecke.

China-Japan

Im Jahr 2023 wurden zwei Cyberangriffe auf sicherheitsrelevante japanische Einrichtungen bekannt, die chinesischen APT-Gruppierungen zugerechnet werden. Demnach wurde bereits im Herbst 2020 ein Cyberangriff auf japanische Verteidigungsnetzwerke entdeckt, der den Angreifern weitreichenden und persistenten Zugang zu militärischen Informationen wie Plänen, Fähigkeiten und Bewertungen von Unzulänglichkeiten und Schwachstellen ermöglichte (siehe Anhang B.13.25). Weiter wurde ein Cyberangriff auf die japanische Cybersicherheitsbehörde NISC (National center of Incident readiness and Strategy for Cybersecurity) bekannt, bei dem die Angreifer mindestens neun Monate lang Zugriff auf die Systeme der Cybersicherheitsbehörde hatten und von dort auch Daten ausschleusten.

Darüber hinaus fallen APTs, die dem chinesischen Nexus zugeordnet werden, seit einigen Monaten durch verstärkte Aktivitäten auf. Diese Aktivitäten sind weit gefächert und richten sich nicht nur gegen Ziele in Japan, sondern auch weltweit, beispielsweise gegen Ziele in anderen asiatischen Staaten, in Europa, Nord- und Südamerika, Australien und Ozeanien sowie in Afrika. Von Angriffen häufig betroffen sind Regierungseinrichtungen, kritische Infrastrukturen, Technologieunternehmen sowie Forschungseinrichtungen. Viele der Angriffe sind auf Persistenz und langfristigen Zugang zu Informationen und Systemen ausgelegt und scheinen auf Spionage abzuzielen. Hinzu kommen disruptive Angriffe. Vielfach werden Unternehmen reihenweise über die Lieferkette angegriffen.

Beispiele für Angriffe, die chinesischen Angreifergruppierungen zugeschrieben werden, sind der Supply Chain Angriff auf E-Mail Security Gateway-Geräte des Herstellers Barracuda, bei dem unter Ausnutzung einer Zero-Day-Schwachstelle Backdoors auf kompromittierten Systemen installiert wurden (siehe Anhang B.15.23) und die Angriffskampagne mit Volt Typhoon zur Ausspähung kritischer Infrastrukturen in den USA (siehe Anhang B.13.26). Bei letzterem wurden von mutmaßlich chinesischen Angreifern vornehmlich Ziele aus den Bereichen Kommunikation, Transport, Herstellung und IT angegriffen sowie militärnahe Einrichtungen auf der Pazifikinsel Guam, auf der sich ein wichtiger US-Luftwaffenstützpunkt befindet.

Nordkorea-Südkorea

Auch Nordkorea hat in den vergangenen Jahren seine Fähigkeiten zu Cyberoperationen deutlich ausgebaut. Angreifergruppierungen wie beispielsweise Kimsuky und Lazarus, die Nordkorea zugerechnet werden, sind weltweit aktiv. Die Angriffe sind hierbei häufig auf Spionage und Sabotage ausgerichtet. Die Ziele sind vielfältig, so wurden in den vergangenen Monaten beispielsweise Forschungseinrichtungen und Unternehmen, die im Energiesektor tätig sind, in Europa, Asien und Nordamerika angegriffen. Hinzu kommen Angriffe auf den Verteidigungssektor und Securityeinrichtungen. Vor allem Angriffe auf Südkorea werden fortwährend durchgeführt. Im August 2023 beispielsweise veröffentlichte eine südkoreanische Polizeibehörde Informationen über Cyberangriffe im Zusammenhang mit einer für Ende August 2023 geplanten gemeinsamen Militärübung der Vereinigten Staaten von Amerika und Südkorea. Demzufolge startete die nordkoreanische APT-Gruppierung Kimsuky (siehe Abschnitt 2.10.8) eine breit angelegte (Spear)Phishing-Kampagne gegenüber Auftragnehmern, die im Zusammenhang mit der Militärübung stehen. Angaben der südkoreanischen Polizei zu Folge wurden keine militärischen Informationen gestohlen.

Ein weiteres, derzeit stark wachsendes Betätigungsfeld nordkoreanischer Angreifergruppierungen ist der Diebstahl von großen Summen Kryptowährung, mutmaßlich zur Finanzierung des nordkoreanischen Atomprogramms sowie des nordkoreanischen ballistischen Programms. Auch Geldwäsche wird kontinuierlich betrieben. Allein die Angreifergruppierung Lazarus soll zwischen Mitte 2022 und Mitte 2023 Geld in Höhe von fast eine Milliarde US-Dollar gewaschen haben. Die Bezifferung des insgesamt durch nordkoreanische Angreifergruppierung in den letzten Monaten gestohlenen Betrags gestaltet sich schwierig und geht daher weit auseinander. Allerdings ist von einer mindestens zehn- aber vermutlich elfstelligen Summe an US-Dollar auszugehen.

Im August wurde bekannt gegeben, dass aufgrund der wachsenden Bedrohung im Cyberraum durch nordkoreanische Angreifergruppierungen künftig regelmäßige Konsultationen zwischen den USA, Südkorea und Japan stattfinden sollen.

Iran-Israel

Seit Jahren werden im politischen Spannungsfeld Iran-Israel von beiden Seiten Cyberangriffe durchgeführt. Ein eindrückliches Beispiel aus dem vergangenen Juni ist der Cyberangriff auf ein iranisches Stahlwerk (siehe Anhang B.14.6).

Die Cyberangriffe sind insgesamt sehr zahlreich und nehmen sowohl an Häufigkeit als auch an Komplexität zu. Bei den Angriffen von iranischen Angreifergruppierungen auf Ziele in rivalisierenden oder verfeindeten Staaten wie Israel zeichnet sich inzwischen ein Shift von überwiegend disruptiven Angriffen hin zu Angriffen zu Spionagezwecken ab. Im vergangenen Jahr wurden u. a. hochentwickelte Spionageangriffe auf Verteidigungs- und Nachrichtendienste in Israel, Saudi-Arabien und Jordanien beobachtet, die alle iranischen Angreifern zugeschrieben werden. Hierbei wurden jeweils nicht nur E-Mail-Kommunikationsdaten ausgeschleust, sondern auch zentrale Informationen über die Cyber-Infrastruktur.

Verschiedene Gruppierungen, welche dem Nexus des Iran zugerechnet werden, verüben zudem seit mehr als einem Jahrzehnt umfangreiche Cyberangriffe. Bereits 2010 wurde von den islamischen Revolutionsgarden (IRGC) des Iran die Rolle des „Soft Wars“ und der Nutzung von psychologischen Operationen („PSYOPS“) zur Stärkung des eigenen Regimes und Schwächung wahrgenommener Feinde offiziell festgeschrieben. Im Verlauf der Entwicklung des iranischen Cyberprogramms wurde daher verstärkt auf Social Engineering Maßnahmen gesetzt. Diese Angriffsmethoden dienen dazu, die Angegriffenen durch die Vorspiegelung falscher Tatsachen und das Ausnutzen menschlicher Verhaltensweisen zur Preisgabe von Zugangsrechten, Passwörtern und anderen wertvollen Details zu bewegen. Social Engineering Angriffe seitens iranischer Angreifer werden inzwischen fortwährend geführt und dabei immer wieder der momentanen Zielsetzung angepasst. Neben Angriffen auf Menschenrechtsaktivisten, Dissidenten und militärische Gegenspieler sind auch Angriffe auf Ziele aus den Bereichen Finanzen, Medizin, Forschung und Entwicklung sowie IT bekannt geworden.

Dies ist nur eine kleine Auswahl an Beispielen für politische Spannungsfelder, in denen es in den vergangenen Monaten vermehrt zu Cyberangriffen gekommen ist. Tatsächlich kommen Cyberangriffe heutzutage in praktisch allen politischen Spannungsfeldern zum Einsatz. Dies schließt Cyberangriffe verschiedenster Komplexität von einfachen disruptiven Angriffen bis hin zu hochausgereifter Schadsoftware und langandauernden Angriffskampagnen ein. Auch das Feld der Angreifer reicht unabhängig vom konkreten politischen Spannungsfeld meist von Aktivisten mit geringen Kenntnissen und wenigen Ressourcen bis hin zu staatlich geförderten APTs mit umfangreichen Ressourcen. Darüber hinaus wird für alle hier angesprochenen politischen Spannungsfelder deutlich, dass sich die Angriffe nicht auf wenige Staaten beschränken. Vielmehr sind konkrete

Spannungsfelder zwischen einzelnen Staaten meist nur Ausprägungen von deutlich breiter gefächerten Spannungsfeldern.

2.10 APT-Gruppierungen

Angreifergruppierungen mit hohem Ressourceneinsatz und langanhaltenden Angriffsmöglichkeiten erlangten seit einiger Zeit besondere Aufmerksamkeit aufgrund ihres Schadpotentials und ihrer ausdauernd eingesetzten Angriffsmöglichkeiten. Erstmals als Advanced Persistent Threats (APT, deutsch fortgeschrittene ausdauernde Bedrohung) im Jahr 2006 bezeichnet, wurde mit dem Begriff versucht, ein Phänomen von Angriffen bzw. Angriffe ausführenden Gruppierungen zu beschreiben, die über erhebliche zeitliche, finanzielle, personelle und technische Ressourcen verfügen.

Der Begriff APT beschreibt hierbei solche Gruppierungen, deren technisches Verständnis über typischerweise etablierte Fähigkeiten hinaus geht. APT-Gruppierungen nutzen zwar auch kommerzielle oder open-source Programme für ihre Aktivitäten, diese jedoch häufig in erweiterter Form oder aber in Verbindung mit komplexen Programmen oder angepasster Form für neue Schwachstellen und Angriffstechniken. In vielen Fällen können APT-Gruppierungen auf verschiedene Angriffsformen, Übertragungsformen und Weiterverbreitungsformen im Rahmen ihrer Cyberangriffe setzen und dabei über das bis dahin bekannte und allgemein etablierte Maß hinausgehen.
Zusätzlich sind diese Gruppierungen häufig langfristig orientiert und besitzen die Ressourcen und das Personal, um ihre Angriffe strategisch zu planen, zu koordinieren, auch über einen langanhaltenden Zeitraum umzusetzen und im Zweifel zu anderen Angriffsstrategien zu wechseln. Die Angriffe von APT-Gruppierungen zeichnen sich häufig durch ein schwer erkennbares und langfristig geplantes Vorgehen aus, welches dauerhaft zum Erfolg der von den Gruppierungen ausgeführten Cyberangriffe führt. Nicht entdeckte Angriffe können immer wieder genutzt werden oder für weitere Angriffe vorbereitend Verwendung finden.

Lange Zeit wurden APT-Gruppierungen zumeist in Verbindung mit staatlichen Strukturen gesehen, entweder als Einheiten von Geheimdiensten und Militär oder aber in einer abstreitbaren Form durch indirekte oder direkte Unterstützung formal privater Gruppierungen. Die Attribuierung von Angriffen durch bestimmte APT-Gruppierungen erfolgt einerseits durch typischerweise sich wiederholende Angriffsmerkmale, z. B. Codeanalysen, wiederkehrende Angriffswerkzeuge und Vorgehensweisen, wiederkehrend verwendete

Server und IP-Adressen und Codeüberreste bzw. Kommentare mit typischen identifizierbaren Merkmalen, andererseits durch seltenere Eigenattribuierung, z. B. im Falle von politisch wirksamen Angriffen. Die von Sicherheitsforschern und Regierungsorganisationen erkannten und öffentlichkeitswirksam benannten APT-Gruppierungen haben jeweils unterschiedliche Bezeichnungen erhalten, abhängig von Sicherheitsforschern und Regierungsorganisationen. Typischerweise gibt es eine Zählweise von erkannten und aufgedeckten APT-Gruppierungen, welche bei APT 1, einer APT der Volksbefreiungsarmee anfing und z. B. die Lazarus Gruppierung als APT 38 bezeichnet. Weiterhin wurden Bezeichnungen nach landestypischen Tieren eingeführt, weshalb APT 28 und APT 29 als Fancy bzw. Cozy Bear bekannt wurden. Andere Namensschema nutzen Mineralien, Pflanzen oder Wetterphänomene. Insgesamt besitzen insbesondere die profiliertesten und langlebigsten Gruppierungen eine ganze Reihe an Namen und Bezeichnungen, welche zumeist eine einzelne Gruppierung, manchmal aber auch mehrere ähnliche Gruppierungen bezeichnen können.

In Verbindung mit den staatlichen Strukturen führen APT-Gruppierungen insbesondere solche Cyberangriffe aus, welche im direkten oder indirekten Interesse der jeweiligen Staaten liegen. Hierbei können erhebliche Ressourcen- und Personalaufwendungen zum Einsatz kommen, so wurde der Stuxnet Angriff auf Basis von vier Zero-Day-Schwachstellen und umfassenden Programmierarbeiten entwickelt. Es wird vermutet, dass hierzu ein erheblicher Millionenbetrag für die Entwicklung sowie geheimdienstliche Vor-Ort-Maßnahmen für die Erstinfektionen notwendig waren. Die bekanntesten APT-Gruppierungen wie Lazarus (Abschnitt 2.10.3), Fancy Bear (Abschnitt 2.10.1) und Kimsuky (Abschnitt 2.10.8) sind zum Teil über Jahre oder Jahrzehnte mit immer wieder sich ändernden Zielen (u. A. Spionage, Sabotage, Beschaffung) aktiv.

In den letzten Jahren haben sich mit Erpressungskampagnen durch Ransomware und Datendiebstähle sowie durch angreifbare Kryptowährungen profitable Angriffsmöglichkeiten und Angriffsziele ergeben, welche auch für private Gruppierungen einen hohen Ressourcen- und Personalaufwand rechtfertigen. In der Konsequenz haben auch private Gruppierungen typische Eigenschaften von APT-Gruppierungen wie die langfristige Orientierung und die Vorgehensweisen übernommen. Zum Teil sind solche Gruppierungen mittlerweile als APT-for-hire verfügbar und bieten ihre Fähigkeiten gegen finanzielle Aufwendungen an, z. B. für Ransomware as a Service (RaaS). Dabei können Angreifer mit weitaus weniger umfangreichen Ressourcen und technischem Verständnis auf die Fähigkeiten einer solchen Gruppierung zurückgreifen und diese für vorgesehene

Cyberangriffe nutzen. Der Austausch zwischen den Auftraggebern und der APT-Gruppierung kann dabei je nach genauer Konstellation und Bedarf unterschiedlich stark ausgeprägt sein. Beispielsweise können einfache, unspezifische oder aber auch auf definierte Gegebenheiten angepasste Angriffswerkzeuge ausgetauscht werden. Dies stellt insofern eine ernstzunehmende Bedrohung dar, als dass dadurch beispielsweise hochentwickelte Angriffswerkzeuge, die nur durch einen kleinen, technisch hochausgebildeten Personenkreis entwickelt werden konnten, potenziell einer Vielzahl von Angreifern zur Verfügung stehen, die keine tiefergehenden technischen Fähigkeiten haben müssen, sondern entsprechend darauf zurückgreifen können. Andere Beispiele sind die Nutzung von Angreiferinfrastruktur und die Bereitstellung von spezifischen Informationen.

Zusätzlich zu APT-for-hire-Angeboten kommt es immer häufiger dazu, dass APT-Gruppierungen die bei Ransomware-Angriffen (siehe Abschnitt 2.1) eingesetzte Schadsoftware als Ransomware-as-a-Service gegen Bezahlung anbieten. Diese Ransomware kann entsprechend unspezifisch sein oder bei Bedarf auf spezifische Gegebenheiten angepasst werden. Beispiele für APT-Gruppierungen, die mutmaßlich Ransomware-as-a-Service anbieten bzw. bereits angeboten haben, sind die mit den IT-Sicherheitsvorfällen des Cyberangriffs auf die Colonial Pipeline und kritische Infrastrukturen im Zusammenhang stehenden Gruppierungen DarkSide (siehe Anhang B.13.2 bzw. B.13.5) und Black Matter (siehe Anhang B.13.7). Auch die vor allem für ihre Ransomware-Angriffe auf den Fleischkonzern JBS (siehe Anhang B.13.10) und den IT-Dienstleister Kaseya (siehe Anhang B.13.4) bekannte APT-Gruppierung REvil (siehe Abschnitt 2.12.10) bietet Ransomware-as-a-Service-Dienste an.

Weiterhin kommt es dauerhaft zu einem Abfluss von Fähigkeiten, Angriffswerkzeugen und Angriffsmethoden von APT-Gruppierungen zu anderen Gruppierungen und Einzelpersonen im Bereich der Cyberangriffe. Neuartige Angriffswerkzeuge und Angriffspfade der APT-Gruppierungen werden aufgedeckt und publiziert, diese werden anschließend in für deutlich mehr Angreifer nutzbare Produkte umgewandelt und veröffentlicht oder verkauft. Hierdurch entsteht zum einen ein Markt für moderne Cyberangriffswerkzeuge, aber auch ein stetiger Fähigkeitstransfer von der Speerspitze der APT-Gruppierungen zu anderen Gruppierungen mit erheblich weniger Mitteln. In der Konsequenz weitet sich die Bedrohungslage durch den Fähigkeitstransfer in die breite Masse aus.

Im Folgenden werden die maßgeblichen, bekanntesten und aktivsten APT-Gruppierungen in einer Kurzübersicht vorgestellt. Maßgebliche Cyberangriffe von APT-Gruppierungen werden darüber hinaus im Anhang B dargelegt.

2.10.1 APT28/Fancy Bear

Übersicht

Die APT-Gruppierung APT28 gehört zu Russlands militärischem Geheimdienst und ist Teil des Hauptnachrichtendienstes des russischen Generalstabes (GRU), 85. Haupt-Sonderdienstleistungszentrum (GTsSS), militärische Einheit 26165 /BAN21w01, REC21w02/. Zu ihren Haupt-Angriffszielen gehören politische und militärische Einrichtungen in Europa, speziell in osteuropäischen Staaten wie Georgien. Seit 2016 ist APT28 auch an US-amerikanischen Einrichtungen und an Unternehmen im Energiesektor interessiert.

Weitere Bezeichnungen

Die APT-Gruppierung APT28 ist auch unter den Namen Fancy Bear, Pawn Storm, Sednit, Strontium, Sofacy, Blue Delta und Tsar Team bekannt. /BLC23w02, BSI21i08, NCS23i01/

Aktivitäten

Die APT-Gruppierung APT28 ist spätestens seit 2004 aktiv /BSI21i08/. Sie ist an Verteidigungs- und geopolitischen Informationen interessiert und betreibt E-Spionage gegen politische und militärische Ziele sowie Regierungen in Georgien und Osteuropa. Nach dem Krieg in Georgien 2008 und aufgrund der Beziehungen des Landes zu westlichen Staaten, führte APT28 Angriffe gegen das georgische Ministerium für innere Angelegenheiten und das Verteidigungsministerium durch. Darüber hinaus zählen zu den Angriffszielen Sicherheitsorganisationen, die in Europa tätig sind, wie zum Beispiel die NATO oder die Organization for Security and Cooperation in Europe (OSCE). Bei einem Cyberangriff auf den deutschen Bundestag im Jahr 2015 wurden von APT28 16 Gigabyte an Daten gestohlen. 2016 mischte sich APT28 in den Wahlkampf zwischen Donald Trump und Hillary Clinton um die US-Präsidentschaft ein. Dabei führte APT28 einen Cyberangriff auf die Mitglieder von Clintons Wahlkampfteam, die Netzwerke des Demokratischen Kongress-Kampagnenkomitees und des Demokratischen Nationalkomitees durch. Es wurden Daten und E-Mails gestohlen und anschließend veröffentlicht. Zwischen Dezember 2018 und Mai 2020 griff APT28 Netzwerke US-amerikanischer Regierungsbehörden, Bildungseinrichtungen und Unternehmen im Energiesektor an. Nach Angaben des Bundesamtes für Verfassungsschutz (BfV) von 2016 gibt es Hinweise auf

Vorbereitungen von Angriffen auf deutsche Energiekonzerne. /ESE22w02, FIR14r01, ITE20w01, TAG16w01/

Seit 2019 führt APT28 eine Brute-Force-Kampagne gegen US-amerikanische und europäische Organisationen aus den Bereichen Regierung und Parteien, Militär und Verteidigungsunternehmen, Energie- und Logistikzentren, Universitäten und Medien sowie Anwaltskanzleien durch /BSI21i08/. Ein jüngerer Cyberangriff von APT28 erfolgte im Jahr 2021. Ende September 2021 führte APT28 einen Spear-Phishing-Angriff auf die E-Mail-Postfächer von 1400 Gmail-Nutzern von Google durch. Ziel des Angriffs war der Diebstahl von Passwörtern, um Zugriff auf die Postfächer zu erhalten und die darin enthaltenen Informationen abzuschöpfen. Diese Informationen sollten dann genutzt werden, um auf die Postfächer weiterer Personen und die darin enthaltenen Informationen zuzugreifen. Der Angriff war zwar global, richtete sich aber gegen einen ausgewählten Personenkreis von Aktivisten, Journalisten, Regierungsmitarbeitern, Menschenrechtlern, Rechtsanwälten und Angestellten im Bereich der Nationalen Sicherheit. Alle schadhaften E-Mails wurden jedoch von Gmail automatisch als Spam-Nachrichten klassifiziert und blockiert. /BSI21i06, MALw03, MOT21w01/

Ab November 2021 hat APT28 damit begonnen Nachrichten-E-Mails über den anhaltenden Konflikt zwischen Russland und der Ukraine zu verteilen. Die Empfänger sollen dazu gebracht werden die schadhaften E-Mails zu öffnen, damit die Angreifer Schwachstellen in Roundcube Webmail-Servern ausnutzen können, um Zugriff auf ungepatchte Server zu erhalten. Betroffen sind die Server mehrerer ukrainischer Organisationen, zu denen auch Regierungseinrichtungen gehören. Hat sich APT28 Zugriff auf einen Server verschafft, dann führen die Angreifer schadhafte Skripte aus, die eingehende E-Mails an eine E-Mail-Adresse der Angreifer umleiten. Zudem ermöglichen die Skripte Auskundschaftungen und den Diebstahl personenbezogener Daten aus der Roundcube-Datenbank wie Adressbücher und Sitzungs-Cookies sowie andere Informationen. Laut einer gemeinsamen Untersuchung des ukrainischen Computer Emergency Response Teams (CERT-UA) und der Bedrohungsforschungsabteilung Insikt Group von Recorded Future will APT28 auf diese Weise militärische Informationen sammeln, um die russische Invasion in der Ukraine zu unterstützen. /BLC23w02/

Seit dem Jahr 2021 nutzt APT28 die seit dem 29.06.2017 bekannte SNMP-Schwachstelle CVE-2017-6742 in der Cisco IOS- und der Cisco IOS XE-Software erfolgreich aus. SNMP steht für Simple Network Management Protocol, einem Netzwerkprotokoll, das Administratoren die Überwachung und Konfiguration von Netzwerkgeräten

ermöglicht. APT28 verwendet die Schwachstelle, um die Schadsoftware Jaguar Tooth auf öffentlich zugänglichen Netzwerkroutern des Herstellers Cisco zu installieren. Jaguar Tooth ermöglicht es den Angreifern Geräteinformationen über das Netzwerk zu sammeln und zu exfiltrieren. Diese Informationen dienen APT28 zu Spionagezwecken oder für die Planung zukünftiger Cyberangriffe. Die Ziele der Kampagne sind auf der ganzen Welt verteilt, erstrecken sich aber hauptsächlich auf Europa, Regierungsinstitutionen in den USA und auf etwa 250 ukrainische Ziele. /BLC23w01, CIS23w01, NCS23i01/

In Verbindung mit dem Ukrainekrieg führt APT28 seit Juni 2022 eine Kampagne durch, die auf Benutzer in der Ukraine abzielt. APT 28 verbreitet ein bösartiges Dokument mit Dateinamen „Nuclear Terrorism A Very Real Threat.rtf“, in dem sich ein Artikel des Atlantic Council vom 10. Mai 2022 mit der Schlagzeile „Wird Putin in der Ukraine Atomwaffen einsetzen? Unsere Experten beantworten drei brennende Fragen“ beinhaltet. Dabei zielt APT28 auf die Furcht der ukrainischen Bürger vor einem nuklearen Angriff durch Russland ab. Das Dokument beinhaltet das Exploit Follina (CVE-2022-30190), um einen .Net-Stealer herunterzuladen. Der Stealer wird dann eingesetzt, um die Daten der Benutzer aus mehreren gängigen Browsern zu stehlen. /ITD22w01/

Seit April 2023 sendet APT28 E-Mails mit dem Titel „Windows Update“ an ukrainische Regierungsbehörden. Gemäß des CERT-UA sollen die Empfänger dazu gebracht werden eine Kommandozeile zu öffnen und einen bestimmten PowerShell-Befehl dort einzugeben. Bei der Ausführung des Befehls wird ein Windows-Update simuliert. Tatsächlich wird aber ein PowerShell-Skript ausgeführt, das grundlegende Systeminformationen sammelt und diese an Mocky sendet. Dabei handelt es sich um einen Dienst, der Programmierschnittstellen simuliert, um Entwicklern beim Test von Apps zu helfen. /THR23w01/

APT28 nutzt Spear-Phishing-E-Mails, um Zugriff auf Accounts und Netzwerke zu erhalten. Eine weitere Taktik ist das Vortäuschen von legitimen Nachrichten-, Politik- und anderen Webseiten. Seit 2007 hat die APT-Gruppierung ihre Schadsoftware regelmäßig aktualisiert. Sie besteht aus drei wesentlichen Komponenten, dem Downloader SOURFACE, der Backdoor EVILTOSS und dem modular aufgebauten Schadsoftware-Werkzeug CHOPSTICK. Der SOURFACE-Downloader lädt die Backdoor EVILTOSS, um eine persistente Verbindung zum infizierten Netzwerk herzustellen. Darüber hinaus ermöglicht die Backdoor die Netzwerküberwachung, den Diebstahl von Berechtigungen und die Ausführung von Shellcode. Das modular aufgebaute Schadsoftware-Werkzeug CHOPSTICK bietet zusätzliche, für den Angriff zugeschnittene Funktionalitäten und wirkt

als eine weitere Backdoor. Die Anwendung von Reverse-Engineering-Techniken auf die Schadsoftware wird durch diverse Gegenmaßnahmen erschwert. Dazu zählen Laufzeitüberprüfungen zur Identifizierung von Analyseumgebungen, das Entpacken bedeutungsloser Strings während der Laufzeit zur Verschleierung der Funktionalität der Schadsoftware und die Einbindung ungenutzter Maschinenbefehle zur Verlangsamung von Softwareanalysefunktionen. /FIR14r01/

Seit 2019 setzt APT28 zusätzlich Brute-Force-Attacken ein. Dabei wird von einem Angreifer versucht ein Passwort, einen Benutzernamen, die Adresse einer verborgenen Webseite oder einen Schlüssel nach dem Versuch-und-Irrtum-Prinzip zu erraten, was je nach Komplexität wenige Sekunden bis mehrere Jahre dauern kann. Die Brute-Force-Angriffe sind auf geschützte Daten wie E-Mails und die Identifizierung von Kontenanmeldeinformationen ausgerichtet. Diese Informationen werden dann genutzt, um den Erstzugriff auf das Netzwerk, eine persistente Verbindung und eine Privilegien-Eskalation zu erreichen, sowie Schutzfunktionen zu umgehen. /KAS21w02, NCS21i01/

2.10.2 APT29/Cozy Bear/Nobelium

Übersicht

APT29/Cozy Bear/Nobelium gilt als eine der am besten organisierten sowie technisch versiertesten APT-Gruppierungen weltweit. Viele IT-Sicherheitsanalysten sehen eine Verbindung zwischen APT29/Cozy Bear und staatlichen russischen Stellen und gehen davon aus, dass APT29/Cozy Bear im Auftrag des russischen Auslandsgeheimdienstes SVR agiert. Es wird davon ausgegangen, dass die APT-Gruppierung Nobelium, die für die IT-Angriffe in Zusammenhang mit schadsoftwarebehafteten Solar Winds Produkten verantwortlich gemacht wird, mit APT29/Cozy Bear identisch ist.

Weitere Bezeichnungen

Die APT-Gruppierung APT29 ist neben den Namen Cozy Bear und Nobelium auch noch unter weiteren Namen bekannt. Hierzu zählen Office Monkey, Cozy Duke, Cozy Car, Dark Halo, The Dukes, Stellar Particlem UNC2452 und Yttrium /KAS21w01/.

Aktivitäten

Angriffe von APT29/Cozy Bear sind typischerweise schwer zu detektieren, da APT29/Cozy Bear sehr diszipliniert vorgeht und ihre Aktivitäten im Zielnetzwerk gekonnt verschleiert. So werden Daten nur unregelmäßig übertragen, die ausgeschleusten Informationen werden als legitimer Datenverkehr getarnt und die Interaktion erfolgt auch über verschlüsselte Verbindungen. Auch erfolgt ein Monitoring der Sicherheitsmaßnahmen in den Zielnetzwerken. Laut FireEye implementiert APT29/Cozy Bear Backdoors, um Bugs in ihrer eigenen Malware zu beheben und neue Funktionen einzufügen. Auch befinden sich die von APT29 entwickelten und eingesetzten Schadsoftwarekomponenten und IT-Angriffswerkzeuge fortlaufend in der Weiterentwicklung und Anpassung, um einer Detektion zu entgehen. /FIR21w02/

Der Gruppierung APT29/Cozy Bear werden seit etwa 2014 zahlreiche Angriffe auf US-amerikanische und europäische Regierungseinrichtungen zugeschrieben /KAS21w01/. Von den USA und britischer Seite wurden die IT-Angriffe mit schadsoftwarebehafteten SolarWinds-Produkten, die Ende 2019 bekannt wurden (siehe Abschnitt B.12.4 im Anhang), ebenfalls APT29/CozyBear zugeschrieben.

Die ersten IT-Angriffe von APT29/Cozy Bear erfolgten im Jahr 2009. Betroffen waren das Verteidigungsministerium von Georgien sowie die Außenministerien der Türkei und von Uganda. Darüber hinaus führte die Gruppierung eine Kampagne gegen in den USA ansässige Denkfabriken für Außenpolitik, sowie Regierungseinrichtungen in Polen und Tschechien durch. Dazu verwendeten die Angreifer schadhafte Microsoft Word Dokumente und PDF-Dateien in E-Mailanhängen. Es wird vermutet, dass APT29/Cozy Bear die Angriffe durchführte, um Informationen zum Standort einer Raketenabwehrstation in Polen zu sammeln. Ebenfalls im Jahr 2009 erfolgten Angriffe gegen eine NATO-Übung in Europa und ein georgisches Informationszentrum zur NATO. /FES15r01/

Während des Jahres 2010 griff APT29/Cozy Bear Organisationen in der Türkei, Georgien, Kasachstan, Aserbaidschan und Usbekistan an. Am 19. Januar 2010 entdeckte der IT-Sicherheitsforscher Tavis Ormandy eine Schwachstelle mit Bezeichnung CVE-2010-0232 in Microsoft Windows, welche es einem Angreifer ermöglicht lokale Privilegien zu erhalten. Bereits sieben Tage später, am 26. Januar 2010, hatte APT29/Cozy Bear seine Schadsoftware CosmicDuke so angepasst, dass sie die Schwachstelle ausnutzen konnte. /FES15r01/

Das IT-Sicherheitsunternehmen FireEye entdeckte am 12. Februar 2013 zwei Zero-Day-Schwachstellen CVE-2013-0640 und CVE-2013-0641. Acht Tage nach der Entdeckung der Schwachstellen hatte APT29/Cozy Bear die Ausnutzung der Schwachstellen in ihre Schadsoftware MiniDuke integriert. Daraufhin setzte APT29/Cozy Bear die Schadsoftware gegen Ziele in Belgien, Ungarn, Luxemburg, Spanien, Rumänien, der Ukraine, Portugal, Tschechien, Irland und den USA ein. Für die Kompromittierung mit MiniDuke nutzten die Angreifer Spear-Phishing-E-Mails mit schadhaften PDF-Dateien im Anhang. Die PDF-Dokumente trugen die folgenden Titel: „Der NATO-Mitgliedschaftsplan der Ukraine (MAP), Debatten“, „Das informelle Asien-Europa-Treffen (ASEM) – Seminar zum Thema Menschenrechte“ und „Die Suche der Ukraine nach einer regionalen Außenpolitik“. /FES15r01/

Im frühen Sommer 2015 führte APT29/Cozy Bear Kampagnen mit der Schadsoftware CozyDuke und CloudDuke durch. Für die Kompromittierung nutzten sie schadhafte Dokumente, die kürzlich geschlossene Schwachstellen ausnutzten. Zu den Zielen gehörten polnische und georgische Organisationen.

Für letztere nutzte APT29/Cozy Bear ein schadhaftes Worddokument mit Namen „Die NATO festigt die Kontrolle über das Schwarze Meer.docx“ /FES15r01/

Im Frühjahr 2020 führte APT29/Cozy Bear einen Lieferkettenangriff durch. Dabei präparierten sie Updates der Solar Winds Orion Unternehmenssoftware mit einer Backdoor namens Sunburst (siehe Abschnitt B.12.4). Kunden, die die Updates installierten, wurden entsprechend kompromittiert. Betroffen sind öffentliche und private Organisationen auf der ganzen Welt und in den Bereichen Regierung, Consulting, Technologie und Telekommunikation. Das Ziel der Angreifer war der Diebstahl von Daten. /MAN20w01, SEC21w12, VOL20w01/

Im April 2021 begann APT29/Cozy Bear damit Regierungsnetzwerke, Denkfabriken, Organisationen für politische Analysen und IT-Unternehmen in den USA und anderen Ländern zu kompromittieren und Daten von diesen abzugreifen. Seit Mai 2021 versucht APT29/Cozy Bear Zugriff auf Kunden von Cloud-Dienstleistern, Managed Service Providern und anderen IT-Dienstleistern in den USA und Europa zu erhalten. Das Microsoft Threat Intelligence Center (MSTIC) vermutet, dass die Angreifer versuchen bestehende technische Vertrauensbeziehungen zwischen den Anbietern und Regierungen, Denkfabriken und anderen Unternehmen auszunutzen. /CIS21r06, MIC21w07, MIC21w08/

Zwischen März und Mai 2023 griff APT29/Cozy Bear diplomatische Einrichtungen in ganz Osteuropa an (siehe Abschnitt B.15.10). Dabei wurde versucht die Ziele mit einer Backdoor namens GraphicalProton zu infizieren, die über die Anhänge von Phishing-E-Mails in die betroffenen Systeme eingebracht wurde. Es wird vermutet, dass die Angriffswelle auf das Interesse der russischen Regierung an strategischen Daten in Bezug auf den Ukrainekrieg zurückzuführen ist. /BSI23r11/

2.10.3 APT 38/ Lazarus Group

Übersicht

Die Gruppierung Lazarus bzw. APT 38 ist eine der aktuell bekanntesten, ältesten und einflussreichsten APT-Gruppierungen, welche bisher der Öffentlichkeit bekannt geworden sind. Die Gruppierung wird für einige der größten Cyberangriffe der Welt (Sony Pictures Hack, WannaCry) verantwortlich gemacht. Erste Erwähnungen der Gruppierung existieren seit 2007, wobei der selbstgegebene und attribuierte Name der Gruppierung regelmäßig wechselte. Die Lazarus Gruppierung wird dem nordkoreanischen Staat als Akteur zugeordnet, wobei die Unterscheidung verschiedener nordkoreanischer Akteure aufgrund der Kooperation und falschen Identifikationsmerkmale zur Tatverschleierung nicht durchgehend möglich ist. /TRM18r02/

Weitere Bezeichnungen

Die APT-Gruppierung APT38 ist neben den Namen Lazarus Group auch noch unter weiteren Namen bekannt. Hierzu zählen Operation DarkSeoul, Dark Seoul, Hidden Cobra, Hastati Group, Andariel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Subgroup: Bluenoroff, Group 77, Labyrinth Chollima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, APT 38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APT-C-26, NICKEL GLADSTONE, COVELLITE, ATK3, G0032, ATK117, G0082. /FRA22w01/

Aktivitäten

Die erstmaligen Operationen der Lazarus Gruppierung waren direkt in den Koreakonflikt eingebettet, mit initialen Angriffen auf südkoreanische Regierungsstellen, Finanzinstitutionen, Medienkonzerne, und weiteren kritischen Infrastrukturunternehmen. Zu diesen Angriffen gehören insbesondere die DDoS-Angriffe im Juli 2009 gegen

US-amerikanische und südkoreanische Webseiten unter dem Titel Operation Troy und die im Jahr 2013 durchgeführten Cyberangriffe gegen den südkoreanischen Staat und seine Institutionen. Hierbei wurden bekannte Typen von Schadsoftware wie der Computerwurm Mydoom verwendet, wodurch ein von den Angreifern nutzbares Computernetzwerk aus fernsteuerbaren Bots entstand. Mit diesem Netzwerk wurden massenhaft Anfragen an Webseiten gesendet, wodurch diese temporär nicht verfügbar waren. 2013 wurde mit dem DarkSeoul Wiper eine eigene Schadsoftware der Gruppierung gegen südkoreanische Fernsehsender, Internetanbieter und Banken angewendet. Hierbei wurde nach bisherigen Informationen über ein Update die Schadsoftware an die IT-Systeme verteilt, die Schadsoftware führte dann zu einer vollständigen Löschung aller auf dem IT-System gespeicherten Daten. Durch die Betroffenheit eines Internetanbieters waren Teile Südkoreas mehrere Stunden vom Internet getrennt. /CPO21w01/

Mit dem Cyberangriff auf den Filmanbieter Sony Pictures begann eine neue Phase der Aktivitäten der Lazarus Gruppierung. Die Gruppierung führte nun weltweit Cyberangriffe durch, welche als mit nordkoreanischen Interessen konvergierend beschrieben werden.

Der Angriff auf Sony Pictures im Jahr 2014 gilt als umfassender gezielter Cyberangriff auf ein Einzelunternehmen. Die Angreifer erlangten langfristigen, tiefgreifenden Systemzugriff, installierten Backdoors für mehrfachen Zugriff und ließen große Datenmengen (die Angreifer sprechen von 100 Terabyte) abfließen. Die Angreifer entwendeten persönliche Mitarbeiterinformationen, bisher nicht veröffentlichte, digitale Versionen von Filmen, Film-Skripten und Filmplanungen, finanzielle Details und weitere Informationen. Zum Abschluss nutzten die Angreifer die Schadsoftware Shamoon, welche als Wiper auf allen betroffenen IT-Systemen sämtliche gespeicherte Daten löschte. Die Angreifer machten den Cyberangriff selbst öffentlich und verlangten den Film „The Interview“, ein Film, welcher sich mit einer fiktiven Tötung des nordkoreanischen Staatsführers beschäftigte, nicht zu veröffentlichen. Der Film wurde schließlich nur eingeschränkt veröffentlicht. IT-Sicherheitsexperten sind sich uneinig, ob die Lazarus Gruppierung für den Cyberangriff verantwortlich war oder aber andere Angreifer sich der Identität der Gruppierung annahmen. /MED18r01/

In den Jahren nach dem Cyberangriff auf Sony-Pictures begann die Gruppierung Lazarus nach bisherigen Erkenntnissen mit deutlich verstärkten Cyberangriffen auf Finanzdienstleister, Finanzunternehmen, Besitzer und Handelsbörsen von digitalen Währungen sowie auf Rüstungsunternehmen und genereller Informationsbeschaffung. So führte die Gruppierung einen Cyberangriff auf die Zentralbank von Bangladesch aus, bei

welchem die Gruppierung insgesamt 81 Millionen Dollar erbeutete. Im Jahr 2018 konnte die Gruppierung mehr als 530 Millionen Dollar durch einen Angriff auf die japanische Börse Coincheck für digitale Währungen erbeuten. WannaCry, ein sich 2017 schnell verbreitender wurmartiger Erpressertrojaner, wird ebenfalls der Gruppierung Lazarus zugeordnet. Dabei wird WannaCry als Fehlschlag angesehen, da die initiale Version aufgrund eines Programmierfehlers keine individuellen Adressen zur Bezahlung des geforderten Lösegelds zur Entschlüsselung erzeugte, sondern drei festgeschriebene und die Erpresser somit keine individuellen Codeschlüssel automatisch nach Bezahlung verteilen konnten. WannaCry legte hunderttausende IT-Systeme weltweit innerhalb kürzester Zeit lahm und verursachte hohe wirtschaftliche Schäden. Auch die Schadsoftware DTrack, mit welcher insbesondere indische Geldautomaten und damit Bankkunden angegriffen wurden und über 3 Millionen Kreditkartendaten abgegriffen wurden, wird der Gruppierung Lazarus zugeordnet. /INT19r01, AVI20r01/

Der Cyberangriff auf das indische Kernkraftwerk Kudankulam wurde mit einer modifizierten Version der Schadsoftware DTrack durchgeführt. Dabei kam es zur Entwendung umfangreicher Daten aus dem administrativen Netzwerk des Kernkraftwerkes. Die Aufklärung und Beschaffung von Daten mit Interesse für die nordkoreanische Regierung gelten als weitere Motivation für die Cyberangriffe von Lazarus. /INT19r01/

Lazarus werden in den folgenden Jahren nach WannaCry direkte Cyberangriffe im Sinne und Auftrag des nordkoreanischen Staates zugeschrieben. Da sich die politischen Ziele verschieben, haben sich mit der Zeit auch die Angriffsziele der bis heute aktiven Gruppierung Lazarus verschoben. Im Jahr 2019 wurden die erfolgreichen Diebstähle mit den neu aufgekommenen Schadsoftwaren ELECTRICFISH und FASTCash 2.0 nordkoreanischen Akteuren und insbesondere Lazarus zugeordnet, welche vermutlich seit Oktober 2018 mehrere 100 Millionen Dollar in digitalen Gütern erbeuten konnten. Die COVID-19-Pandemie verschob die Ziele in den medizinischen Bereich, wobei ein Angriff auf das britisch-schwedische Unternehmen AstraZenica, ein Hersteller von COVID-19-Impfungen, Ende 2020 für hohe Aufmerksamkeit sorgte. Im Verlauf der Jahre 2020 bis 2022 lagen die drei Hauptziele von Lazarus in der Akquirierung finanzieller Mittel aus den Bereichen Kryptowährungen, Blockchain und Banking, der Informationsbeschaffung im Bereich Verteidigung und auch nuklearen Industrien sowie der Disruption und Angriffen auf Ziele in Südkorea. /CIS20r07, REU20w02, DRW21r01, CIS20r08, ESE20r01/

Ende 2022 wurden neben der Mittelbeschaffung im Rahmen von Angriffen auf Börsen für Cryptowährungen weitere Spionageoperationen der Gruppierung Lazarus zugeschrieben. So wurden Cyberangriffe auf medizinische Einrichtungen, Forschungseinrichtungen und Unternehmen aus dem Energiesektor bekannt, welche Lazarus im vierten Quartal 2022 zugeschrieben wurden. Hierzu wurden bestehende Schwachstellen in einem Mail-Server, um initialen Zugang zu den Netzwerken der Betroffenen zu erreichen. Mit legitimen Möglichkeiten von Windows- und Linuxsystemen (Living-off-the-Land) wurden dann weitergehende Zugriffsmöglichkeiten geschaffen um letztlich Kontakt zu den Command-and-Control (C2) Servern aufzunehmen und Daten aus den betroffenen Netzwerken abzuschöpfen. /ZEI23w02, WIS23r01/

Weitere Spionageoperationen betreffen insbesondere Energieversorger in den USA, Kanada und Japan, bei welchem Lazarus insbesondere auf die schwerwiegende Schwachstelle Log4Shell der Java Bibliothek Log4j und die diese einsetzende Software VMWare Horizon einsetzte. Mit insgesamt 3 verschieden Remote Access Trojanern mit den Namen „VSingle“, „YamaBot“ und „MagicRAT“ wurde ein umfassendes Programm durchgeführt, welches mit dem Ziel des langfristigen Zugangs und der Datenspionage einherging. Dieses Programm begann vermutlich im Februar 2022 und damit 2 Monate nach der Entdeckung von Log4Shell und wurde im April 2022 erstmalig aufgedeckt. /CSD22w01, CIS22r06/

Die Angriffe auf Börsen für Cryptowährungen wurden im zweiten und dritten Quartal durch Lazarus intensiviert, es wird davon ausgegangen, dass Lazarus in dieser Zeit ca. 100 Millionen $ von der Börse Atomic Wallet, 37,3 Millionen $ von der Börse CoinsPaid, 60 Millionen $ von der Börse Alphapo, 41 Millionen $ von der Börse Stake.com und bis zu 54 Millionen $ von der Börse CoinEx entwendete. Neben klassischen Angriffsmethoden wurden hierbei Social Engineering Methoden wie gefälschte Bewerbungsmöglichkeiten als Möglichkeiten für die Erstinfektion der betroffenen IT-Systeme verwendet. /ELL23r01/

Ende September 2023 wurde ein weiterer Social Engineering Angriff aufgedeckt, welcher Lazarus zugeschrieben wird. Bei dem Ziel des Angriffes handelt es sich um ein Luft- und Raumfahrtunternehmen, bei welchem Mitarbeiter über die Social-Networking-Plattform LinkedIn kontaktiert wurden und Programmieraufgaben im Rahmen eines Einstellungsverfahren bearbeiteten sollten. Die hierbei zur Verfügung gestellten Daten wurden von Lazarus mit verschiedenen Schadsoftwaren versehen. Mit der komplexesten Schadsoftware, einem Remote Access Trojaner namens LightlessCan wurde eine

Schadsoftware für die Spionage, die Schaffung von Hintertüren und Systemmanipulationen eingesetzt, welche umfassende Techniken zur Verschleierung ihrer Präsenz nutzt. Zu diesen Methoden zählten auch erstmal von Lazarus verwendete Methodiken zur Verhinderung der Aufdeckung durch SoC-SIEM Sicherungs- und Überwachungssysteme. /WEL23r01/

Die Cyberangriffe, welche Lazarus zugeschrieben werden, deuten auf ein umfassendes, sich ständig weiterentwickelndes Arsenal an Fähigkeiten der Gruppierung hin. Zum initialen Zugriff nutzt Lazarus Spear Phishing, Watering Holes, Schwachstellen, früher erfahrene bzw. ausgespähte Zugriffsdaten und Brute Force Methoden. Danach nutzt Lazarus sowohl öffentlich verfügbare, aber auch selbst erstellte Schadsoftware. Nach lateraler Verbreitung in den betroffenen Netzwerken werden zumeist entweder Daten oder Gelder entwendet und schlussendlich Ransomware oder Wiper verwendet, um die eigenen Spuren zu verwischen oder aber weitere aktive Schäden zu verursachen. /AVI20r01

Der Gruppierung Lazarus werden eine große Anzahl von Cyberangriffen zugeordnet, wobei die individuelle Zuordnung umstritten ist.

Andere APT-Gruppierungen nutzen die Bekanntheit von Lazarus, um ihre eigenen Spuren zu verwischen und bauen absichtlich koreanische Spuren in ihre Schadsoftware. Weiterhin agieren in Nordkorea mehrere APT-Gruppierungen und die Unterscheidung von Lazarus und anderen Gruppierungen ist nicht immer vollständig möglich. So überschneiden sich die Tätigkeitsfelder der APT Kimsuky und der APT Lazarus oder es besteht Zusammenarbeit, weshalb beide Gruppierungen auch unter die Bezeichnung Hidden Cobra fallen könnten, welche aktuell von der amerikanischen Bundespolizei für Lazarus bzw. Kimsuky verwendet wird.

Kerntechnischer Bezug

Der Cyberangriff auf das indische Kernkraftwerk Kudankulam wird direkt der APT Lazarus zugeschrieben. Weiterhin richten sich die Cyberangriffe der Gruppierung insbesondere auch auf Unternehmen der kritischen Infrastruktur und solcher Bereiche, welche im Interesse des nordkoreanischen Staates liegen. Daher sind weitere kerntechnische Bezüge nach aktuellem Kenntnisstand nicht auszuschließen.

2.10.4 Chernovite

Übersicht

Informationen über die Gruppierung „Chernovite“ gelangten am 13.04.2022 erstmals an die Öffentlichkeit, als die US-amerikanische CISA in Zusammenarbeit mit dem FBI, der NSA und dem DoE eine Warnmeldung zu einem ICS-spezifischen Set aus Angriffswerkzeugen *„APT Cyber Tools Targeting ICS/SCADA Devices“* veröffentlichte, zu welchem es zudem entsprechende Berichte und Analysen von den IT-Analysten der Firmen Dragos und Mandiant gibt. Es handelt sich um ein hochkomplexes, maßgeschneidertes und sehr breit aufgestelltes Set aus Angriffswerkzeugen, welches vor allem auf die Manipulation von industriellen Steuerungssystemen abzielt und gezielt dafür entwickelt wurde. Hinter der Entwicklung dieses Incontroller/Pipedream genannten Sets aus Angriffswerkzeugen steht laut Dragos die Gruppierung Chernovite. Dragos geht mit hoher Wahrscheinlichkeit davon aus, dass es sich dabei um einen staatlichen Akteur handelt, der Incontroller/Pipedream mit der Absicht entwickelt hat, die Angriffswerkzeuge für zukünftige Operationen zu nutzen. Da die IT-Analysten Incontroller/Pipedream nach eigenen Angaben seit Anfang 2022 untersuchen, ist davon auszugehen, dass die dahinterstehende Gruppierung Chernovite mindestens seit 2021 aktiv ist. /CIS22r01, DRA22w01, MAN22w01/

Weitere Bezeichnungen

Bislang sind keine weiteren Bezeichnungen der Gruppierung bekannt.

Aktivitäten

Nach Angaben von Dragos wurde Incontroller/Pipedream mit hoher Wahrscheinlichkeit bisher noch nicht für einen Cyberangriff eingesetzt. Die bisherigen Aktivitäten von Chernovite beschränken sich somit nach bisherigen Informationen auf die Entwicklung der Angriffswerkzeuge. Mit diesen hat Chernovite ein leistungsfähiges, offensives ICS-Malware-Framework entwickelt, mit dem die Gruppierung in der Lage ist, industrielle Umgebungen und physische Prozesse in industriellen Umgebungen zu stören, zu beeinträchtigen und potenziell zu zerstören. Incontroller/Pipedream bietet Angreifern konkret beispielsweise Möglichkeiten, Geräte im Netzwerk zu suchen, Passwörter mit Brute-Force-Angriffen zu knacken, Verbindungen zu trennen und Zielgeräte zum Absturz zu bringen, beispielsweise über Denial-of-Service-Angriffe. Auf höchster Ebene bieten

die SPS-bezogenen Komponenten von Incontroller/Pipedream Angreifern eine Schnittstelle zur Manipulation entsprechender Zielgeräte. Zu diesem Zweck verwendet Incontroller/Pipedream mehrere verschiedene Protokolle, darunter das von Omron-SPS verwendete FINS, Modbus, OPC-UA[2] und die CoDeSys-Implementierung von Schneider Electric.

Incontroller/Pipedream zielt auf Anlagen in den Bereichen Flüssigerdgas (LNG), teilweise Öl und außerdem Elektrizität ab. Es ist jedoch davon auszugehen, dass Chernovite die Fähigkeiten der Angriffswerkzeuge leicht anpassen könnte, um eine breitere Palette von Zielen zu kompromittieren und anzugreifen. Entsprechend sind potenziell auch andere Industriezweige, generell kritische Infrastrukturen inklusive kerntechnischer Anlagen und Einrichtungen und Hersteller entsprechender Komponenten – vor allem SPS – mögliche Angriffsziele.

[2] Unter OPC-UA bzw. Open Platform Communications Unified Architecture versteht man einen Standard zum Datenaustausch im Rahmen von plattformunabhängiger Kommunikation.

2.10.5 Dragonfly/Energetic Bear

Übersicht

Die Angreifergruppierung Dragonfly/Energetic Bear fällt seit einigen Jahren durch Cyberangriffe auf kritische Infrastrukturen auf. Hierbei konzentriert sich die Gruppierung vornehmlich auf Credential Harvesting, sowie auf das Ausspähen und Ausleiten von Informationen. Hierbei liegt ihr Fokus auf industriellen Steuerungssystemen. Analysten gehen davon aus, dass es sich um eine russische, staatlich geförderte APT-Gruppierung handelt. In der Fachwelt herrscht weitgehend Einigkeit darüber, dass diese Angreifergruppierung das Potenzial hat, gezielt Sabotage an industriellen Steuerungssystemen und physische Schäden hervorzurufen, dieses Potenzial bislang aber noch nicht eingesetzt hat /THA20f01, SYM17r01/.

Weitere Bezeichnungen

Der APT-Gruppierung werden neben den Namen Dragonfly und Energetic Bear auch noch eine Reihe weiterer Namen zugeordnet, darunter Berserk Bear, Crouching Yeti, ALLANITE, DYMALLOY, Group 24, TeamSpy, Havex und Koala Team. Ob es sich bei all den genannten Namen um dieselbe oder nur sehr ähnliche Gruppierungen handelt, wird in der Fachwelt kontrovers diskutiert. Die APT-Gruppierung, die für die zweite Angriffswelle verantwortlich ist, wird zusätzlich noch als Dragonfly 2.0 und IRON LIBERTY bezeichnet. Da es eine starke Überlappung zwischen Dragonfly und Dragonfly 2.0 hinsichtlich der Angriffstechniken und der eingesetzten Angriffswerkzeuge gibt, gehen viele Analysten davon aus, dass es sich um dieselbe Gruppierung handelt /SYM17r01/. Teilweise werden Dragonfly und Dragonfly 2.0 derzeit aber auch getrennt weiterverfolgt /MIT20w01/, da es prinzipiell denkbar ist, dass sich eine weitere APT-Gruppierung als Dragonfly ausgibt.

Aktivitäten

Die APT-Gruppierung ist seit etwa 2010 aktiv. Bislang werden Dragonfly zwei Angriffswellen zugeordnet, wobei die erste ihren Höhepunkt 2013 erreichte und nach ihrer Entdeckung 2014 abflaute. Die zweite Welle wurde ab 2015 ausgemacht und dauert nach wie vor an. /SYM14r01, BSI20i01/. Nach Bekanntwerden der ersten Welle von Cyberangriffen durch diese Gruppierung und der Veröffentlichung von Details zu den eingesetzten Angriffswerkzeugen im Jahr 2014, wurden etwa ein Jahr lang nur wenige Aktivitäten

von Dragonfly beobachtet. Es wird vermutet, dass die Gruppierung diese Zeit zur Entwicklung neuer Angriffswerkzeuge intensiv nutzte. Anfang 2015 gab es erste Hinweise auf eine neue Angriffswelle. Betroffen waren und sind vornehmlich Unternehmen mit Verbindung zum Energiesektor, einschließlich der Nuklearindustrie sowie der Öl- und Gasindustrie /CYC18w01/. Ab 2017 wurden verstärkt Angriffe bekannt, unter anderem ein Angriff auf das US-Kernkraftwerk Wolf Creek. Ein Ende der zweiten Angriffswelle ist derzeit noch nicht abzusehen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichte zuletzt am 19.05.2020 eine BSI-Cyber-Sicherheitswarnung /BSI20i01/ zu Hinweisen auf eine größere Angriffskampagne dieser APT-Gruppierung gegen deutsche kritische Infrastrukturen. Parallel dazu fiel die Angreifergruppierung Dragonfly/Energetic Bear ab 2019 auch durch Cyberangriffe auf und monatelange Kompromittierung von ukrainischen Webseiten, unter anderem im Energiesektor auf. Eine weitere Angriffskampagne, die ebenfalls Dragonfly/Energetic Bear zugeschrieben wird, hatte vornehmlich US-amerikanische Flughäfen zum Ziel. Weitere Aktivitäten gab es wohl im Zusammenhang mit der Präsidentschaftswahl 2020 in den USA.

2.10.6 Electrum

Übersicht

Die APT-Gruppierung ELECTRUM diente ursprünglich dazu die APT-Gruppierung Sandworm bei der Entwicklung von Schadsoftware zu unterstützen, wird aber inzwischen von vielen IT-Analysten als eigenständige APT-Gruppierung geführt.

Weitere Bezeichnungen

Bislang sind keine weiteren Bezeichnungen bekannt.

Aktivitäten

Beim Angriff mit der Schadsoftware Crashoverride auf das ukrainische Stromnetz am 17.12.2016 war ELECTRUM zum ersten Mal nicht nur als Entwickler, sondern auch als Angreifergruppierung tätig. Nach Dragos handelt es sich um eine der kompetentesten und am höchsten entwickelten APT-Gruppierungen, welche auf die Manipulation von industriellen Steuerungssystemen ausgerichtet ist /DRA20w01/. ELECTRUM besitzt weitreichende Kenntnisse von industriellen Steuerungssystemen und Kommunikationsprotokollen, die in elektrischen Einrichtungen des Übertragungsnetzes zum Einsatz

kommen. Es ist sehr wahrscheinlich, dass ELECTRUM auch Zugang zu entsprechenden Materialien und Geräten besitzt, um die passende Schadsoftware zu programmieren und zu testen /ESE17r01/. Seit dem Cyberangriff mit Crashoverride auf das ukrainische Stromnetz 2016, ist ELECTRUM vorerst nicht wieder öffentlich in Erscheinung getreten. Die APT-Gruppierung ELECTRUM steht nach Einschätzung der Analysten in direkter Verbindung mit der APT-Gruppierung Sandworm /DRA20r01/.

2.10.7 Erythrite/SolarMarker

Übersicht

Die APT-Gruppierung Erythrite ist seit mindestens Mai 2020 bekannt. Die Aktivitäten von Erythrite zielen vor allem auf die Vergiftung von Suchmaschinen[3] (Suchmaschinen-Poisoning) und den Einsatz von Malware zum Diebstahl von Zugangsdaten und sensiblen Informationen ab. Die von Erythrite eingesetzte Malware wird im Rahmen eines schnellen Entwicklungszyklus ständig neu kompiliert, um einer Erkennung durch den Virenschutz angegriffener Endgeräte zu entgehen. Ein weiteres Ziel ist der Fernzugriff auf OT-Umgebungen. Die Cyberangriffe von Erythrite richten sich vor allem gegen Unternehmen in den USA und Kanada, wobei Angriffe auf die OT-Umgebung eines Fortune-500-Unternehmens sowie auf IT-Netzwerke von Stromversorgungsunternehmen, Lebensmittel- und Getränkeherstellern, Automobilherstellern, IT-Dienstleistern, Öl- und Erdgasunternehmen sowie einem Unternehmen zur Verwaltung elektronischer Verträge und Dokumente (mehrere hundert Millionen Nutzer weltweit) bekannt sind. Schätzungen zufolge waren im Jahr 2021 etwa 20 % der Fortune-500-Unternehmen durch die Angriffe von Erythrite gefährdet. Die Aktivitäten von Erythrite deuten auf einen Sitz der Organisation in Russland hin, wobei Reverse Proxys in Nordamerika und Europa genutzt werden. /DRA22w02, ASI22w01, IND22w01, DRA23w01/

[3] Angriffsmethode, bei der bösartige Webseiten erstellt werden und Taktiken zur Suchmaschinenoptimierung angewendet werden, damit diese bösartigen Webseiten bei Suchen an prominenter Stelle erscheinen

Weitere Bezeichnung

Die von Erythrite genutzte Vorgehensweise hat Überschneidungen zur Gruppierung SolarMarker, wobei keine klare Aussage getroffen werden kann, ob es sich um ein und dieselbe Gruppierung handelt oder ob es zwei unterschiedliche Gruppierungen sind. /DRA22w02, IND22w01, DRA23w01/

Aktivitäten

Erythrite ist seit mindestens Mai 2020 aktiv und nutzt eine für den Fernzugriff konzipierte Malware, die entwickelt wurde, um der Erkennung durch Virenscanner in Endgeräten zu umgehen. /DRA22w02, DRA23w01/

Die Aktivitäten von Erythrite haben Stufe 2 der ICS-Cyber-Kill-Chain erreicht. Dies bedeutet, dass die Angreifer direkten Zugang zu Netzwerken erlangt haben und dass sie bereit sind, Zeit, Mühe und Ressourcen darauf zu verwenden, ICS-Umgebungen anzugreifen, zu kompromittieren und Informationen für zukünftige Zwecke zu sammeln. /ASI22w01, IND22w01/

Bei seinen Cyberangriffen nutzt Erythrite legitime Webseiten, die zur Verbreitung von Malware kompromittiert werden. Dabei werden speziell gestaltete pdf-Dokumente auf ansonsten legitime Webseiten hochgeladen. Diese pdf-Dokumente sind mit Webseiten zur Verbreitung von Malware verlinkt. Zum Hochladen der pdf-Dokumente wird das WordPress-Plugin „Formidable Forms“ verwendet, wobei große Mengen maliziöser pdf-Dateien hochgeladen werden, die mit tausenden von Schlüsselworten versehen sind. Diese Schlüsselworte wurden für das Crawling durch Suchmaschinen mittels Methoden wie Cloaking[4] oder Link Farming[5] optimiert, um den Seitenrang der manipulierten Webseiten bei einer Suche zu erhöhen. Außerdem wurde eine große Menge weiterer Webseiten kompromittiert oder neu erstellt und mit Links versehen, die auf die maliziösen pdf-Dokumente verweisen. /DRA22w02, ASI22w01, DRA 23w01/

---

[4] Technik zur Suchmaschinenoptimierung, bei welcher den Suchmaschinen eine andere Seite präsentiert wird als dem Besucher (trotz selber URL), um gleichzeitig eine für Suchmaschinen und Besucher optimierte Seite zu präsentieren

[5] Technik zur Suchmaschinenoptimierung, bei welcher eine Webseite durch gegenseitige Verlinkung mit anderen Webseiten für Suchanfragen auf die ersten Plätze der Trefferliste gebracht werden soll

2.10.8 Kimsuky

Übersicht

Im Oktober 2020 wurde von der Cybersecurity and Infrastructure Security Agency (CISA), dem Federal Bureau of Investigation (FBI) und der U.S. Cyber Command Cyber National Mission Force (CNMF) der USA ein Warnhinweis in Bezug auf die nordkoreanische APT-Gruppierung Kimsuky veröffentlicht /CIS20i02/. Diese Gruppierung operiert weltweit, mutmaßlich bereits seit 2012, im Auftrag der nordkoreanischen Regierung in Verbindung mit dem nordkoreanischen Nachrichtendienst (Reconnaissance General Bureau, RGB). Hauptsächlich standen dabei Organisationen und Individuen in Südkorea, Japan und den USA im Fokus der Gruppierung, die sich auf die Beschaffung spezifischer und vertraulicher Informationen spezialisiert hat. Kimsuky konzentriert die Aktivitäten nach Angaben der CISA-Meldung neben Think Tanks und der Kryptowährungsindustrie auf südkoreanische Regierungs- und Militäreinrichtungen, außenpolitische und nationale Sicherheitsfragen im Zusammenhang mit der koreanischen Halbinsel, sowie auf die Nuklearindustrie.

Darüber hinaus veröffentlichten das Bundesamt für Verfassungsschutz (BfV) und der National Intelligence Service der Republik Korea (NIS) im März 2023 einen gemeinsamen Sicherheitshinweis im Zusammenhang mit Kimsuky, um auf eine Cyberspionagekampagne aufmerksam zu machen. Die jüngeren Aktivitäten der Gruppierung zeichnen sich demnach durch den Missbrauch von Googles Browser Chromium sowie maliziösen Android Play-Store Apps aus, die gegen Forscher zum innerkoreanischen Konflikt eingesetzt werden. /BFV23r01/

Weitere Bezeichnungen

Die Gruppierung ist auch bekannt als Velvet Chollima, Black Banshee, Thallium, G0086, APT43, ARCHIPELAGO oder Operation Stolen Pencil.

Aktivitäten

Die Gruppierung nutzt typischerweise zur Erlangung des initialen Zugriffs auf das Netzwerk des Opfers neben Phishing-E-Mails mit Login-Sicherheitswarnungen und Watering-Hole-Angriffen überwiegend Spear-Phishing-Techniken, bei denen E-Mails mit schadsoftwarebehaftetem Anhang gezielt an Personen oder Organisationen versendet

werden. Dazu werden teilweise auch Ziele außerhalb der eigentlichen Zielgruppe angegriffen, um Schadsoftware auf Subdomains zu platzieren, die legitime Website und Dienste wie beispielsweise Google oder Yahoo-Mail imitieren, um an Zugangsdaten zu gelangen. Außerdem agierte die Gruppierung, um das Vertrauen Ihrer Zielpersonen zu erlangen, in einigen Fällen zunächst über die Kontaktaufnahme via E-Mail ohne Schadsoftwareanhang, wobei eine falsche Identität vorgegeben wurde, bevor weitere E-Mails mit schadsoftwarebehaftetem Anhang oder entsprechende Links gesendet wurden /CIS20i02/. Dabei sind die Spear-Phishing-Angriffe jeweils auf für die Zielperson relevante Themengebiete, wie das nordkoreanische Atomprogramm, Medienanfragen oder aktuell auch die COVID-19-Pandemie /MAL20w01/ ausgerichtet.

Nach der Erlangung des initialen Zugriffs setzt Kimsuky unter anderem die erstmals im November 2018 beobachtete, auf Microsoft Visual Basic skriptbasierte Malware Babyshark ein. Durch diese wird u. a. zusätzlicher Schadsoftwarecode heruntergeladen und Informationen über das System gesammelt. Weitere typischerweise verwendete Schadsoftwarekomponenten sind AppleSeed, Meterpreter und VNC-Malware. /ASE23w01/ Unter Ausnutzung verschiedener Exploits erfolgen die Rechteausweitung und Aktionen zur Umgehung von Schutzmaßnahmen des Systems /TAR13w01/, unter anderem mit Hilfe des open-source Metasploit-Framework /GIT21f01/, einem Werkzeug zur Entwicklung und Ausführung von Exploits. Im Fokus der Gruppierung liegt insgesamt hauptsächlich die Informationsbeschaffung im Rahmen von oftmals langanhaltenden Spionagekampagnen, bei denen entsprechend Maßnahmen ergriffen werden, um die Aktionen zu verschleiern und das Risiko einer Entdeckung zu minimieren.

Im Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines Cyberangriffs wurde, bei dem Informationen in Form von Mitarbeiterdaten und Bauplänen von Kernkraftwerken gestohlen wurden /TRE14w01/. Die Angreifer verwendeten dabei Techniken, die mit dem Angriffsmuster von Kimsuky übereinstimmen. So wurden etwa 6000 E-Mails mit schadsoftwarebehaftetem Anhang an über 3500 Mitarbeiter der Korea Hydro & Nuclear Power Co. gesendet, wobei acht Computer mit Malware infiziert wurden /KIM19r01/. Die Staatsanwaltschaft in Seoul vermutet, dass die Gruppierung Kimsuky für den Angriff verantwortlich ist /PAR15w01/. Nach Informationen des auf Cybersecurity spezialisierten Unternehmens Cyberreason, welches u. a. nordkoreanische Akteure im Bereich IT-Sicherheit beobachtet, hat die Gruppierung ihr Zielgebiet in den vergangenen Jahren zudem neben den USA und dem asiatischen Raum nach Russland und Europa

ausgeweitet, wobei insbesondere staatliche Organisationen, nicht-staatliche Forschungsorganisationen, der Sicherheitsrat der Vereinten Nationen und neuerdings auch Organisationen aus dem pharmazeutischen Bereich, die an Impfstoffen und Medikamenten im Zusammenhang der COVID-19-Pandemie arbeiten, im Fokus stehen /CYB20w01/.

Nach Informationen aus dem September 2020 führte Kimsuky Spear-Phishing-Aktivitäten durch, um 28 Vertreter der Vereinten Nationen, darunter mindestens 11 Vertreter des Sicherheitsrats der Vereinten Nationen, die sechs Mitgliedstaaten des Sicherheitsrats repräsentieren, zu kompromittieren. Die Aktivitäten wurden zwischen März und April 2020 durchgeführt und beinhaltete eine Serie von Spear-Phishing-Angriffen abzielend auf Google Mail-Accounts der UN-Vertreter. Die verwendeten E-Mails wurden derartig gestaltet, dass sie den Eindruck erweckten, es handele sich um Interview-Anfragen von Reportern oder UN-Sicherheitswarnungen. Dadurch sollten die UN-Vertreter dazu gebracht werden, entsprechend präparierte Internetseiten aufzurufen bzw. Schadsoftware auf ihr System herunterzuladen. Die Angriffe wurden zudem auf Regierungsmitarbeiter eines der Mitgliedstaaten des Sicherheitsrats der Vereinten Nationen durchgeführt. /ZDN20w03/

Im Juni 2021 wurde bekannt, dass es einen Monat zuvor einen Cyberangriff aus Nordkorea auf eine südkoreanische Forschungsorganisation für Nuklearenergie gab. Dabei wurden nach Angaben eines Abgeordneten aus Südkorea möglicherweise Technologieinformationen gestohlen. Ziel des Angriffs war demnach das Korea Atomic Energy Research Institute, welches sich mit Forschungen und Fragestellungen zur Kernenergie beschäftigt. Die im Zusammenhang dieses Angriffs beobachteten IP-Adressen werden mit der Gruppierung Kimsuky in Verbindung gebracht. /NIK21w01/

Nach einer Warnmeldung des BfV und NIS vom 20.03.2023 hat Kimsuky in den letzten Jahren gezielt deutsche und koreanische Einrichtungen mit Spear-Phishing E-Mails angegriffen. Im Rahmen von zwei kürzlich beobachteten Spionagekampagnen missbrauchte die Gruppierung unter anderem Webbrowser Erweiterungen von Googles Browser Chromium, wobei Zielpersonen durch Spear-Phishing-E-Mails zur Installation von maliziösen Erweiterungen verleitet und damit Anmeldeinformationen für E-Mail-Konten abgegriffen wurden. Somit erlangten die Angreifer unbemerkt Zugriff auf die Inhalte des E-Mail-Postfachs des Opfers. In einem zweiten Schritt wird mit Hilfe der erbeuteten Anmeldeinformationen eine maliziöse App aus dem Google Play Store durch einen

Missbrauch der Synchronisierungsfunktion auf einem Android-Mobilgerät installiert, wodurch weitere Zugriffsmöglichkeiten für die Angreifer entstehen. /BFV23r01/

Im August 2023 wurde bekannt, dass Kimsuky über einen längeren Zeitraum eine Spionagekampagne durchgeführt hat, bei der Informationen von einer Organisation zur Kriegssimulation in Südkorea gesammelt wurden, die unter anderem im Zusammenhang mit einer jährlich stattfindenden gemeinsamen Militärübung der USA und Südkorea steht. Südkoreanische Auftragnehmer, die Verbindungen zum Zentrum für kombinierte Militärübungen zwischen Südkorea und den USA haben, erhielten im Rahmen einer (Spear)Phishing-Kampagne nach Angaben der Polizeibehörde der Provinz Gyeonggi Nambu in Südkorea maliziöse E-Mails. Militärische Informationen wurden nach derzeitigen Informationen nicht gestohlen. Ermittlungen der südkoreanischen Polizei und des US-Militärs ergaben, dass für den Cyberangriff unter anderem IP-Adressen verwendet wurden, die bereits im Jahr 2014 bei einem Cyberangriff auf ein südkoreanisches Kernkraftwerk verwendet wurden. /KOR23w01, REU23w01/

2.10.9 Kostovite

Übersicht

Im März 2021 veröffentlichten Sicherheitsforscher des Unternehmens Dragos einen Bericht zu drei von ihnen neu entdeckten APTs mit Bezügen zu Cyberangriffen auf industrielle Steuerungssysteme. Diese APT-Gruppierungen erhielten die Bezeichnung Kostovite, Petrovite und Erythrite. Kostovite erlangte hierbei im Jahr 2021 direkten Zugang zu den Netzwerken von industriellen Steuerungssystemen eines Wartungs- und Betreiberunternehmens für Wind- und Solarkraftanlagen. /DRA21r01/

Weitere Bezeichnungen

Es sind keine weiteren Bezeichnungen bekannt. Es ist nach aktuellem Stand unbekannt, ob Kostovite eine eigenständige APT-Gruppierung ist oder ob die Kostovite attribuierten Cyberangriffe von einer bereits bekannten APT-Gruppierung ausgeführt wurden.

Aktivitäten

Die Kostovite genannte Gruppierung wurde erstmalig im Jahr 2021 beschrieben und zeichnete sich durch tiefgreifenden Zugriff auf die Netzwerke von industriellen

Steuerungssystemen eines Wartungs- und Betreiberunternehmens im Bereich der erneuerbaren Energien aus. Hierbei nutzte Kostovite eine bis dahin unbekannte Schwachstelle der Pulse Connect Secure (siehe Abschnitt B.14.12) um erstmaligen Netzwerkzugriff auf die IT-Netze des betroffenen Unternehmens zu erhalten. Von hier aus eignete sich Kostovite legitime Accountdetails an, um schrittweise im Netzwerk tiefergehende Zugriffe zu erhalten. Schließlich erlangte Kostovite Zugriff auf mehrere leittechnische Systeme und Netzwerke der Kunden des betroffenen Unternehmens. Es wurde bis zur Entdeckung der Zugriffe kein direkter Schaden durch Kostovite verursacht, obwohl der Netzwerkzugriff zur Abschaltung von Anlagen hätte genutzt werden können. Die Datenlage deutet darauf hin, dass Kostovite ein Interesse am langfristigen Netzwerkzugang und dem Erlangen von Daten und Informationen hatte. Kostovite hatte mindestens einen Monat lang unerkannten Zugriff auf das leittechnische Netzwerk des betroffenen Unternehmens. /DRA21r01/

2.10.10 REvil

Übersicht

Bei der APT-Gruppierung REvil handelte es sich um eine der finanziell profitabelsten Ransomware- und Ransomware-as-a-Service Gruppierungen weltweilt mit jährlichen Umsätzen im Bereich von 100 Millionen US-Dollar, die im Wesentlichen von 2019 bis 2021 agierte. Mutmaßlich handelte es sich um eine aus Russland heraus agierende Gruppierung, die sich nach dem Ende der Aktivitäten der APT-Gruppierung GandCrab und möglicherweise aus Mitgliedern dieser Gruppierung gebildet hat. Die eingesetzte Schadsoftware fragt unter anderem die Spracheinstellungen des infizierten Systems ab und wird bei Benutzern mit russischer Spracheinstellung nicht aktiv. Nach der Verschlüsselung der Daten im Falle eines erfolgreichen Angriffs stellt die Gruppierung bzw. der Auftraggeber eine Lösegeldforderung und droht mit der Veröffentlichung von Informationen im Falle der Verweigerung einer Zahlung der Opfer. Wenn die Betroffenen daraufhin weiterhin nicht der Lösegeldforderung nachkommen, startet die Gruppierung typischerweise im dritten Schritt Distributed-Denial-of-Service-Angriffe auf deren Kunden und Geschäftspartner. Im November 2021 gelang es dem US-Justizministerium, mehrere Partner des REvil-Netzes zu verhaften und rund sechs Millionen Dollar an erbeuteten Lösegeldern zu beschlagnahmen. Im Januar 2022 nahmen der russische Inlandsgeheimdienst FSB und die russische Polizei nach eigenen Angaben auf Ersuchen von Behörden der Vereinigten Staaten 14 mutmaßliche REvil-Mitglieder fest und zerschlugen das Netzwerk. Im April 2022 veröffentlichte die Gruppierung auf ihrem Blog jedoch

Informationen über zwei neue Opfer und seitdem wurden weitere Angriffe bekannt, sodass davon auszugehen ist, dass die Gruppierung zumindest teilweise weiterhin aktiv ist. /MAL22w03, SEC22w11/

Weitere Bezeichnungen

Die APT-Gruppierung REvil ist auch unter den Namen Sodinokibi, Sodin und BlueCrab bekannt. /SEC22w11/

Aktivitäten

Die Aktivitäten von REvil lassen sich bereits auf das Jahr 2019 zurückführen wobei insbesondere im Jahr 2021 mehrere Angriffe mutmaßlich durch die Gruppierung durchgeführt wurden, die weitreichende Auswirkungen hatten und international große Beachtung fanden. Zudem ist die Gruppierung bzw. Teile der Gruppierung nach zwischenzeitlichen Erfolgen von Ermittlungsbehörden Anfang des Jahres 2022 wenige Monate später weiterhin aktiv. Zu den Opfern gehören verschiedene Industriebereiche unter anderem im Fertigungsbereich, (IT-) Dienstleister aber auch Organisationen im Gesundheitswesen wie Krankenhäuser. Dabei wählt REvil bevorzugt Opfer aus, die potenziell sehr ertragsstark sind und hohe Lösegeldgewinne versprechen.

Zu den von REvil angegriffen Unternehmen zählt mutmaßlich der taiwanische Computerhersteller Acer, der am 14. März 2021 Opfer eines entsprechenden Ransomware-Angriffs wurde. Dabei wurde nicht nur das Verwaltungsnetz von Acer verschlüsselt, sondern auch vorher Daten gestohlen. Die Erpresser forderten 50 Millionen Dollar Lösegeld in Form der Kryptowährung Monero und drohten damit, ggf. die erbeuteten Daten zu veröffentlichen, sollte die Zahlung durch Acer nicht erfolgen. Möglicherweise nutzte REvil bei dem Angriff auf Acer die Schwachstelle ProxyLogon aus, die Teil der 2021 in Microsoft Exchange (siehe Abschnitt A.4.1 im Anhang) bekannt gewordenen Schwachstellen ist. Acer äußerte sich nicht zu dem Vorfall. /SPI21w01, HEI21w11/

Im Mai 2021 wurde einer der weltweit größten Fleischkonzerne, JBS, Opfer eines Ransomware-Angriffs von REvil (siehe Abschnitt B.13.10). Der Angriff betraf Betriebsstätten in den USA, Kanada und Australien. JBS war angesichts erheblicher Einschränkungen im Betriebsablauf gezwungen, einzelne Betriebsstätten temporär zu schließen. Der Konzern zahlte daraufhin 11 Millionen Dollar Lösegeld in Bitcoins und erhielt von der Gruppierung ein Tool zur Entschlüsselung der Daten. /BLE21w03/

Im Juli 2021 kam es zu einem IT-Sicherheitsvorfall, der weltweit erhebliche Auswirkungen hatte und durch einen Angriff von REvil auf den amerikanischen IT-Dienstleister Kaseya ausgelöst wurde (siehe Abschnitt B.13.4 im Anhang). Im Rahmen dieses Ransomware-Angriffs wurde durch die Gruppierung ein schadsoftwarebehaftetes Softwareupdate der Remote-Monitoring und -Management-Tool-Software VSA erstellt und auf die Systeme der Kunden von Kaseya aufgespielt. So waren weltweit tausende Systeme von dem Angriff betroffen und wurden durch die Ransomware verschlüsselt. Die Lösegeldforderungen für die Entschlüsselung aller Daten beliefen sich auf etwa 70 Millionen Dollar. Nach Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) waren auch Unternehmen in Deutschland betroffen. Die Auswirkungen beschränkten sich nicht nur auf direkte Kunden von Kaseya, sondern auch auf Institutionen und Organisationen, deren IT-Dienstleister Kaseya-Produkte einsetzten. Dazu zählte beispielsweise die schwedische Supermarktkette Coop, die in der Folge am 3. Juli 2021 alle 800 Filialen schließen musste, da die Kassensysteme blockiert waren. /VAR21w01/

Obwohl es US-amerikanischen und russischen Behörden Ende 2021 bzw. Anfang 2022 vermeintlich gelang, Mitglieder der Gruppierung festzunehmen und zumindest Teile der Infrastruktur zu zerschlagen, gab es im Verlauf des Jahres 2022 weitere Cyberangriffe, bei denen mutmaßlich Teile der Ransomware von REvil verwendet wurden. So wird REvil beispielsweise in Verbindung mit den Angriffen auf das zweitgrößte Öl- und Gasunternehmen Indiens, Oil India und den französischen Werbe- und Lichtspezialist Visotec gebracht. Außerdem wird vermutet, dass die Gruppierung für Angriffe auf die Stratfort University und die chinesische Midea Group, ein Hersteller für Klimaanlagen, Lüftungs- und Heizgeräte sowie elektrische Haushaltsgeräte mit Umsätzen im zweistelligen Milliardenbereich, verantwortlich ist. Im August 2022 wurde das französische Rüstungsunternehmen Nexeya Opfer eines erheblichen Datendiebstahls und einer weitreichenden Verschlüsselung von Daten mutmaßlich durch REvil. Das Unternehmen stellt unter anderem Rüstungsgüter und elektronische Komponenten wie Sensoren und Radaranlagen her, die möglicherweise im aktuellen Krieg der Ukraine mit Russland zum Einsatz kommen. Zudem gibt es seit April 2022 Hinweise darauf, dass Teile der REvil-Ransomware bei neueren Angriffen eingesetzt wurden und dass die ursprünglichen Entwickler der Ransomware direkt beteiligt sind. /BLE22w08, CYB22w02, HEI22w12,0 TND22w01/

Ab Dezember 2021 wurden Aktivitäten einer „Ransom Cartel“ genannten neuen Gruppierung beobachtet, die Organisationen überwiegend in Frankreich und den USA in den Bereichen Bildung, Fertigung sowie Energie und Versorgung angegriffen hat und

gewisse Ähnlichkeiten und technische Überschneidungen mit REvil-Ransomware aufweist. Somit ist davon auszugehen, dass es Verbindungen zwischen den Mitgliedern von REvil und Ransom Cartel gibt bzw. in der Vergangenheit gegeben hat. Ransom Cartel bietet wie REvil ihre Dienste als Ransomware-as-a-Service an. Neben der Verschlüsselung von Daten werden gestohlene Daten außerdem veröffentlicht und an Partner oder Mitbewerber der Opfer gesendet, um deren Ruf weiter zu schädigen. Den initialen Zugriff auf Opfernetzwerke erlangt die Gruppierung überwiegend über kompromittierte Anmeldeinformationen von externen Remote-Diensten, dem Remote Desktop Protokoll sowie Virtual Private Networks (VPNs). /ZDN22w06/

2.10.11 Sandworm

Übersicht

Bei der APT-Gruppierung Sandworm handelt es sich um die Militäreinheit 74455 des russischen, militärischen Geheimdienstes GRU /BID20w01, ESE22w02, FDD20w01, WIR19w01/, die ihre Aktivitäten bereits 2009 aufnahm /INT20r01/. Sie ist an kritischen Infrastrukturen in Europa und den USA interessiert, wobei sie klassische, strategische Cyber-Spionage betreibt. Darüber hinaus ist die Gruppierung auf Cyberangriffe auf industrielle Steuerungssysteme spezialisiert. Aktionen von Sandworm wurden zum ersten Mal 2014 aufgedeckt, als die Schadsoftware Black Energy 2 gegen Telekommunikationsinfrastrukturen der EU und der NATO eingesetzt wurde /SOC20w01, UAG15r01/. Dabei fanden sich in der Schadsoftware BlackEnergy 2 codierte Referenzen zur Sciencefiction Serie Dune, weshalb der Gruppierung der Name Sandworm gegeben wurde /ZDN14w01/. Nach der Entdeckung ihrer Tätigkeiten 2014 trat die Gruppierung einige Monate lang nicht in Erscheinung bevor sie am 23.12.2015 /EWB20w01/ wieder einen viel beachteten Cyberangriff durchführte und mit der Schadsoftware Black Energy 3 (siehe Abschnitt B.7.1) einen Blackout im ukrainischen Stromnetz verursachte. /FIR16w01/

Weitere Bezeichnungen

Die APT-Gruppierung Sandworm ist auch unter den Namen Quedagh und BlackEnergy bzw. BlackEnergy Group, Voodoo Bear, TeleBots und Einheit 74455 bekannt. /BFV18r02, ESE22w02, STE22w01/

Aktivitäten

Sandworm war in den letzten Jahren sehr aktiv. Im Jahr 2016 entdeckten Sicherheitsforscher von ESET die Schadsoftware TeleBots, ein Nachfolger der Schadsoftware BlackEnergy. TeleBots zielte auf Finanzinstitute in der Ukraine ab. Benannt wurde die Schadsoftware nach der Programmierschnittstelle Telegram Bot, die von ihr verwendet wird, um die Kommunikation zwischen den Angreifern und den kompromittierten Computern zu tarnen. Die Angreifer richteten Telegram-Konten ein, von denen aus sie Befehle an die Geräte sendeten. Bei der letzten Stufe des Angriffs verwendete TeleBots Varianten der KillDisk-Ransomware, von denen eine Dateien mit zwei Zeichenfolgen überschrieb. Weiter Varianten der KillDisk-Ransomware waren in der Lage sowohl Windows- als auch Linux-Systeme zu verschlüsseln und deren Bootfähigkeit aufzuheben. Die Angreifer stellten eine Lösegeldforderung in Höhe von 222 Bitcoins (damals etwa 250000 US-Dollar) für die Datenwiederherstellung. /ESE22w02/

Ebenfalls im Jahr 2016 mischte sich APT28, eine andere GRU-Einheit, in den Wahlkampf zwischen Donald Trump und Hillary Clinton um die US-Präsidentschaft ein. Dabei führte APT28 einen Cyberangriff auf die Mietglieder von Clintons Wahlkampfteam, die Netzwerke des Demokratischen Kongress-Kampagnenkomitees und des Demokratischen Nationalkomitees durch. Es wurden Daten und E-Mails gestohlen. Sandworm unterstützte gezielt die anschließende Veröffentlichung der Daten und Dokumente. /ESE22w02/

Im Juni 2017 wurden immense Schäden mit der Schadsoftware NotPetya (siehe Abschnitt B.9.6) in Europa und den USA angerichtet, die ebenfalls dieser APT-Gruppierung zugerechnet wird. Zu den Opfern zählen zum Beispiel die Firmen Maersk und Merck. Am stärksten war jedoch die Ukraine mit 300 Firmen, 22 Banken, vier Krankenhäusern, mehreren Flughäfen und nahezu allen Regierungsbehörden betroffen. Ebenfalls im Jahr 2017 gelang es Sandworm, die Präsidentschaftswahlen in Frankreich zu beeinflussen. Über Phishing-Mails erhielt die Gruppierung Zugriff auf neun Gigabyte der E-Mails der Präsidentschaftskampagne von Emmanuel Macron. Im Oktober 2017 erfolgte eine globale Angriffswelle gegen Behörden und Unternehmen. Nach der Behörde für nationale Cybersecurity des Vereinigten Königreichs, dem National Cyber Security Center (NCSC), ist für die Angriffe vermutlich Sandworm verantwortlich. Die Angriffe richteten sich vor allem gegen Organisationen in der Ukraine und Russland. Betroffen waren die russische Nachrichtenagentur, die U-Bahn in Kiew und der Flughafen in Odessa.

Weitere Angriffsziele befanden sich in europäischen Staaten (darunter Deutschland), den USA und Japan. Ziel der Angriffe war die Datenverschlüsselung mit anschließender Lösegeldforderung. Im Herbst und Winter 2017 zielte Sandworm auf Südkorea und einige Unternehmen ab, die an den Olympischen Winterspielen in Pyeongchang 2018 beteiligt waren. Dabei infizierten sie einige in Südkorea beliebte Apps für Android-Mobiltelefone wie Transitplan-Apps, darunter auch eine App von Busfahrplänen, koreanische Sprach-Apps sowie Medien- und Finanzsoftware. Zwei Monate zuvor war dies auch mit einer Version der ukrainischen Mail-App Ukr.net geschehen. Die eingesetzte Schadsoftware konnte sich dann über die Android-Telefone verbreiten. /AIR17w01, NCS18i02, TRE17w02, WIR19w01, CSO19w01/

Im Frühjahr 2018 unternahm Sandworm Angriffe auf russische Unternehmen, darunter Unternehmen für Gewerbeimmobilien, Finanzinstitute und die Automotiveindustrie. Dagegen wurden im Herbst desselben Jahres hauptsächlich in der Ukraine Softwareentwickler und Entwickler für Mobiltelefonanwendungen von der Gruppierung attackiert. Im Oktober und November 2018 attackierte die Gruppe Android-Entwickler mit Phishing-Mails, welche infizierte Anhänge zur Auffindung von Schwachstellen in Microsoft Office und zur Etablierung der Schadsoftware Powershell Empire enthielten. Es gelang Sandworm den Entwickler einer App für ukrainische Geschichte zu kompromittieren. Seit 2018 kompromittiert Sandworm ukrainische Webseiten von religiösen Organisationen, der Regierung, Sport und Medien, wodurch Nutzer von diesen Seiten direkt auf Phishing-Seiten weitergeleitet werden. 2018 und 2019 versuchte Sandworm in das Medien- und Regierungsnetz in Georgien einzugreifen. /CSO19w01, IRN20w01, WIR19w01/

Im Februar 2022 wurde bekannt, dass Sandworm seit 2019 Router des Herstellers Watchguard mit der Schadsoftware Cyclops Blink infiziert. Die Schadsoftware wird für den Datendiebstahl aus dem Netzwerk genutzt. Sie kann den Router aber auch zum Teil eines Botnetzes machen und ihn für Angriffe auf andere Ziele nutzen. Zusätzlich kapert Cyclops Blink den Update-Prozess, so dass es einen Neustart des Routers übersteht. Eine Übertragung der Schadsoftware auf Router anderer Hersteller kann nicht ausgeschlossen werden, ist aber bis jetzt noch nicht beobachtet worden. /STE22w01/

Im Zuge der russischen Invasion der Ukraine wurde im April 2022 von Sandworm mit der Schadsoftware Industroyer 2 ein Cyberangriff gegen das ukrainische Stromnetz durchgeführt. Der Angriff wurde jedoch nach ukrainischen Angaben rechtzeitig entdeckt und Schäden konnten verhindert werden.

Die Schadsoftwarekomponente Industroyer2 basiert auf der Schadsoftware Industroyer/Crashoverride, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert. /BSI22i03, BSI22i04, ESE22w01, MAN22w02/

Zwischen 2022 und 2023 hat Sandworm versucht über fünf verschiedene Wiper mit Namen CaddyWiper, ZeroWipe, SDelete, AwfulShred und BidSwipe die ukrainische Nachrichtenagentur Ukrinform anzugreifen, um deren Datensysteme zu löschen bzw. zu überschreiben. Das ukrainische Computer Emergency Response Team (CERT-UA) gab an, dass der Cyberangriff nur teilweise erfolgreich war und den Betrieb von Ukrinform nicht beeinträchtigt hat. Im Januar 2023 entdeckte ESET einen weiteren Cyberangriff, bei dem Sandworm einen zusätzlichen Wiper mit Namen SwiftSlicer gegen eine unbekannte ukrainische Organisation eingesetzt hatte. /DAR23w02/

Ebenfalls im Jahr 2023 nutzte Sandworm kompromittierte VPN-Zugangsdaten, um Zugriff auf öffentliche Netzwerke in der Ukraine zu erhalten. Mithilfe des BAT-Skripts mit Namen RoarBat kundschafteten die Angreifer die Netzwerke nach Dateien mit spezifischen Dateiendungen aus und archivierten diese mit dem legitimen WinRAR-Programm. /SEA23w01/

Sandworm führte im August 2023 Cyberangriffe mit der Schadsoftwarefamilie Infamous Chisel auf militärische Ziele der Ukraine durch. Die Schadsoftware zielte auf die Android-Mobiltelefone von Militärangehörigen ab, um diese zu kompromittieren und auszuspionieren. Auf diese Weise wollten die Angreifer an Informationen wie Truppenpositionen, -bewegungen und deren technischen Ausrüstung gelangen. Der Security Service of Ukraine (SBU) gab an, dass es ihm in Zusammenarbeit mit dem ukrainischen Militär gelungen ist den Diebstahl sensibler Daten zu verhindern. /COW23w02/

Nach Informationen der NSA /NSA20i01/ nutzt die Gruppierung mindestens seit August 2019 eine Schwachstelle im Exim Mail Transfer Agent (MTA) aus. Exim wird häufig in Unix-Systemen verwendet und ist in manchen Linux-Systemen vorinstalliert. Mit Hilfe der Schwachstelle kann ein nicht authentifizierter Angreifer eine spezielle E-Mail senden, über die er verschiedene Aktionen wie die Installation von Programmen, die Modifikation von Daten und die Erstellung neuer Accounts durchführen kann. So können die Angreifer ihre eigenen privilegierten Nutzer zum E-Mail-Server hinzufügen, Sicherheitseinstellungen des Netzwerks deaktivieren, ihren Nutzern mehr Rechte für den Fernzugriff einräumen und ein Skript ausführen, welches weitere Schritte zur Ausspionierung des

Netzwerks ermöglicht. Die infizierten Server dienen als Ausgangspunkt für das weitere Vordringen in andere Netzwerkbereiche. Die Zielobjekte der Angreifer wurden von der NSA allerdings nicht bekannt gegeben. /NSA20i01, WIR20w01/

2.10.12 Tonto Team

Übersicht

Am 22. Oktober 2020 wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Cyber-Sicherheitswarnung bezüglich möglicher Supply-Chain-Angriffe durch die APT-Gruppierung Tonto Team ausgegeben /BSI20i05/. Diese mutmaßlich der chinesischen Regierung nahestehende Gruppierung ist bereits seit über zehn Jahren für Cyberangriffe auf militärische, diplomatische und infrastrukturelle Ziele überwiegend in Osteuropa (Russland) und Asien (Japan, Südkorea) bekannt. Seit Anfang des letzten Jahres wurden außerdem Cyberangriffe auf Organisationen in Australien, Bangladesch, Indien, den USA und auch Deutschland entdeckt. Dabei standen neben Regierungsorganisationen außerdem Ziele aus dem Energie-, Finanz-, Gesundheits- und IT-Sektor im Vordergrund. Die aktuellen Informationen der Sicherheitswarnung des BSI geben Hinweise auf Angriffsversuche auf spezialisierte IT-Dienstleister, deren Hauptkunden im Finanzsektor angesiedelt sind.

Weitere Bezeichnungen

Die Gruppierung ist auch bekannt unter den Namen Karma Panda, Red Beifang, Cactus Pete und Earth Akhlut.

Aktivitäten

Dem BSI ist ein Vorfall bekannt, bei dem ein nicht näher genanntes Unternehmen angegriffen wurde, das Software für das Handeln und Verwalten von Wertpapieren entwickelt und für solche Systeme Unterstützungsdienstleistungen anbietet. Dabei wurde mutmaßlich der Remote Access Trojaner (RAT) Bisonal verwendet. Diese Schadsoftware ist bereits seit über zehn Jahren bekannt und wurde im Laufe der Zeit angepasst, um eine Erkennung zu vermeiden /MER20w01/. Neben eigener Schadsoftware verwendet die Gruppierung auch diverse Schadprogramme, die von mehreren weiteren APT-Gruppierungen gemeinsam genutzt werden. Neben dem Ausspähen von Informationen gehören auch der Up- und Download von Dateien, sowie das Ausführen von

Kommandozeilen-Befehlen zu den Funktionalitäten der verwendeten Schadsoftware. Ein Beispiel ist die Nutzung der Schadsoftware ShadowPad, die u. a. bei einem Supply-Chain-Angriff auf das südkoreanische Server-Management Unternehmen NetSarang im Jahr 2017 verwendet wurde.

Die Gruppierung nutzt verschiedene Angriffsvektoren zur Erlangung des initialen Zugriffs in das Netzwerk ihrer Ziele. Überwiegend werden die Angriffe mit dem Versand von E-Mails eingeleitet, welche mit Schadsoftware behaftete Dokumente in ihrem Anhang beinhalten. Das sogenannte Spear-Phishing zielt im Gegensatz zum „normalen“ Phishing auf konkrete Unternehmen oder Organisationen ab, um nicht autorisierten Zugriff auf vertrauliche Daten und Systeme zu erlangen. Die Schadsoftware nutzt dabei verschiedene bekannte Schwachstellen aus. Außerdem versucht die Gruppierung durch das Kopieren von Anmeldeformularen legitimer Webmail-Server und dem Ersetzen des Submit-Felds in den kopierten Formularen, Zugangsdaten zu erhalten, indem die auf den Phishing-Seiten eingegeben Zugangsdaten an einen Server geschickt werden, der unter der Kontrolle der Angreifer steht.

Nachdem die Angreifer über einen kompromittierten Rechner Zugang zu einem Netzwerk erlangt haben, versuchen sie diesen mit den in diesem Bereich üblichen Methoden weiter auszubreiten. Mittels Werkzeugen wie GsecDump werden Windows-Zugangsdaten aus dem Arbeitsspeicher gesammelt, um sich auf weiteren Rechnern anzumelden und unter Ausnutzung von Schwachstellen werden die eigenen Benutzerrechte erhöht. Ggf. wird zur Ausbreitung im Netzwerk auch die bekannte Schwachstelle Eternal Blue verwendet, die u. a. beim Supply-Chain-Angriff NotPetya im Jahr 2017 verwendet wurde. /HOR20r01/

Im Juli 2022 wurden Informationen zu einer mutmaßlich von einer chinesischen Gruppierung initiierten Kampagne gegen russische Organisationen zur Informationsbeschaffung über Aktivitäten der russischen Regierung veröffentlicht. Hinter diesen Angriffen steht mutmaßlich die Gruppierung Tonto Team. Die Angreifer nutzten dabei vermeintliche behördliche Empfehlungen in Form von Rich Text Files (RTFs) aus, wobei diese mit Schadsoftware präpariert sind und die Opfer dazu bewegt werden sollen, die Dokumente zu öffnen und das Ausnutzen von Remote-Code-Execution-Sicherheitslücken in Microsoft Office zu ermöglichen. Die präparierten, in russischer Sprache formulierten Dokumente erweckten den Anschein, dass es sich um Sicherheitswarnungen handele. Sie gaben vor, Behörden und Infrastrukturanbieter vor potenziellen Angriffen zu warnen und auf die Einhaltung der russischen Gesetze hinzuweisen. Obwohl es in der Vergangenheit

bereits Angriffe von chinesischen Gruppierungen auf russische Organisationen und Behörden gab, hat die Intensität seit Beginn des russischen Angriffs auf die Ukraine stark zugenommen. /DAR22w01, SEN22w01/

Im Februar 2023 veröffentlichte der in Singapur ansässige IT-Dienstleister für Dienstleistungen und Beratungen zu Fragen der Cybersicherheit Group-IB Informationen über einen Cyberangriff auf ihre Systeme, der mutmaßlich von der Gruppierung Tonto Team ausgeführt wurde. Dabei wurden im Sommer 2022 gezielt Mitarbeiter der Organisation mit Hilfe von Phishing-Emails angegriffen. Die Angreifer gaben sich dabei als Mitarbeiter eines legitimen Unternehmens aus versendeten eine Datei im RTF-Format als Anhang, die Schadsoftware (unter anderem Komponenten der oben genannten Schadsoftware Bisonal) enthielt. Im Rahmen der Ermittlungen zu diesem Vorfall stellte Group-IB fest, dass es bereits ein Jahr zuvor im Sommer 2021 ähnliche Cyberangriffe durch die Gruppierung gegeben hat, die durch interne IT-Sicherheitsmaßnahmen vereitelt wurden. Auch wenn die bisherigen Angriffsversuche von Tonto Team auf Group-IB scheiterten, geht die Organisation davon aus, dass Cyberangriffe insbesondere auf IT-Dienstleister bzw. über die Lieferkette durch die Gruppierung im Rahmen ihrer Spionage- und Informationsbeschaffungskampagne zukünftig fortgeführt werden. Am 26.04.2023 veröffentlichten Forscher des südkoreanischen Unternehmens AhnLab Security Response Center (ASEC) Informationen über Cyberangriffe durch Tonto Team auf südkoreanische Organisationen aus dem Bereich Bildung und der Bau-Branche, sowie auf diplomatische und politische Institutionen. Dabei setzten die Angreifer unter anderem eine Datei im Zusammenhang mit Anti-Malware-Produkten ein, um Angriffsschritte auszuführen. /ASE23w02, GRO23w01/

2.10.13 Turla

Übersicht

Die APT-Gruppierung Turla ist für Cyberangriffe zur Cyber-Spionage bekannt. Ziel von Turla ist es dabei, möglichst lange unentdeckt zu bleiben und Informationen zu sammeln. Hierbei setzt sie häufig Spear-Phishing-Angriffe (z. B. E-Mails mit maliziösen Anhängen oder Links), Watering-Hole-Attacken und Living-off-the-Land-Techniken ein. Außerdem ist Turla dafür bekannt, sich über USB-Sticks verteilende Malware einzusetzen, um sich Zugang zu Zielen zu verschaffen. Dabei ist der von Turla entwickelte Code im Vergleich zu dem vieler anderer APT-Gruppierungen deutlich ausgefeilter, die Infrastruktur komplexer und die Ziele sorgfältiger ausgewählt. Damit versucht Turla, möglichst unentdeckt zu agieren und übermäßige öffentliche Aufmerksamkeit zu vermeiden. Die Cyberangriffe von Turla richten sich oftmals gegen diplomatische Ziele, wie beispielsweise die Botschaften von Belgien, der Ukraine, China, Jordanien, Griechenland, Kasachstan, Armenien, Polen und Deutschland. /MAL21w04/ Es wurden aber auch eine Reihe anderer Ziele wie Regierungsstellen, Militär, Bildung, Forschung, Einzelhandel sowie Medizin angegriffen. /MIT21w03/ Schwerpunkt der Angriffe von Turla in den letzten Jahren war die Ukraine, die Opfer von Turla befinden sich aber auf der ganzen Welt, wobei Länder in Europa, Asien und dem Nahen Osten besonders betroffen waren. Angegriffene Länder waren beispielsweise Frankreich, Rumänien. Kasachstan, Polen, Tadschikistan, Österreich, Russland, USA, Saudi-Arabien, Deutschland, Indien, Armenien, Belarus, Niederlande, Iran, Usbekistan und Irak. Die Aktivitäten von Turla deuten auf einen militärischen Geheimdienst hin, der vermutlich in Russland agiert. Es gibt Hinweise darauf, dass Turla mit dem russischen Geheimdienst FSB in Verbindung steht. /HEI20w02, BAY22w01 SOC23w01/

Nach Angaben des US-Justizministeriums gelang es Mitarbeitern der US-Bundespolizei FBI, die von Turla eingesetzte Spionagesoftware Snake auszuschalten. Dazu wurde ein vom FBI geschriebener Code eingeschleust. Dieser Code soll Snake den Befehl gegeben haben, sich selbst zu überschreiben. /ZEI23w01/

Weitere Bezeichnungen

Turla ist ebenso unter den Namen Group 88, Belugasturgeon, Waterbug, Venomous Bear, Snake, Krypton, Wraith, Pfinet, TAG_0530, CTG-8875, ATK 13, ITG12, Hippo Team, Pacifier APT, Popeye, SIG2, SIG15, SIG23, Secret Blizzard, Iron Hunter,

Makersmark, UAC-0003, UNC4210 und Uroburos bekannt. Im Zusammenhang mit Turla fällt auch immer wieder der Name WhiteBear, wobei noch nicht klar ist, ob es sich bei WhiteBear und Turla um ein und dieselbe Gruppierung handelt. /CER21w01, MIT21w03, MAL21w04, SOC23w01, HEL23w01/

Aktivitäten

Turla ist seit mindestens 2004, vermutlich eher seit den späten 1990er Jahren, aktiv. Im Jahr 2008 ließ die APT-Gruppierung auf einer Militärbasis im Nahen Osten USB-Sticks auf Parkplätzen verteilen, auf welchen sich eine Schadsoftware befand. Mindestens ein Soldat hat einen solchen USB-Stick an einen Rechner angeschlossen, woraufhin sich die Schadsoftware installiert hat.

Dadurch gelang es Turla, dass normalerweise vom Internet getrennte Netz des US-Militärs zu infiltrieren, in welchem die Kriegseinsätze in Afghanistan und im Irak koordiniert wurden. Weltweite Aufmerksamkeit erlangte die APT-Gruppierung spätestens 2014 durch die unter dem Namen Epic Turla bekannt gewordenen Cyberangriffe (siehe Abschnitt 9.2.7.4 im Anhang). Turla ist auch dafür bekannt, immer wieder die Schadsoftwarekomponenten und Cyberangriffswerkzeuge sowie die Command-and-Control Infrastruktur anderer Angreifergruppierungen zu kapern und bei ihren eigenen Angriffen einzusetzen, wie beispielsweise 2019, als Turla Cyberangriffe auf britische Angriffsziele mit und über Angriffswerkzeuge und Infrastruktur der iranischen APT-Gruppierung APT34 (in diesem Bericht aufgrund der bisherigen Ausrichtung der Gruppierung nicht näher beschrieben) durchführte. Auch wurden 2019 weitere Angriffswerkzeuge von Turla bekannt. /SYM19w01, BAY22w01, SOC23w01/

Wie Forscher der Sicherheitssoftware-Firma ESET entdeckt haben, nutzt Turla unter anderem die Windows-Malware „Crutch“, mit der Daten von infizierten Systemen kopiert und verschickt werden können. Dabei wird der Filehosting-Dienst „Dropbox“ genutzt. Die Daten werden dabei von „Crutch“ automatisch gesammelt und unter Verwendung der offiziellen Dropbox-Programmierschnittstelle an von Turla kontrollierte Dropbox-Konten geschickt. In der letzten Version von „Crutch“ sind dazu keine manuellen Befehle mehr notwendig, die Übermittlung der Daten erfolgt automatisch über das Tool „wget“. Die Nutzung von „Dropbox“ erfolgte vermutlich, da sich der Dropbox-Traffic unauffällig in den regulären Netzwerkverkehr einfügt und damit relativ wenig Aufmerksamkeit erregt. /ESE20w02, HEI20w02/

Im Jahr 2015 wurde entdeckt, dass Turla Satellitenkommunikation nutzt, um seine Malware zu steuern und Daten zu exfiltrieren. Um die Spur gestohlener Daten zu verschleiern, hat Turla durch das Fälschen der IP-Adresse eines legitimen Satelliten-Internet-Teilnehmers die Möglichkeit erlangt, Daten über einen Satelliten zu senden und mit einer Satellitenantenne, welche mit dem Turla Command and Control Server verbunden war, aufzufangen. /SOC23w01/

Im Jahr 2019 wurde ein Cyberangriff von Turla bekannt, bei dem ein Außerministerium in Osteuropa, eine diplomatische Einrichtung im Nahen Osten, eine Organisation in Brasilien und möglicherweise unentdeckt noch weitere Organisationen betroffen waren. Für diesen Angriff wurden legitime Funktionen von Microsoft-Exchange-Servern missbraucht, um Daten zu stehlen. Dazu wurde von Turla ein Transport Agent für Microsoft Exchange programmiert, der von der Sicherheitssoftware-Firma ESET LightNeuron genannt wurde. Dieser ist an zentraler Stelle im System installiert und kommt so mit allen ein- und ausgehenden E-Mails in Berührung. Somit kann der komplette E-Mail-Verkehr eines Ziels kontrolliert werden. Dabei können beispielsweise Spear-Phishing-Nachrichten verschickt werden, wobei der Absender legitim erscheint, Links in ausgehende E-Mails eingefügt werden, Betreffzeilen geändert und gestohlene Daten verschickt werden. LightNeuron lässt sich zur Ausführung dieser Aktionen durch Kommandos steuern, die per Steganografie in JPG- oder PDF-Dateien versteckt sind. Nach dem Auslesen der Kommandos werden die entsprechenden Mails von LightNeuron gelöscht, so dass diese nie bei einem tatsächlichen Empfänger ankommen. /SPI19w01/

Im Jahr 2023 wurden Angriffe von Turla bekannt, die mit E-Mails vermutlich kompromittierten UKR.NET-Konten begannen, welche Dokumente mit maliziösen Makros enthielten und den Download von Backdoor-Malware auslösten. Diese Malware stellt eine Verbindung zu den Command and Control Servern von Turla her, um Befehle abzurufen und Daten zu exfiltrieren. Turla verwendete außerdem Desired State Configuration (DSC), eine PowerShell-Funktion, mit der Administratoren die Konfiguration von Linux und Windows automatisieren können. Dabei wurde von DSC eine MOF-Datei (Managed Object Format) generiert, die ein PowerShell-Skript enthält, welches die eingebettete Nutzlast in den Speicher lädt und so einen legitimen Server in ein Malware-Command and Control-Zentrum verwandelt. /HEL23w01/

Laut Kaspersky nutzt Turla Tools, die darauf abzielen, das Erkennungsrisiko ihrer Malware zu minimieren. Beispielhaft genannt werden die JavaScript-Malware „KopiLuwak“ und der Dropper „Topinambour“. „Topinambour“ ist eine von Turla verwendete

„NET-Datei“, mit der die Malware „KopiLuwak“ in Angriffszielen unter Nutzung legitimer Softwareprogramme gestreut werden kann. Der Prozess zur Infektion der Angriffsziele beinhaltet dabei Funktionalitäten, die dazu dienen, eine Erkennung des Angriffs zu vermeiden. Beispielsweise verfügt die Command-and-Control-Infrastruktur über IPs, die gewöhnliche LAN-Adressen imitieren. „KopiLuwak“ ist in der Lage, die individuellen Spezifika infizierter Zielrechner zu analysieren, gespeicherte Informationen über System- und Netzwerkadapter zu sammeln, Daten zu stehlen sowie zusätzliche Malware herunterzuladen und auszuführen sowie Screenshots zu machen. /KAS19w02, DAT19w01/

Laut /SOC23w01/ nutzt die APT-Gruppierung Turla eine breite Palette selbst entwickelter Malware aber auch öffentlich verfügbarer Tools, um Schwachstellen auszunutzen und seine Ziele zu erreichen. Einige der Tools, die mit Turla in Verbindung gebracht werden, sind laut /SOC23w01/:

- Agent.btz: Wurm, der sich vor allem über Wechseldatenträger wie USB-Laufwerke verbreitet (verwendet für erwähnten Angriff auf US-Militärnetzwerk im Jahr 2008)
- ComRAT: neue Version von Agent.btz, ein Remote-Access-Trojaner, welcher die Gmail-Webschnittstelle für Befehls- und Steuerungsoperationen nutzt
- KopiLuwak: JacaScript-basiertes Programm zur Erleichterung der Befehls- und Kontrollkommunikation und zur Erstellung von Opferprofilen
- TunnusSched (QUIETCANARY): Backdoor zur Aufrechterhaltung von Persistenz und Kontrolle über kompromittierte Systeme; erlaubt es dem Angreifer, beliebige Befehle auszuführen
- Gazer: Für Ihre Stealth- und Persistenzfähigkeiten bekannte Backdoor; kommuniziert mit Befehls- und Kontrollserver über verschlüsselte Kanäle und kann mit verschiedenen Plugins angepasst werden, um ihre Funktionalität zu erweitern
- Carbon: modular aufgebautes Backdoor-Framework, welches für seine Peer-to-Peer-Fähigkeiten sowie seine Fähigkeit bekannt ist, die herkömmliche Command and Control Infrastruktur mit Aufgaben zu erweitern, die von legitimen Webdiensten bereitgestellt werden
- HyperStack: Backdoor für Remote Procedure Calls (Technik zur Realisierung von Interprozesskommunikation, welche den Aufruf von Funktionen in anderen Adressräumen (also in der Regel anderer Computer zur Funktionsausführung als zum Aufruf der Funktion) ermöglicht), welche Named Pipes zur Ausführung verwendet

- Kazuar: Fernverwaltungs-Trojaner, der Befehle über interne Knoten im Netzwerk des Opfers empfängt, aber auch in der Lage ist, Befehle über Server außerhalb des Opfernetzwerks zu empfangen

2.10.14 Xenotime

Übersicht

Xenotime wurde 2017 in Zusammenhang mit den Cyberangriffen mit der Schadsoftware Triton/TriSIS bekannt und gilt seither als eine der gefährlichsten APT-Gruppierungen weltweit. Ihr werden Verbindungen zu einem russischen Forschungsinstitut in Staatsbesitz zugeschrieben /FIR18w02/.

Weitere Bezeichnungen

Die APT-Gruppierung Xenotime wird auch unter dem Namen Temp.Veles geführt.

Aktivitäten

Die Aktivitäten von Xenotime konzentrieren sich auf kritische Infrastrukturen. Die APT-Gruppierung ist seit mindestens 2014 aktiv. Bekannt wurde Xenotime in Zusammenhang mit den Cyberangriffen mit der Schadsoftware Triton/TriSIS 2017. Seither gab es mehrere, häufig nicht näher beschriebene mit Triton/TriSIS in Verbindung stehende Cyberangriffe, welche ebenfalls Xenotime zugerechnet werden /FIR19w01/.

Xenotime fokussierte sich zunächst auf Angriffsziele im Öl- und Gassektor im Mittleren Osten, weitete ihre Aktivitäten aber Stück für Stück aus. 2018 berichteten IT-Sicherheitsunternehmen von Verletzungen der IT-Sicherheit bei einigen US-amerikanischen Unternehmen sowie Unternehmen im Mittleren Osten, die einen klaren Bezug zu kritischen Infrastrukturen aufweisen /CYB18w01/.

Das IT-Sicherheitsunternehmen Dragos berichtete im Juni 2019 über weitere Aktivitäten dieser APT-Gruppierung auch in Nordamerika und Europa /DRA19w01/. Zudem kompromittierte Xenotime laut Dragos auch mehrere Hersteller und Zulieferer von industriellen Steuerungssystemen, was als Vorbereitung für weitere Cyberangriffe über die Lieferkette gedeutet werden kann. Dragos berichtet weiterhin ab Ende 2018 von Spionage- und Aufklärungsaktivitäten im Bereich von US-amerikanischen Energieversorgungsunternehmen sowie Energieversorgungsunternehmen in der Asien-Pazifik Region. Hierbei wird ausdrücklich betont, dass es sich um eine Ausweitung der Aktivitäten von Xenotime und nicht um deren Verlagerung handelt /DRA19w01/

2.11 Killnet

Bei der Angreifergruppierung Killnet handelt es sich nicht um eine APT-Gruppierung im eigentlichen Sinn, da die Eigenschaften hochentwickelt und beharrlich zum derzeitigen Zeitpunkt noch nicht wirklich auf sie zutreffen. Bislang ist Killnet ausschließlich durch disruptive Angriffe aufgefallen. Killnet wird hier dennoch aufgrund ihrer ausgeprägten Aktivitäten im Jahr 2023 sowie ihrer eindeutigen politischen Motivation, die sich in ihrem Vor-gehen gegen Einrichtungen auch in Deutschland äußert, hier mit betrachtet.

Übersicht

Bei Killnet handelt es sich um eine prorussische Angreifer-Gruppierung, die sich aufgrund der wachsenden Spannungen zwischen Russland und der Ukraine formierte und im Januar 2022 erstmalig in Erscheinung trat. Seit Beginn des Krieges in der Ukraine fällt die Gruppierung regelmäßig durch prorussisch motivierte Cyberangriffe vornehmlich in Europa auf. Dabei greift sie zumeist zu DDoS-Angriffen, mit denen sie Webseiten, häufig von Regierungseinrichtungen, lahmlegt.

Killnet wirbt Mitglieder beispielsweise mit dem Versprechen an, dass diese einer Einberufung entgehen können /ZDF23w01/. Die Gruppierung hatte anfangs die Angriffe als Dienstleistung verkauft, veränderte aber ihr Geschäftsmodell mit Beginn des russischen Angriffs auf die Ukraine. Killnet hat sich im Dezember 2022 mit weiteren Hackergruppen, wie Anonymous Russia oder Mirai Botnet zusammengeschlossen. Auf einer gemeinsam gegründeten Onlineplattform werden Schadsoftware, Cyberdienstleistungen und Datenleaks verbreitet und gehandelt. Zudem wird sich über zukünftige Angriffsziele und Methoden ausgetauscht.

Es wird vermutet, dass sich Angehörige der Gruppierung Killnet mit weiteren Gruppierungen vernetzt haben, wie CyberArmy oder NoName057(16) /TAG23w01/.

In der zweiten Jahreshälfte 2022 und im Jahr 2023 bleibt Killnet weiterhin eine der aktivsten prorussischen Hacktivisten-Gruppierung und führt weitere zahlreiche Cyberangriffe durch. Diese Cyberangriffe beschränken sich weiterhin hauptsächlich auf DDoS-Angriffe, die vergleichsweise harmlose Störangriffe sind /BSI22w04/. Ziele von Killnet sind weiterhin Länder, die sich für die Ukraine oder gegen Russland aussprechen. Im Fokus liegen europäische Länder, wie Rumänien /ROM23w01, BSI22r17/, Moldawien /TYL22w01/, Tschechien /EXP22w01/, Italien /BSI22r17, TEC22w01/, Litauen /REU22w04, ARS22w01/, Norwegen /SPI22w03, BSI23r03/, Lettland /BSI22r17/, Estland /BSI22r17/, Georgien /TTOw01/, Großbritannien /BSI23r03/, COM23w01/ und Deutschland /SPIw03, BSI23r03/, aber auch die USA /BSI22r17, BSI23w03/ und Japan /REU22w05/.

Weitere Bezeichnungen

Die Gruppierung Killnet ist unter keinem weiteren Namen bekannt, kann jedoch aufgrund des Zusammenschließens mit anderen prorussischen Hacktivisten-Gruppierungen an Cyberangriffen beteiligt gewesen sein, die nicht explizit der Gruppierung Killnet zugerechnet wer-den. Zudem nennt sich der Anführer der Gruppierung KillMilk /BSI23r04/. Dieser versucht seit März 2023 eine private militärische Hacking Firma zu gründen namens „Black Skills“ /FLA23w01, SEC23w05/. Anzeichen für eine staatliche Finanzierung oder zur Einsatzfähigkeit gibt es nicht /GRE23w01/.

Aktivitäten

Die Killnet-Gruppierung ist spätestens seit Januar 2022 aktiv. Killnet führt hauptsächlich DDoS-Angriffe durch, ist mittlerweile aber auch durch die Veröffentlichung von Daten und Dokumenten bekannt. Es ist nicht genau bekannt, wie Killnet diese Daten und Dokumente erlangt hat, aber es wird vermutet, dass Malware-Angriffe verwendet wurden. Des Weiteren droht bzw. ruft Killnet zu Angriffen auf, die sich beispielsweise gegen verschiedene NATO-Einrichtungen /BSI23r04/ oder das SWIFT-Netzwerk /BLO23w01/ richten.

Ziel der durchgeführten oder angedrohten DDoS-Angriffe der Killnet-Gruppierung ist die Erreichbarkeit von Online-Präsenzen zu beeinträchtigen.

Beliebte Ziele sind Webseiten von unterschiedlichen Unternehmen, Internetseiten von verschiedenen Institutionen, wie die Webseite vom EU-Parlament /ZDF22w01/, sowie Angriffe auf zahlreiche Kranken-häuser /COM23w01, DFP23w01, BSI23r03/ in der EU (siehe Abschnitt B.15.12) oder Webseiten von Flughäfen /ZDF23w01, TAG23w01/. Teilweise werden Cyberangriffe von Killnet nach politischen Entscheidungen oder Äußerungen durchgeführt, wie beispielsweise nach der Zusage von Panzerlieferungen /ZDF23w02, HAN23w01, TAG23w01, CSO23w03/ an die Ukraine von Deutschland (siehe Abschnitt B.15.12) oder der Bezeichnung des EU-Parlaments von Russland als staatlicher Unterstützer von Terrorismus. Bei dem Cyberangriff auf die europäische Flugsicherungsbehörde Eurocontrol /CPO23w01, BLI23w01, CSO23w04/ im April 2023 kam es sogar zu physischen Auswirkungen (siehe Abschnitt B.15.11), da die Kommunikation von einigen Mitarbeitenden eingeschränkt war. Es ist zudem anzumerken, dass Deutschland sehr im Fokus der Cyberangriffe von Killnet steht, im Januar 2023 verbreitete die Gruppierung den Hashtag #DeutschlandRIP /HAN23w01, TAG23w01, CSO23w03/ in den sozialen Netzwerken, woraufhin diverse Ziele der Bundesrepublik angegriffen wurden. Die Cyberangriffe werden alle in Bezug auf den Angriff von der Ukraine durch Russland durchgeführt, aber die Ukraine selbst als Angriffsziel steht weniger im Fokus von der Gruppierung Killnet.

3 Zusammenfassung und Fazit

Die IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen, und damit auch die Situation, der die deutschen kerntechnischen Anlagen und Einrichtungen gegenüberstehen, entwickelt sich sehr dynamisch. Um ein vollständiges Bild zu erhalten, beobachtet die GRS diese IT-Bedrohungslage kontinuierlich und wertet die verschiedenen hierfür relevanten Aspekte, wie relevante Schwachstellen in industriellen Steuerungssystemen, Angriffswerkzeuge, Schadsoftwarekomponenten, IT-Sicherheitsvorfälle, IT-Angriffe, und Aktivitäten von Advanced Persistent Threats fortwährend aus. Das Gesamtbild, das sich im Rahmen dieses kontinuierlichen Screenings ergibt, macht Folgendes deutlich: Das Spektrum der Angriffswerkzeuge und Schadsoftwarekomponenten wird immer breiter und die einzelnen Werkzeuge ausgefeilter. Gleichzeitig wird die Angriffsoberfläche kontinuierlich größer, was nicht zuletzt am wachsenden Einsatz von programmierbaren und rechnerbasierten Komponenten, der zunehmenden Komplexität dieser Systeme und der zunehmenden Vernetzung von IT-Systemen sowie Schwachstellen in industriellen Steuerungssystemen aber auch in der restlichen IT-Infrastruktur liegt. Darüber hinaus spielen Lieferkettenaspekte wie Hersteller, Zulieferer, Wartung und Instandhaltung sowie Abhängigkeiten für die Angriffsoberfläche eine wichtige Rolle. Gleiches gilt für die zunehmende Auslagerung von sensiblen Informationen und Diensten beispielsweise zu Software-as-a-Service-Anbietern oder zu Security Operation Centres. Zusätzlich muss sowohl von einem wachsenden Feld an Angreifern als auch von einer steigenden Komplexität der Cyberangriffe ausgegangen werden.

Auch im Jahr 2023 war Ransomware der am häufigsten eingesetzte Schadsoftware-Typ. Dies gilt vermutlich auch dann noch, wenn man berücksichtigt, dass der Anteil der entdeckten und bekanntwerdenden Ransomware-Angriffe vergleichsweise hoch liegt, da eine Entdeckung bei einem Ransomware-Angriff Teil des Angriffsziels ist, während die Angreifer bei vielen anderen Cyberangriffen versuchen, einer Entdeckung zu entgehen. Gründe für den Boom bei Ransomware-Angriffen sind sowohl die starke finanzielle Motivation durch die zu erzielenden Lösegeldbeträge als auch die niederschwelligen Möglichkeiten zu ihrer Durchführung was Kenntnisse und Fähigkeiten anbelangt. Inzwischen lassen sich Ransomware-Angriffe durch Inanspruchnahme von Ransomware-as-a-Service-Lösungen auch weitgehend ohne eigene Fachkenntnisse ausführen. Trotz der häufig finanziell motivierten Ransomware Angriffe ist es wichtig zu beachten, dass nicht alle Ransomware Angriffe darauf abzielen, Geld zu erpressen und danach auch die verschlüsselten Daten wieder zu entschlüsseln. Immer häufiger ist zu beobachten, dass

Ransomware ähnlich wie Wiper Schadsoftware rein destruktiv eingesetzt wird, mit dem Ziel, die infizierten Systeme unbrauchbar zu machen. Ein weiterer, immer stärker zutage tretender Aspekt von Ransomware-Angriffen ist, dass sich die Erpressung meist nicht auf die Wiedererlangung der verschlüsselten Daten beschränkt, sondern sich zumeist auch auf eine angedrohte Veröffentlichung von im Zuge des Angriffs gestohlenen, sensiblen Daten beziehen. Darüber hinaus erstrecken sich die Drohungen der Angreifer häufig auch auf mögliche Angriffe auf den Kundenstamm eines Unternehmens. Ein in den letzten Monaten verstärkt beobachteter Trend zeigt zudem, dass besonders erfolgreiche Angreifergruppierungen mehr und mehr auch durch indirekte Miteinbeziehung von industriellen Steuerungssystemen und die Hervorrufung von Ausfällen bei verfahrenstechnischen Prozessen den Druck auf die betroffenen Unternehmen noch deutlich erhöhen. Dieser Aspekt wiegt bei Ransomware Angriffen auf Organisationen im Bereich der kritischen Infrastrukturen besonders schwer. Generell war in den vergangenen Monaten zu beobachten, dass mehr und mehr Ransomware-Angriffe auf IT-Dienstleister ausgeführt werden, was durch die meist große Zahl an über die Lieferkette indirekt betroffenen Kunden die Auswirkungen deutlich verstärkt. Sehr häufig wurden beispielsweise Ransomware-Angriffe auf Regierungs- und Verwaltungseinrichtungen beobachtet, was in nahezu allen Fällen signifikante Einschränkungen bei deren Fähigkeiten zur operativen Führung zur Folge hatte. Betroffen waren in den vergangenen Monaten und Jahren auch häufig deutsche Behörden auf Landes- oder Kommunalebene. Auf Basis der insgesamt beobachteten Ransomware-Angriffe entsteht der Eindruck, dass diese Art Angriff immer weniger nach dem Gießkannenprinzip durchgeführt wird, sondern die Angriffsziele deutlich sorgfältiger und unter dem Gesichtspunkt der Gewinnmaximierung ausgewählt werden. Zusätzlich ist anzumerken, dass Ransomware-Angriffe in vielen Fällen nur aufgrund der Mithilfe eines unwissentlich agierenden Innentäters erfolgreich sind.

Betrachtet man allgemein alle bekannt gewordenen Cyberangriffe, sind Angriffe unter Mithilfe eines unwissentlichen Innentäters deutlich häufiger als jeder andere Angriffsvektor. Dies liegt hauptsächlich da-ran, dass die Manipulation und Ausnutzung von Menschen häufig einfacher und ressourcenschonender zu bewerkstelligen ist als die Manipulation von Software und die Ausnutzung von Schwachstellen. Wesentlich ist dabei das Social Engineering, das insbesondere bei den ersten Angriffsschritten wie beispielsweise der Reconnaissance oder der Erlangung des Erstzugriffs, aber auch bei späteren Angriffsschritten beispielsweise zur Eskalation von Rechten stark eingesetzt wird.

Hierbei spielen neben der Recherche über öffentlich verfügbare Informationen wie beispielsweise Social Media Accounts von relevanten Personen insbesondere Spear Phishing Angriffe, Watering Hole Angriffe, Baiting, Pretexting, Piggybacking und alle Formen von Credential Harvesting eine große Rolle. Dies ist insbesondere als kritisch anzusehen, da hier auf Mitarbeiter abgezielt wird, die aufgrund von Unachtsamkeit oder durch mangelnde Vorsicht die Aushebelung oder Umgehung von Sicherheitsmaßnahmen ermöglichen können, sodass diese einem potenziellen Angriff nicht mehr oder nur noch unvollständig entgegenstehen. Grundsätzlich zielen viele Angriffstechniken, insbesondere bei den ersten Angriffsschritten auf die Arglosigkeit der Nutzer und den Mangel an Cybersicherheitsbewusstsein sowie das unzureichende Verständnis für die Vielzahl der Gefahren ab. Dies unterstreicht, wie essenziell eine Einbeziehung der Mitarbeiter in Sicherungsmaßnahmen und gezieltes Training im Hinblick auf potenzielle Angriffsversuche sind. Ein weiterer wichtiger Aspekt ist die Qualität des Social Engineering, d. h. in diesem Fall die Fähigkeit zur Täuschung der Opfer. Diese Qualität hat in den vergangenen Jahren bereits stark zugenommen, hat aber in den vergangenen Monaten durch den breiten Einsatz von KI eine neue Stufe erreicht. Es ist zu erwarten, dass der Einsatz von KI es künftig noch leichter machen wird, relevante Personen zu unwissentlichen Innentätern bei einem Cyberangriff zu machen, da Social Engineering immer ausgefeilter und stärker auf einzelne Personen zugeschnitten wird und gleichzeitig Täuschungen schwerer zu erkennen sind.

Ein weiterer Trend, der im vergangenen Jahr deutlich auszumachen war, ist die Zunahme schadsoftwarefreier Cyberangriffe, d. h. von Cyberangriffen, bei denen keine Schadsoftwarekomponenten eingebracht werden, sowie von Cyberangriffen, bei denen zumindest teilweise auf schadsoftwarefreie Techniken zurückgegriffen wurde. Hierzu zählen neben vielen Social Engineering Techniken auch sogenannte Living-off-the-Land-Techniken. Bei Living-off-the-Land nutzen die Angreifer bereits auf dem angegriffenen System vorhandene, legitime Programme, Funktionen oder Dienste missbräuchlich für ihre Zwecke. Da auf diese Art und Weise keine Schadsoftware eingebracht werden muss und die Kommunikation mit oder von den missbräuchlich eingesetzten Programmen zu-dem häufig wie legitime Kommunikation wirkt, ist dies mit einem deutlich geringeren „Fußabdruck“ verbunden als die Einbringung einer Schadsoftware, welche dieselben Zwecke erfüllt. Somit ist die Gefahr einer Detektion deutlich geringer. Der wesentliche Grund für die deutliche Zunahme derartig ausgeführter Angriffe ist daher auch der Fokus auf Detektionsevasion, der heutzutage bei vielen Cyberangriffen, insbesondere zu Spionagezwecken und strategischen Zwecken, sehr ausgeprägt vorhanden

ist. So gibt es inzwischen APT-Gruppierungen, die nahezu ausschließlich Living-off-the-Land-Techniken einsetzen und bei bereits seit Jahren agierenden APT-Gruppierungen ist ein zunehmen-der Einsatz von Living-off-the-Land-Techniken zu verzeichnen. Gerade die Kombination aus Social Engineering Techniken, um den Erstzugriff zu ermöglichen, und Living-off-the-Land-Techniken für weitere Angriffsschritte kann immer häufiger beobachtet werden.

Cyberangriffe auf und über die Lieferkette haben in den vergangenen Jahren stark an Be-deutung gewonnen. Solche Supply Chain Angriffe haben ein hohes Gefährdungspotenzial, da sie auf die in Bezug auf Sicherungsmaßnahmen schwächeren Glieder in der Lieferkette zielen und damit letztlich die Sicherungsmaßnahmen der eigentlich anvisierten Ziele, die selbst meist besser gegen Cyberangriffe geschützt sind, umgehen. Supply-Chain-Angriffe haben daher eine Art Bypasswirkung an den Sicherungsmaßnahmen der eigentlichen Angriffsziele vorbei. Neben gezielten Supply Chain Angriffen auf ausgewählte Kunden werden häufig auch Supply Chain Angriffe beobachtet, die aufgrund des Kundenkreises der betroffenen Hersteller bzw. Zulieferer oder Beratungs-, Wartungs- oder sonstige im Unterauftrag eingesetzte Unternehmen einen sehr hohen Verbreitungsgrad aufweisen. Besonders kritisch sind IT-Angriffe über die Lieferkette dann, wenn davon weit verbreitete Software betroffen ist, die auf IT-Systemen, auf denen sie installiert ist, mit weitreichenden Rechten ausgestattet ist, wie beispielsweise Überwachungs-, Management oder Antiviren Software. Gleiches gilt für Cyberangriffe auf Dienstleister wie Software-as-a-Service-Anbieter oder Security Operation Centres. Typischerweise reduzieren sich die Möglichkeiten, die der Endkunde zur Detektion von schadsoftwarebehafteten Produkten hat, je früher im Entwicklungsprozess der Soft- oder Hardware die Angreifer ihre Manipulationen vorgenommen haben. Auch sind die Detektionschancen für eine vorliegende Infektion mit Schadsoftware typischerweise geringer, wenn die Schadsoftware über die Lieferkette eingebracht wurde, da so der Fußabdruck beim eigentlichen Angriffsziel kleiner bleibt. Daher sind die Erfolgsaussichten bei Supply Chain Angriffen auf gut geschützte Ziele meist deutlich höher als bei direkten Cyberangriffen von außen. Daher muss gerade bei Anlagen und Einrichtungen, die ein hohes Sicherungsniveau in Bezug auf die Cybersicherheit umgesetzt haben, potenziellen Supply Chain Angriffen besondere Aufmerksamkeit gewidmet werden. Bei vielen Supply Chain Angriffen steht das Einbringen von kompromittierter Soft- oder Hardware im Vordergrund. Neben diesem klar ersichtlichen Weg gibt es aber noch einen diffuseren Weg einer Angreifbarkeit oder Kompromittierung über die Lieferkette: den Weg über Abhängigkeiten der eingesetzten, lokal installierten Softwarekomponenten von weiteren, in diese

eingebundenen, zentralen Softwarekomponenten wie Bibliotheken. Hier besteht die Problematik häufig darin, dass dem Endanwender im Detail gar nicht bekannt ist, welche der eingesetzten IT-Systeme welche Abhängigkeiten besitzen. Insgesamt ist festzustellen, dass die Angriffsoberfläche einer konkreten Anlage oder Einrichtung durch die immer stärker verzweigten Lieferketten, Abhängigkeiten in Softwareprodukten und die Auslagerung von sensiblen Informationen und Diensten an externe Anbieter zum einen größer und zum anderen immer diffuser und für die einzelne Anlage immer schlechter abgrenzbar wird. Es ist bereits jetzt absehbar, dass sich sowohl die Nutzung von externen Softwarekomponenten wie Bibliotheken als auch die Abhängigkeit von externen Dienstleistungen wie SOCs oder Cloud-Anbietern in Zukunft noch verstärken wird. Daher sollte dieser Aspekt der Supply-Chain-Angriffe über die Lieferkette zukünftig stärker berücksichtigt werden. Zu berücksichtigen ist auch, dass sich das Feld der Supply-Chain-Angriffe nicht auf direkte Cyberangriffe auf die Lieferketten von Softwareprodukten oder IT-Systemen beschränkt, sondern deutlich breiter ist. In den vergangenen Monaten wurden beispielsweise Angriffe auf Ziele innerhalb der Lieferkette von Lieferanten beobachtet, was den zuvor erwähnten Aspekt der Diffusität der Angriffsoberfläche noch einmal unterstreicht. Zudem wurden auch Angriffe beobachtet, bei denen gezielt physische Lieferketten über Cyberangriffe lahmgelegt wurden. Es bleibt abzuwarten, wie sich dieser Aspekt in den kommenden Monaten weiterentwickeln wird.

Im Einzelnen zeigt sich im Zusammenhang mit Schwachstellen in industriellen Steuerungssystemen, dass durchaus auch Schwachstellen in industriellen Steuerungssystemen oder anderen Komponenten und Einrichtungen auftreten, die in kerntechnischen Anlagen zum Einsatz kommen. Zusätzlich werden zunehmend Schwachstellen in Komponenten, Programmen und Betriebssystemen bekannt, die innerhalb der IT-Infrastruktur solcher Anlagen eingesetzt sind. Es zeigt sich wiederholt, dass es gerade Schwachstellen in gebräuchlicher Büro IT sind, welche den Angreifern die Durchführung erster Angriffsschritte erlauben. Gegenwärtig arbeiten viele IT-Spezialisten an der Entdeckung von Schwachstellen und informieren im Regelfall die Hersteller der betroffenen IT-Systeme deutlich vor der Öffentlichkeit, um diesem Zeit für die Entwicklung von Patches oder mitigativen Maßnahmen zu geben, aber es werden bei weitem nicht alle Schwachstellen auf diese Art und Weise entdeckt. Häufig werden Schwachstellen bereits lange vor ihrem Bekanntwerden unbemerkt genutzt, teilweise sogar durch sogenannte Zero-Day-Exploits, d. h. Schwachstellen werden bereits ausgenutzt bevor der Hersteller selbst über das Vorhandensein der Schwachstellen Kenntnis erlangt.

Hinzu kommt, dass Schwachstellen in vielen Fällen sehr spät oder gar nicht gepatcht werden, sodass sie auch noch Jahre nach ihrem Bekanntwerden für Angreifer interessant sind und entsprechend ausgenutzt werden. Beispielsweise war die 2010 als Zero Day Schwachstelle im Rahmen des Cyberangriffs mit der Schadsoftware Stuxnet bekannt gewordene LNK-Schwachstelle noch Jahre nach Veröffentlichung eines geeigneten Patches die von Angreifern am häufigsten ausgenutzte Einzel-Schwachstelle. Prinzipiell gibt es zwei unterschiedliche Ursachen dafür, dass bereits bekannte Schwachstellen nicht gepatcht werden: Entweder stehen herstellerseitig keine oder noch keine Patches zur Verfügung oder zur Verfügung stehende Patches werden anwenderseitig nicht eingespielt. Für beides gibt es eine Vielzahl von Gründen, die beispielsweise von fehlender Schwachstellenbehebung in Legacy Systemen über langwierige Entwicklungszyklen und Genehmigungsverfahren über Nachlässigkeit und Unwissen auf Anwenderseite bis hin zur Einhaltung von Testzeiträumen und Nichtumsetzung aufgrund erfolgter Risiko Nutzen Abwägungen reichen. Allein aus dieser beispielhaften Aufzählung wird ersichtlich, dass trotz der Problematik ungepatchter Schwachstellen eine generelle Kritik am Nicht Patchen nicht möglich ist, da teilweise dieses Vorgehen auf sorgfältigen, nachvollziehbaren Überlegungen basiert. Letzteres ist allerdings nur dann möglich, wenn ein Update bzw. ein Patch vom Hersteller zügig zur Verfügung gestellt wird und die Entscheidung, ob und wann es eingesetzt wird, beim Kunden liegt. Dabei ist aber zu bedenken, dass die erste Generation an rechnerbasierten und programmierbaren Geräten inzwischen teilweise veraltet, was dazu führt, dass diese Entscheidung häufig nicht mehr beim Kunden liegt, sondern bei bekanntwerdenden Schwachstellen in entsprechend alten IT-Systemen vom Hersteller schlicht kein Patch mehr zur Verfügung gestellt wird. Gerade in den vergangenen Monaten und Jahren war diese Problematik der softwarebedingten Alterung und des damit verbundenen Mangels an Support für Legacy Systeme verstärkt zu beobachten. Grundsätzlich und unabhängig von den Gründen, aus denen nicht gepatcht wird oder werden kann, stellt eine ungepatchte Schwachstelle durch die Vergrößerung der Angriffsoberfläche aus Sicht der Cybersicherheit immer ein Problem dar, das einer Lösung bedarf, gegebenenfalls in Form alternativer Sicherungsmaßnahmen.

In Bezug auf Cyberangriffe auf den Energiesektor ist festzuhalten, dass die eigentlichen Angriffszwecke und vermutlich auch die Motivation der Angreifer sehr breit gefächert sind. Zum einen gibt es immer wieder Cyberangriffe, die auf direkte physische Auswirkungen abzielen, beispielsweise auf die Hervorrufung von Stromausfällen. Zudem gibt es eine große Anzahl an Angriffen, bei denen Informationsdiebstahl und Spionage im

Vordergrund stehen. Ebenfalls beobachtet werden Cyberangriffe, die eher vorbereitenden Charakter für spätere Angriffsschritte oder den Zweck einer geeigneten Positionierung für spätere Angriffe zu haben scheinen. Zusätzlich zu diesen eher strategisch, politisch oder ideologisch motivierten Cyberangriffen gibt es aber auch Cyberangriffe mit deutlich finanzieller Motivation, wobei Erpressung und der Handel mit gestohlenen Daten im Vordergrund stehen. Eine Problematik, die in den vergangenen Monaten und Jahren immer wieder zutage getreten ist, ist der Einsatz alter Kommunikationsprotokolle. Diese Protokolle wurden in einer Zeit entwickelt, in welcher der Fokus ausschließlich auf der Bereitstellung von Funktionalitäten lag und zu der die Berücksichtigung von Aspekten der Cybersicherheit noch nicht üblich war. Erfolgreiche Angriffe auf die elektrische Energieversorgung sind generell mit deutlichen Auswirkungen verbunden. Die Verursachung physischer Schäden hat hierbei häufig weitreichende Folgen wie beispielsweise flächendeckende Stromausfälle und dadurch Kollateralschäden in von der elektrischen Energieversorgung abhängigen Bereichen. Dies gilt insbesondere für Angriffe, die zu länger andauernden Stromausfällen führen.

Kerntechnische Anlagen und Einrichtungen sind immer wieder von Cyberangriffen betroffen, wobei sie meist nicht direkt angegriffen werden, sondern indirekt von Cyberangriffen auf Zulieferer, Behörden und Energieversorgungsunternehmen betroffen sind. Auch wird das kerntechnische Umfeld für Social Media Angriffe genutzt. Darüber hinaus ist der Nuklearsektor nicht nur in Deutschland, sondern auch darüber hinaus, ein Feld im öffentlichen Interesse, das auch stark von ideologischen und politischen Motiven geprägte Aufmerksamkeit erfährt. Dies schlägt sich auch in Cyberangriffen, die eine entsprechende Meinungsäußerung zum Ziel haben, nieder wie beispiels-weise den Cyberangriffen in Zusammenhang mit der Einleitung von radioaktivem Ab-wasser aus Fukushima Daichi ins Meer.

Geopolitische Spannungsfelder begünstigen traditionell die Entwicklung defensiver und offensiver Fähigkeiten und den Aufbau entsprechender Ressourcen. Hierbei stellen Cyberangriffe keine Ausnahme dar. Gerade in Zusammenhang mit dem Krieg in der Ukraine ist es in den vergangenen Jahren zu zahlreichen Cyberangriffen gekommen. Bereits vor Beginn der Kampfhandlungen war hier eine deutliche Zunahme an Cyberangriffen zu verzeichnen. Seit Beginn der Kampfhandlungen wurde darüber hinaus ein deutlicher Anstieg bei den bekannt gewordenen Cyberangriffen festgestellt. Hierzu zählen Cyberangriffe auf kritische Infrastrukturen und Kommunikationskanäle, aber insbesondere auch strategisch und politisch motivierte Cyberangriffe, die nicht nur Russland und die

Ukraine sondern darüber hinaus beispielsweise auch die NATO Partner und weitere Staaten, die eine offizielle Form der Unterstützung für die Ukraine signalisiert haben, betreffen. Ähnliches gilt für die meisten geopolitischen Spannungsfelder. Cyberangriffe kommen heutzutage in praktisch allen geopolitischen Spannungsfeldern zum Einsatz. Dies schließt Cyberangriffe verschiedenster Komplexität von einfachen disruptiven Angriffen bis hin zu hochausgereifter Schadsoftware und langandauernden Angriffskampagnen ein. Hierbei stehen meist strategische Motive, Spionage, politische Meinungsäußerung und psychologische Effekte wie Destabilisierung und Demoralisierung im Vordergrund. Insgesamt wird deutlich, dass eine Abgrenzung geopolitischer Spannungsfelder nur oberflächlich möglich ist. Auf einer tiefer liegenden Ebene sind konkrete Spannungsfelder zwischen einzelnen Staaten meist nur Ausprägungen von deutlich breiter gefächerten Spannungsfeldern, an denen typischerweise nicht nur zwei Staaten beteiligt sind. Dies schlägt sich auch in den entsprechenden Cyberangriffen nieder.

Allgemein ist davon auszugehen, dass nur ein kleiner Teil der tatsächlich stattfindenden Cyberangriffe publik gemacht wird und auch bei den bekanntwerdenden Cyberangriffen werden in der Regel relevante Informationen zurückgehalten. Hierfür können sehr viele verschiedene Gründe eine Rolle spielen, die von der Vermeidung eines Reputationsverlusts und der Begrenzung finanzieller Auswirkungen bis hin zu strategischen Überlegungen reichen. Letzteres gilt generell, aber noch verstärkt im Umfeld der kriegerischen Auseinandersetzungen in der Ukraine oder in anderen geopolitischen Spannungsfeldern, da hier die Bekanntmachung erfolgreicher wie auch vereitelter Cyberangriffe, insbesondere auf kritische Infrastrukturen, eine starke politische Dimension hat. Daher ist vor dem Hintergrund des laufenden Angriffskrieges und schwelenden Konflikten in anderen geopolitischen Spannungsfeldern von einer verschärften IT-Bedrohungslage und einer Zunahme an Cyberangriffen bei gleichzeitig dünner werdender Informationslage auszugehen.

Grundsätzlich zeigt die gegenwärtige IT-Bedrohungslage: Eine große Zahl der beobachteten Cyberangriffe ist mehrstufig, komplex und beinhaltet den Einsatz verschiedenster Cyberangriffswerkzeuge und Schadsoftwarekomponenten. Manche Cyberangriffe scheinen lediglich zu Testzwecken durchgeführt zu werden, andere wiederum nur, um durch die Demonstration von Fähigkeiten eine Drohkulisse aufzubauen. Die Mehrheit der Cyberangriffe folgt allerdings mit anderen Zielen, beispielsweise dem Ziel, finanziellen Gewinn zu erzielen, Manipulationen durchzuführen oder Informationen auszuspähen. Cyberangriffe werden zunehmend von langer Hand geplant und über lange

Zeiträume durchgeführt. So erfolgen häufig zunächst Spionageschritte und erst Monate oder Jahre später der Einsatz der ausspionierten Informationen. Kritische Infrastrukturen sind inzwischen häufig von Cyberangriffen betroffen. Auch rückt die Ausspähung, Manipulation oder Sabotage von industriellen Steuerungssystemen immer stärker in den Fokus von Angreifern. Gerade für und insbesondere in weiterführenden Angriffsschritten ist gezielte Spionage in Bezug auf industrielle Steuerungssysteme keine Seltenheit. Insgesamt sind industrielle Steuerungssysteme zunehmend von Cyberangriffen betroffen. Die beobachteten IT-Sicherheitsvorfälle und Cyberangriffe der vergangenen Jahre zeigen deutlich, dass es eine ganze Reihe von Angreifer Gruppierungen gibt, die in der Lage sind, komplexe und über lange Zeiträume unentdeckte Cyberangriffe auszuführen, die – sofern dies zum Ziel der Angreifer zählt – sich auch auf industrielle Steuerungssysteme erstrecken. Hierzu zählen ausdrücklich nicht nur die hier vorgestellten APT-Gruppierungen, sondern neben weiteren APT-Gruppierungen auch andere Typen von Angreifern. Dabei ist nicht nur anzunehmen, dass hochentwickelte Angriffswerkzeuge zeitverzögert in die Hände von Angreifern mit weniger ausgeprägten Fähigkeiten gelangen, sondern es hat sich gezeigt, dass teilweise gezielt Entwicklungsaufwand betrieben wird, um solchen Angreifern den aktiven Einsatz dieser Werkzeuge zu erleichtern.

Sowohl aus dem Blickwinkel der IT-Bedrohungslage als auch ausgehend von der individuell vorhandenen Angriffsoberfläche zählen prinzipiell auch alle deutschen kerntechnischen Anlagen und Einrichtungen zu potenziellen Angriffszielen für Cyberangriffe. Grundsätzlich bietet die korrekte und vollständige Umsetzung der SEWD Richtlinie IT aus Sicht der GRS weitreichenden Schutz vor den Gefahren von Cyberangriffen. Aus Sicht der GRS ist zunächst davon auszugehen, dass in Anlagen, die ihre IT-Systeme konsequent gemäß SEWD Richtlinie IT schützen, die Hürden für die Kompromittierung eines sicherheitstechnisch relevanten Systems deutlich höher sind als in vielen anderen kritischen Infrastrukturen. Insgesamt ist allerdings zu beachten, dass auch die korrekte und vollständige Umsetzung der SEWD Richtlinie IT – oder eines beliebigen anderen Regelwerks zur Cybersicherheit – zwar einen weitreichenden, aber keinen vollumfänglichen Schutz vor den Gefahren eines langfristig angelegten Cyberangriffs durch eine Angreifer Gruppierung mit den entsprechenden zeitlichen, finanziellen und personellen Ressourcen bieten kann. Die hier beschriebenen IT-Sicherheitsvorfälle und weiteren Aktivitäten der Angreifer verdeutlichen, dass Strategien zur frühzeitigen Detektion solcher Cyberangriffe und angemessene Maßnahmen zur Reaktion auf entsprechende IT-Sicherheitsvorfälle in diesem Zusammenhang von zentraler Bedeutung für die Sicherheit und Sicherung deutscher kerntechnischer Anlagen sind.

Dies wird noch unterstrichen durch eine signifikante Entwicklung der IT-Bedrohungslage in Bezug auf das Vorgehen der Angreifer hinsichtlich der Vermeidung einer Entdeckung des Angriffs. So verwenden hoch entwickelte, versierte Angreifer Gruppierungen immer mehr Zeit auf Detektionsevasion und nehmen diesbezüglich erheblichen zeitlichen, finanziellen und personellen Aufwand auf sich.

Ein weiterer, besorgniserregender Trend in den letzten Jahren ist auch die Tatsache, dass durch Angebote wie „APT for hire“ und „Ransomware as a Service“ hochentwickelte Angriffswerkzeuge, Schadsoftwarekomponenten und die entsprechende IT Angreifer Infrastruktur inzwischen auch einem Personenkreis zur Verfügung stehen, der zahlungskräftig ist, aber auf sich gestellt nicht in der Lage wäre, einen erfolgreichen Cyberangriff vorzubereiten und durchzuführen. Dies schließt beispielsweise terroristische Vereinigungen ein. Zusätzlich gibt es inzwischen hochentwickelte Angriffswerkzeuge, die offenbar gezielt so entwickelt wurden, dass sie auch von weniger versierten Angreifern nutzbar sind. Das bedeutet eine weitere Verschärfung der IT-Bedrohungslage für kritische Infrastrukturen insgesamt und damit auch für deutsche kerntechnische Anlagen und Einrichtungen.

Quellen

/ABB14r01/ ABB System 800xA: System Introduction, 2014

/ABB19w01/ Abbasi, A. et al., Blackhat Europe 2019 Vortrag, Doors of Durin: The Veiled Gate to Siemens S7 Silicon, https://www.blackhat.com/, Dezember 2019 [abgerufen am 29.04.2021]

/ABB20r01/ ABB Cybersecurity Advisory: Security System 800xA Information Manager – Remote Code Execution, CVE-2020-8477, 2020

/ABB20r02/ ABB Cybersecurity Advisory: Security System 800xA Weak Registry Permissions, CVE-2020-8474, 2020

/ABB20r03/ ABB Cybersecurity Advisory: Security System 800xA Weak File Permissions, CVE-2020-8472, CVE-2020-8473

/ABB20r04/ ABB Cybersecurity Advisory Update: System 800xA Information Manager – Remote Code Execution, CVE-2020.8477, 2020

/ABB20r05/ ABB Cyberssecurity Advisory Update: System 800xA Weak File Permission, VE.2020-8474, 2020

/ABB20r06/ ABB Cybersecurity Advisory Update: Weak File Permissions, CVE-2020-8472, CVE-2020-8473, 2020

/ABB20r08/ ABB Cybersecurity Advisory: Multiple Vulnerabilities in Central Licensing Server, CVE-2020-8481, CVE-2020-8479, CVE-2020-8475, CVE-2020-8476, CVE-2020-8471, 2020

/ABB20r09/ ABB Cybersecurity Advisory: Inter process communication vulnerability in System 800xA, CVE-2020-8478, CVE-2020-8484, CVE-20208485, CVE-2020-8486, CVE-2020-8487, CVE-2020-8488, CVE-2020-8489, 2020

/ABB20r10/ ABB Cybersecurity Advisory: abb central Licensing System Vulnerabilities, impact on System 800xA, Compact HMI and Controller Builder Safe: CVE-2020-8481, CVE-2020-8479, CVE-2020-8475, CVE-2020-8476, CVE-2020-8471, 2020

/ABB20w01/ ABB Ability™ System 800xA References, abgerufen auf https://new.abb.com/control-systems/system-800xa/references-case-studies, am 22.09.2020

/ABR20w01/ Abrams, L., Large scale Snake Ransomware campaign targets healthcare, https://www.bleepingcomputer.com/, 06.05.2020 [abgerufen am 05.05.2020]

/AIR17w01/ Airbus Cybersecurity, Ransomware BadRabbit, https://airbus-cyber-security.com/, 16.11.2017 [abgerufen am 09.05.2021]

/ALT19i01/ Atran Technologies, Presse-Mitteilung, Information on a cyber-attack, 28.01.2019

/ANS21r01/ Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Campagne d’attaque du mode opératoire Sandworm ciblant des serveurs Centreon, v. 1.0, 27.01.2021, TLP:White

/ART22w01/ Ars Technica, Botnet that hid for 18 months boasted some of the coolest tradecraft ever, 03.05.2022, https://arstechnica.com/, [abgerufen am 31.08.2022]

/AUT19w01/ Automotive News, Toyota among companies targeted by Vietnam-linked hacking group, 22 December 2019, https://www.autonews.com [abgerufen am 19.04.2021]

/AVI20r01/ Avisa partners whitepaper: The Lazarus Constellation, A Study on North Korean malware, 2020

/BBC12w01/ BBC News, Shamoon Virus Targets Energy Sector Infrastructure, 17 August 2012, https://bbc.com [abgerufen am 22.04.2021]

/BBC22w01/ BBC, Predatory Sparrow: Who are the hackers who say they started a fire in Iran?, 11 July 2022, https://www.bbc.com/ [abgerufen am 09.09.2022]

/BFV18r01/ Bundesamt für Verfassungsschutz, BfV Cyber-Brief Nr. 01/2018, Hinweis auf aktuelle Angriffskampagne, Andauernde Bedrohung durch die Angriffe der APT1Berserk Bear auf deutsche Unternehmen, Juli 2018

/BFV18r02/ Bundesamt für Verfassungsschutz, BfV Cyber-Brief Nr. 02/2018, Hinweis auf aktuelle Angriffskampagne, Hochwertige Cyberangriffe gegen deutsche Medienunternehmen und Organisationen im Bereich der Chemiewaffenforschung, Juli 2018

/BID20w01/ Binary Defense, Garrett Thompson, Sandworm Threat Actor Hijacks Mail Servers According to NSA, 29. Mai 2020, https://www.binarydefense.com/ [abgerufen am 04.11.2020]

/BIH19r01/ Biham, E. et al. Rogue 7: Rogue Engineering-Station attacks on S 7 Simatic PLCs. (2019)

/BLE18w01/ Bleeping Computer, Security, New GreyEnergy Malware Targets ICS, Tied with BlackEnergy and TeleBots, 17 October 2018, https://www.bleepingcomputer.com [abgerufen am 07.05.2021]

/BLH20r01/ Black Hat Ethical Hacking: Iranian Hackers have been hacking VPN Servers to plant Backdoors in Companies around the world, 2020

/BMU13n03/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMU), Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT), VS-Nur für den Dienstgebrauch, 8.Juli 2013

/BOR21w01/ Borns IT- und Windows-Blog, Gab es beim Exchange-Massenhack ein Leck bei Microsoft? 13.03.2021, https://www.borncity.com, [abgerufen am 14.06.2022]

/BRI19w01/ Briggs, B., Microsoft, Hackers hit Norsk Hydro with ransomware. The company responded with transparency, 16.12.2019 [abgerufen am 06.05.2021]

/BSI13t01/ Bundesamt für Sicherheit in der Informationstechnik (BSI), ICS-Security Kompendium, 2013

/BSI14r01/ Bundesamt für Sicherheit in der Informationstechnik BSI, Die Lage der IT-Sicherheit in Deutschland 2014, 2014

/BSI16i01/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Angriffe des Mirai Botnetzes auf Port7547, CSW-Nr. 2016-454513-1161, Version 1.1, 01.12.2016

/BSI17i01/ Bundesamt für Sicherheit in der Informationstechnik (BSI), Schwachstelle, Gefährdung, Vorfall, IT-Assets, Crashoverride, Gezielte Angriffe durch Schadsoftware auf den Betrieb von Stromnetzen, CSW-Nr. 2017-191668-1031, Version 1.0, 2017

/BSI17i06/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Empfehlungen zum Schutz vor Angriffen auf isolierte Netzwerke über USB-Wechseldatenträger, CSW-Nr. 2017-191981-1063, Version 1.0, 28.06.2017

/BSI20i01/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Bedrohung deutscher KRITIS-Unternehmen durch Cyberangriffe der APT-Gruppierung Berserk Bear/Energetic Bear, TLP:AMBER, CWS-Nr. 2020-208716-1064, Version 1.0, 19.05.2020

/BSI20i02/ Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Cyber-Sicherheitswarnung, Kritische Schwachstelle im Windows Netlogon Remote Protocol (ZEROLOGON), Version 1.2 vom 09.10.2020

/BSI20i03/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Supply-Chain-Angriff übermanipulierte SolarWinds OrionSoftware, CSW-Nr. 2020-533179-10k3, Version 1.0, 14.12.2020

/BSI20i04/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Supply-Chain-Angriff übermanipulierte SolarWinds OrionSoftware, CSW-Nr. 2020-533179-11k3, Version 1.1, 28.12.2020

/BSI20i05/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Supply-Chain-Angriffe durch APT-Gruppe Tonto Team, CSW-Nr. 2020-253018-12k4, Version 1.0, 06.11.2020

/BSI20r03/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Schwachstellen in Open Source Netzwerkstacks (AMNESIA:33), CSW-Nr. 2020-532768-11k3, Version 1.1, 09.12.2020

/BSI20r04/ BSI für Bürger: Aktuelle Informationen zur Schadsoftware Emotet

/BSI20w01/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Glossar der Cyber-Sicherheit, https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288 [abgerufen am 22.06.2020]

/BSI20w04/ BSI, Steckbriefe aktueller Botnetze, Mirai, https://www.bis.bund.de [abgerufen am 8.8.2020]

/BSI21i03/ BSI, Mehrere Schwachstellen in MS Exchange, CSW-Nr. 2021-197772-17k2, Version 1.7, 10.03.2021

/BSI21i11/ BSI, Tageslagebericht vom 29.07.2021

/BSI21r01/ EMOTET YARA Regeln: Aktuelle Informationen zum Takedown von Emotet, April 21

/BSI22i06/ BSI, Tageslagebericht vom 29.04.2022

/BSI22i07/ BSI, Tageslagebericht vom 14.04.2022

/BSI22r17/ BSI, Tageslagebericht vom 19.05.2022

/BUS17w01/ Business Insider, The 'Petya' global cyberattack may have just been cover for an attack in Ukraine, 30 June 2027, https://www.businessinsider.com [abgerufen am 07.05.2021]

/BUS20w01/ Business Insider, Here's a list of the US agencies and companies that were reportedly hacked in the suspected Russian cyberattack, K. Vlamis, 19 December 2020, https://www.businessinsider.com [abgerufen am 19.04.2021]

/CIA12r01/ Central Intelligence Agency, Information Operations Center, Shadow v1.0, User Guide, SECRET//X1, 31 August 2012

/CIA13r01/ Central Intelligence Agency, Information Operations Center, (U) Engineering Development Group, EzCheese v6.3, Users Guide, Rev. B, SECRET//20350629, 18 July 2013

/CIA13r02/ Central Intelligence Agency, Information Operations Center, (U) Engineering Development Group, Emotional Simian v2.2, User Manual, Rev. 1.1, SECRET//X1, 30 August 2013

/CIA16r01/ Central Intelligence Agency, Information Operations Center, (U) Engineering Development Group, Brutal Kangaroo Program, Drifting Deadline v1.2, User Guide Rev. A, SECRET//NOFORN, 23 February 2016

/CIS14r01/ U. S. Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency (CISA), ICS Alert ICS-ALERT-14-176-02A, ICS Focused Malware (Update A), 27 June 2014 [abgerufen am 16.06.2020]

/CIS16i01/ U. S. Department of Homeland Security, CISA, ICS Alert, Cyber-Attack Against Ukrainian Critical Infrastructure, IR-ALERT-H-16-056-01, https://us-cert.cisa.gov [abgerufen am 07.05.2021]

/CIS17i02/ U. S: Department of Homeland Security, CISA, Alert (TA17-132A), Indicators Associated With WannaCry Ransomware, 12 May 2017, https://us-cert.cisa.gov [abgerufen am 15.01.2021]

/CIS17r01/ Cisco Talos Intelligence Group – Comprehensive Threat Intelligence: Player 3 Has Entered the Game: Say Hello to 'WannaCry', 12 May 2017, https://blog.talosintelligence.com [abgerufen am 13.01.2021]

/CIS18r01/ U. S. Department of Homeland Security, CISA, Alert (TA18-074A). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors, March 15, 2018, https://us-cert.cisa.gov [abgerufen am 6.11.2020]

/CIS20i02/ U.S. Department of Homeland Security, CISA, Alert AA20-301A: North Korean Advanced Persistent Threat Focus: Kimsuky, 27.10.2020

/CIS20r01/ U. S. Department of Homeland Security, CISA, Alert (AA20-296A). Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets, October 22, 2020, https://us-cert.cisa.gov [abgerufen am 6.11.2020]

/CIS20r02/ U. S. Department of Homeland Security, CISA, Alert (AA20-283A). APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations, October 9, 2020, https://us-cert.cisa.gov [abgerufen am 6.11.2020]

/CIS20r03/ U. S. Department of Homeland Security, CISA, ICS Advisory (ICSA-20--343-01), Multiple Embedded TCP/IP Stacks, 09.12.2020

/CIS20r04/ U. S. Department of Homeland Security, CISA, ICS Advisory (ICSA-20-343-05), Siemens Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33), 08.12.2020

/CIS20r05/ U. S. Department of Homeland Security, CISA Alert AA20-049A: Ransomware Impacting Pipeline Operations, 2020

/CIS21i01/ U. S. Department of Homeland Security, CISA, ICS Advisory (ICSA-21-119-04), Multiple RTOS (Update A), 6 May 2021

/CIS21i09/ Cybersecurity & Infrastructure Security Agency CISA, ICS Advisory (ICSA-21-208-03) Geutebrueck G-Cam E2 and G-Code, July 27 2021

/CNE18w01/ CNET, US: Russia's NotPetya the most destructive cyberattack ever, 15 February 2018, https://www.cnet.com [abgerufen am 07.05.2021]

/CNN17w01/ CNN Business, Another big malware attack ripples across the world, 28 June 2017, https://money.cnn.com [abgerufen am 07.05.2021]

/COM21w01/ Computer Weekly, More intel emerges on WhisperGate Malware that hit Ukraine, 26 January 2022

/CON18w01/ Control Engineering, Advice from the Triton cybersecurity incident, April 18, 2019

/CON19w01/ Context, AVIVORE Hunting Global Aerospace through the Supply Chain, https://www.contextis.com/, 03.10.2019 [abgerufen am 05.05.2021]

/CPO21w01/ Cyber-Peace.org: Operation Troy / Dark Seoul

/CSO19w01/ CSO, Cynthia Brumfield, Russia's Sandworm hacking group heralds new era of cyber warfare, 22 Nov 2019, https://www.csoonline.com/ [abgerufen am 04.11.2020]

/CYB18w01/ Cyberscoop, Trisis Masterminds have expanded operations to target U. S. industrial firms, Chris Bing, May 24, 2018

/CYB19w01/ Cyberscoop, Vietnams premier hacking group ramps up targeting of global car companies, 21 March 2019, https://www.cyberscoop.com [abgerufen am 07.05.2021]

/CYB20w01/ Cyberreason Blog, Back to the Future: Inside the Kimsuky KGH Spy-ware Suite, https://www.cybereason.com/, 02.11.2020 [abgerufen am 21.12.2020]

/CYB22w03/ Cyberscoop, How the French fiber optic cable attacks accentuate critical infrastructure vulnerabilities, April 28 2022, https://www.cyber-scoop.com/french-fiber-optic-cables-attack-critical-infrastructure/, [abgerufen am 26.08.2022]

/CYB22w04/ Cyberscoop, DHS investigators say they foiled cyberattack on undersea internet cable in Hawaii, April 13 2022, https://www.cyberscoop.com/un-dersea-cable-operator-hacked-hawaii/, [abgerufen am 29.08.2022]

/CYC18w01/ Cyclane Threat Vector, Energetic DragonFly DYMALLOY Bear 2.0, J. Gross and K. Livelli, 16 March 2018, https://threatvector.cyclane.com [abgerufen am 24.06.2020]

/DAR12w01/ Dark Reading, Shamoon Code 'Amateur' But Effective, K. Hig-gins, 11 September 2012, https://www.darkreading.com [abgerufen am 22.04.2021]

/DAR21w01/ Dark Reading, More SolarWinds Attack Details Emerge, K. Higgins, Jan-uary 2019, https://www.darkreading.com [abgerufen am 04.03.2021]

/DIG20w01/ Digital Shadows, DarkSide: The New Ransomware Group Behind Highly Targeted Attacks, 22 September 2020, https://www.digitalshadows.com [abgerufen am 11.05.2021]

/DIG22w01/ Digicomp, Was ist ein LotL-Angriff (Living off the Land), 11.02.2022, https://www.digicomp.ch/, [abgerufen am 31.08.2022]

/DIN20n01/ DIN, DIN IEC 62645, Kernkraftwerke – Leittechnische und elektrische Systeme – Anforderungen an die Cybersicherheit (IEC 62645:2019); Deutsche Fassung EN IEC 62645:2020, Oktober 2020

/DOJ16r01/ The United States Department of Justice, Office of Public Affairs, Former U.S. Nuclear Regulatory Commission Employee Pleads Guilty to Attempted Spear-Phishing Cyber-Attack on Department of Energy Computers, 2 February 2016

/DOR19w01/ Dorks Delivered, Cybersecurity Attacks on Toyota Australia and Other Subsidiaries, 2019

/DOU18w01/ DoublePulsar Cybersecurity Threat Intelligence, Root Bridge how thousands of internet connected Android devices now have no security, and are being exploited by criminals, K. Beaumont, 8 June 2018, https://doublepulsar.com [abgerufen am 24.08.2020]

/DRA17r02/ Dragos, CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations, February 2017

/DRA19r01/ Dragos, Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on Industrial Environments, Joe Slowik, October 2019

/DRA19w01/ Dragos, Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targetting Electric Sector, in Addition to Oil and Gas, June 2019

/DRA20r01/ Dragos Inc., CRASHOVERRIDE, Analysis of the Threat to Electric Grid Operations, Version 2.20170613, www.dragos.com, 2020

/DRA20w01/ Dragos Inc., Electrum, Since 2016, https://www.dragos.com, [abgerufen am 27.07.2020]

/DRA20w02/ DRAGOS Inc., Blogpost "EKANS Ransomware and ICS Operations", Februar 2020 [abgerufen am 05.05.2021]

/DWE22w01/ Deutsche Welle, Pro-Russia Killnet Hackers target Italian institutions, May 2022, www.dw.com [abgerufen am 09.08.2022]

/ESE17r01/ ESET Enjoy Safer Technology, Anton Cherepanov, WIN32/INDUSTROYER, A new threat for industrial control systems, Version 2017-06-12, https://www.welivesecurity.com, [abgerufen am 14.07.2020]

/ESE18r01/ ESET, A. Cherepanov, GreyEnergy – A successor to BlackEnergy, White Paper, October 2018

/ESE18w01/ ESET, R. Lipovsky, GreyEnergy: Eine der gefährlichsten APT-Gruppen rüstet auf, 17 October 2018, https://www.welivesecurity.com [abgerufen am 07.05.2021]

/ESE20w01/ ESET, New cyber espionage framework named Ramsaydiscovered by ESET Research, 13 May 2020, [https://www.eset.com]

/ESE21w01/ ESET We live security, Exchange servers under siege from atleast 10 APT groups, 10.03.2021, https://www.welivesecurity.com, [abgerufen am 14.06.2022]

/ESE21w02/ Eset Welivesecurity, FamousSparrow: Cyberspionage statt ZimmerService, https://www.welivesecurity.com/, [abgerufen am 01.09.2022]

/EWB20w01/ Energiewirtschaft.blog, Ukraine: Blackout durch Hackerangriff, https://energiewirtschaft.blog, [abgerufen am 09.07.2020]

/EWO20w01/ Ewon, Kompetenzzentrum für Remote Solutions das sind wir, https://www.ewon.biz/de [abgerufen am 15.07.2020]

/FBI21w01/ FBI, Press Release, FBI Statement on Network Disruption at Colonial Pipeline, 9 May 2021, https://www.fbi.gov [abgerufen am 11.05.2021]

/FDD20w01/ Foundation for Defense of Democracies (FDD), Trevor Logan, NSA Re-port Attributing Malware to Russian Hacking Group Sandworm Signals That the Group Is Still Active, June 4, 2020, https://www.fdd.org, [abgerufen am 13.07.2020]

/FIN22w01/ Fineproxy, Was sind SOCKS-Proxys?, https://fineproxy.de/knowledge-base/was-sind-socks-proxys/, [abgerufen am 31.08.2022]

/FIR16w01/ Fire Eye, John Hultquist, Threat Research, Sandworm Team and the Ukrainian Power Authority Attacks, January 08, 2016, https://www.fireeye.com, [abgerufen am 28.07.2020]

/FIR17w01/ FireEye, Threat Research, Attackers Deploy New ICS Attack Framework TRITON, and Cause Operational Disruption to Critical Infrastructure, https://www.fireeye.com, December 14, 2017 [abgerufen am 27.01.2020]

/FIR18w02/ FireEye, Threat Research, TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers, FireEye Intelligence, https://www.fireeye.com, October 23, 2018 [abgerufen am 27.01.2020]

/FIR19w01/ FireEye, Threat Research, Triton Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping, S. Miller, N. Brubaker, D. Kapellmann Zafra, D. Caban, https://www.fireeye.com, April 10, 2019 [abgerufen am 27.01.2020]

/FIR20r01/ FireEye, Threat Research, Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, Dezember 13, 2020, https://www.fireeye.com [abgerufen am 07.01.2021]

/FIR21w02/ FireEye, Die Hackergruppen hinter Advanced Persistent Threats, https://www.fireeye.de [abgerufen am 28.04.2021]

/FOR17w01/ Forbes, Medical Devices Hit by Ransomware For The First Time In US Hospitals, 17 May 2017, https://www.forbes.com [abgerufen am 12.01.2021]

/FOR20f01/ Forescout Research Labs, How Embedded TCP/IP Stacks Breed Critical Vulnearbilities, D. de Santos et al., BlackHat Europe 2020, 9.12.2020

/FOR20r01/ Forescout Research Labs, Research Report, Amnesia:33 – How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices, 07.12.2020

/FOR21r01/ Forescout: NAME:WRECK Forecout Research Labs and JSOF discover nine new vulnerabilities affecting four popular TCP/IP Stacks used in millions of IoT, OT and IT devices, 2021

/FSE14r01/ F-Secure Labs, BLACKENERGY & QUEDAGH, The convergence of crimeware and APT attacks, 2014

/FSE19r02/ F-Secure Labs, The state of the station, A report on attackers in the energy industry, Whitepaper, 2019

/GIT20w01/ Github, ZeroLogon exploitation script, https://github.com [abgerufen am 19.11.2020]

/GIT20w02/ mimikatz lsadump::zerologon (CVE-2020-1472 @SecuraBV @djrevmoon), https://github.com [abgerufen am 19.11.2020]

/GIT21f01/ GitHub, Metasploit-framework, https://github.com [abgerufen am 08.05.2021]

/GOO19w01/ Goodin, D. , Ars Technica, Severe ransomware attack cripples big aluminum producer, 19.03.2019 [abgerufen am 06.05.2021]

/GRS10i01/ GRS, Weiterleitungsnachrichten zu meldepflichtigen Ereignissen in Kernkraftwerken der Bundesrepublik Deutschland, WLN 2010/07, Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7, 30. September 2010

/GRS11i01/ GRS, Weiterleitungsnachrichten zu meldepflichtigen Ereignissen in Kernkraftwerken der Bundesrepublik Deutschland, WLN 201 0/07a, Ergänzung zur Weiterleitungsnachricht 2010/07 "Malware auf speicherprogrammierbaren Steuerungen unter SIMATIe WinCC und SIMATIC PCS 7", 25.10.2011

/GRS12f01/ GRS, Manipulation von speicherprogrammierbaren Steuerungen durch stuxnet, C. Quester, Vortrag Bund-Länder-Ad-hoc-AG Si IT, 6. März 2012

/GRS20r01/ GRS, Stellungnahme zu den IT-Angriffen im Zusammenhang mit der Schadsoftware Triton/TriSIS, VS-NfD, Juli 2020

/GRS21i01/ GRS, Weiterleitungsnachricht 2021/01, IT-Angriffe auf kritische Infrastrukturen im Zusammenhang mit der Schadsoftware Triton/TriSIS, 23.02.2021

/GRS21r03/ GRS, IT-Sicherheit in der Lieferkette, Initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik, GRS-638, 978-3-949088-27-8, Mai 2021

/GRS21r05/ GRS, Stellungnahme zu den IT-Angriffen im Zusammenhang mit manipulierten Solar Winds Produkten, VS-NfD, Oktober 2021

/GRS21r09/ GRS, Stellungnahme zu bekannt gewordenen Schwachstellen in Siemens S7- und PCS7-Systemen (VS-NfD), August 2021

/GRS21r10/ GRS, Stellungnahme zur kritischen Schwachstelle im Windows Netlogon Remote Protokoll (Zerologon) (VS-NfD), August 2021

/GRS21r11/ GRS, Stellungnahme zu den IT-Angriffen im Zusammenhang mit der APT-Gruppierung Dragonfly (VS-NfD), August 2021

/GUA17w01/ The Guardian, Ransomware attack 'not designed to make money', researchers claim, 28 June 2017, https://www.theguardian.com [abgerufen am 07.05.2021]

/GUT19w01/ J. Gutmanis, Triton – The early days, S4x19, Miami, January 2019

/HEI17w01/ Heise, WannaCry: Fast nur Windows-7-PCs infiziert, Mai 2017, https://www.heise.de [abgerufen am 11.01.2021]

/HEI17w03/ Heise, Ransomware WannaCry: Sicherheitsexperte findet Kill-Switch – durch Zufall, Mai 2017, https://www.heise.de [abgerufen am 13.01.2021]

/HEI17w04/ Heise, NSA meldete kritische Sicherheitslücke aus Angst vor den Shadow Brokers an Microsoft, Mai 2017, https://www.heise.de [abgerufen am 13.01.2021]

/HEI17w05/ Heise, WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm, Mai 2017, https://www.heise.de [abgerufen am 13.01.2021]

/HEI17w06/ Heise, WannaCry: Was wir bisher über die Ransomware-Attacke wissen, Mai 2017, https://www.heise.de [abgerufen am 11.01.2021]

/HEI20w01/ Heise Security, Amnesia:33 Sicherheitslücken in TCP/IP-Stacks betreffen Millionen Geräte, 08.12.2020 [abgerufen am 10.12.2020]

/HEI21w01/ Heise, Markus Oberhumer, László Molnár, John F. Reiser, UPX (Ultimate Packer for eXecutables) 3.91, 21.01.2021, https://www.heise.de [abgerufen am 28.01.2021]

/HEI21w02/ Heise, Frankreich: Centreon-Server waren jahrelang infiltriert, 16. Februar 2021, https://www.heise.de [abgerufen am 21.4.2021]

/HEI22w15/ Heise Online, Schadcode-Attacken auf Videoüberwachungssystem und NAS von Qnap möglich, Wichtige Sicherheitsupdates schließen mehreren Lücken in Netzwerkprodukten von Qnap, 06.05.2022, https://www.heise.de/news, [abgerufen am 08.08.2022]

/HEI22w16/ Heise Online, Spyware blieb in Unternehmen bis zu 18 Monate lang unentdeckt, 04.05.2022, https://www.heise.de, [abgerufen am 06.05.2022]

/HEI22w17/ Heise online, Verfassungsschutz: "Hyperbro"-Angriffskampagne auf deutsche Unternehmen, 26.01.2022, https://www.heise.de/, [abgerufen am 28.03.2022]

/HEI22w18/ Heise online, Frankreich: Unbekannte durchtrennen Glasfaser-Backbones, 28.04.2022, https://www.heise.de/news/, [abgerufen am 26.08.2022]

/HNN22w01/ Hawaii News Now, Federal agents disrupted cyberattack targeting phone, internet infrastructure on Oahu, April 13 2022, https://www.hawaiinewsnow.com/, [abgerufen am 29.08.2022]

/HOR20r01/ Horejsi, J. et al., EARTH AKHLUT: EXPLORING THE TOOLS, TACTICS, AND PROCEDURES OF AN ADVANCED THREAT ACTOR OPERATING A LARGE INFRASTRUCTURE, VB2020, Oktober 2020

/HTE22w01/ Hawaii Tech, Homeland Security thwarts attack on Oahu underseacable, April 13 2022, https://www.hawaiitech.com, [abgerufen am 29.08.2022]

/HUB22w01/ Hubspot, API Calls: What They Are & How to Make Them in 5 Easy Steps, April 28 2022, https://blog.hubspot.com/website/api-calls, [abgerufen am 04.11.2022]

/IBM20i01/ IBM Security, New Destructive Wiper ZeroCleare Targets Energy Sector in the Middle East, January 2020

/ICF16w01/ I.C.F: Israel Cyber Forces, BlackEnergy, 10. Januar 2016, https://0xicf.wordpress.com [abgerufen am 20.01.2021]

/ILA20w01/ Ilascu, I., Honda investigates possible ransomware attack, networks impacted, https://www.bleepingcomputer.com/, 08.06.2020 [abgerufen am 05.05.2021]

/IMP22w01/ Imperva, Web Shell, https://www.imperva.com/learn/application-security/web-shell/, [abgerufen am 31.08.2022]

/IND21w01/ Industrial Cyber, Security loopholes identified in Geutebrueck G-Cam E2 and G-Code IP cameras, July 31 2021, https://industrialcyber.co/, [abgerufen am 24.05.2022]

/INF14w01/ Infosec, API hooking, April 22 2014, https://resources.infosecinstitute.com/topic/api-hooking/, [abgerufen am 04.11.2022]

/INS18r01/ Inside IT: CCleaner-Hack: Raffinierte Malware mit Keylogger-Funktionalität entdeckt, 2018

/INT19r01/ India Today: What is DTrack: North Korean virus being used to hack ATMs to nuclear power plant in India

/INT20r01/ INTSIGHTS, Defend Forward, Russias Most Dangerous Cyber Threat Groups, 2020, https://www.intsights.com [abgerufen am 28.07.2020]

/IRN20w01/ IronNet, Adam Hlavek, Kimberly Ortiz, Russian cyber-attack campaigns and actors, The latest updates from IronNet threat intelligence research, 2020, https://www.ironnet.com/ [abgerufen am 04.11.2020]

/ITB16r01/ iTrust, Siddhant Shrivastava, BlackEnergy – Malware for Cyber-Physical Attacks, May 2016

/ITS22w01/ IT-Service, Verfassungsschutz warnt vor Cyberattacken, Hackergruppe APT27 greift mit Schadsoftware Hyperbro Unternehmen an, 02.02.2022, https://it-service.network/blog/2022/02/02/verfassungsschutz/, [abgerufen am 02.09.2022]

/JOE22w01/ Joecomp, Was sind symbolische Links? Wie erstellen Sie Symlinks in Windows 10?, 2022, https://joecomp.com/what-are-symbolic-links, [abgerufen am 04.11..2022]

/JUN20w01/ Jung, J., ZDnet, So greift EKANS Ransomware kritische Infrastrukturen an, https://www.zdnet.de/, 07.06.2020 [abgerufen am 05.05.2021]

/KAS19f01/ Kaspersky Lab Security Service Team, Radu Motspan, Alexander Korotin and Gleb Gritsai, On the insecure nature of turbine control systems in power generation, 36C3, Dezember 2019

/KAS19r01/ Kaspersky Lab: Operation ShadowHammer: a high-profile supply chain attack, 2019

/KAS21w01/ Kaspersky, What's behind APT29?, https://www.kaspersky.com [abgerufen am 18.04.2021]

/KIM19r01/ Kim, J. et al., Financial Security Institute, Republic of Korea, VB conference London 2019, KIMSUKY GROUP: TRACKING THE KING OF THE SPEAR PHISHING, Oktober 2019

/KOC18r01/ Kocher, P. et al., Spectre Attacks: Exploiting Speculative Execution, Januar 2018

/KRE20w01/ Krebs Security, Europes Largest Private HospitalOperator Fresenius Hit by Ransomware, https://krebsonsecurity.com/, 06.05.2020 [abgerufen am 05.05.2021]

/LIF19w01/ Lifars, APT32 in the Networks of BMW and Hyundai, 21 December 2019, https://lifars.com [abgerufen am 19.04.2021]

/LIP18r01/ Lipp, M. et al., Meltdown: Reading Kernel Memory from User Space, Januar 2018

/MAL17w01/ Malwarebytes Labs, How did the WannaCry Ransomware Worm spread, 19 May 2017, https://blog.malwarebytes.com [abgerufen am 12.01.2021]

/MAL19w01/ Malin, U. et al., Blackhat USA 2019 Vortrag, Rogue7: Rogue Engineering-Station Attacks on S7 Simatic PLCs, https://www.blackhat.com/, August 2019 [abgerufen am 29.04.2021]

/MAL20w01/ Malwarebytes Threat Intelligence Team, APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure, https://blog.malwarebytes.com/, 09.04.2020 [abgerufen am 21.12.2020]

/MAL21w05/ Malwarebytes LABS, UDP Technology IP Camerafirmware vulnerabilities allow forattacker to achieve root, July 28 2021, https://www.malwarebytes.com/, [abgerufen am 24.08.2022]

/MAN22w03/ Mandiant, UNC3524: Eye Spy on Your Email, May 02 2022, https://www.mandiant.com/resources/blog/unc3524-eye-spy-email, [abgerufen am 31.08.2022]

/MBC20w01/ MB Connect Line GmbH, Universelle Produkte für weltweite Fernwartung von Maschinen und Anlagen, https://www.mbconnectline.com/de/ [abgerufen am 15.07.2020]

/MCA18r01/ McAfee Labs: Operation Sharpshooter targets global Defense, Critical Infrastructure

/MED18r01/ Muyuan Li für Medium.com: The Sony Pictures Entertainment Hack Case Report, 2018

/MER20w01/ Mercer, W. et al., Talos Blog, Bisonal: 10 years of play, https://blog.talosintelligence.com/, 05.03.2020 [abgerufen am [26.10.2020]

/MIC15r01/ Microsoft, Microsoft Security Intelligence Report, Volume 19, January through June, 2015, 2015

/MIC17r01/ Microsoft Defender Security Research Team, WannaCrypt ransomware worm targets out-of-date systems, 12 May 2017, https://www.microsoft.com [abgerufen am 12.01.2021]

/MIC20w01/ Microsoft, CVE-2020-1472 Netlogon Elevation of Privilege Vulnerability

/MIC20w02/ Microsoft Security Intelligence Tweet, 24.09.2020, https://twitter.com/MsftSecIntel/status/ [abgerufen am 19.11.2020]

/MID18w01/ Midnight Blue Labs, Analyzing the TRITION industrial malware, https://www.midnightbluelabs.com, January 16, 2018 [abgerufen am 27.01.2020]

/MIT19w01/ MIT Technology Review, Triton is the worlds most murderous malware, and its spreading, Martin Giles, March 5, 2019

/MIT20w01/ MITRE ATT&CK, Groups, Dragonfly 2.0, October 2020, https://attack.mitre.org [abgerufen am 4.11.2020]

/NCS18i02/ National Cyber Security Centre, Reckless campaign of cyber-attacks by Russian military intelligence service exposed, 03.11.2018

/NER19r01/ "NERC, North American Electric Reliability Corporation, Lesson Learned, Risks Posed by Firewall Firmware Vulnerabilities, https://www.nerc.com/, 04.9.2021[abgerufen am 08.05.2021]

/NET20w01/ Netzwelt, Dropbear Schlanker SSH-Client und Server, 25.10.2020, https://www.netzwelt.de/, [abgerufen am 31.08.2022]

/NIS12n01/ National Institute of Standards and Technology, NIST Special Publication 800-30, Revision 1, Information Security, Guide for Conducting Risk Assessments, September 2012

/NIS15t01/ National Institute of Standards and Technology, NIST Special Publication 800-82, Revision 2, Guide to Industrial Control Systems (ICS) Security, May 2015

/NIS22i01/ NIST National Vulnerability Database NVD, CVE-2022-27588 Detail, 05.05.2022

/NIS22i02/ NIST National Vulnerability Database NVD, CVE-2021-44141 Detail 23.02.2022, CVE-2021-44142 Detail 23.02.2022

/NPR21r01/ NPR: FBI Called In After Hacker Tries To Poison Tampa-Area City's Water With Lye, Februar21

/NSA20i01/ NSA, National Security Agency, Cybersecurity Advisory, Sandworm Actors Exploiting Vulnerability in Exim Mail Transfer Agent, 28 May2020

/NVD18w01/ National Vulnerability Database NVD, CVE17-0144 Details, June2018, nist.gov [abgerufen am 25.01.2021]

/NYT12w01/ The New York Times, In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, 23 October 2012, https://www.nytimes,com [abgerufen am 22.04.2021]

/NYT17w01/ The New York Times, Hackers are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say, July 6, 2017, https://www.nytimes.com [abgerufen am 3.11.2020]

/NYT17w02/ The New York Times, Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core, 12 November 2017, https://www.nytimes.com [abgerufen am 11.11.2021]

/NYT17w03/ The New York Times, Cyberattack Hits Ukraine Then Spreads Internationally, https://www.nytimes.com [abgerufen am 27.06.2021]

/NYT20w02/ The New York Times, Russians Are Believed to Have Used Microsoft Resellers in Cyberattacks, 24 December 2020, https://www.nytimes.com [abgerufen am 14.04.2021]

/NYT21w01/ The New York Times, Blackout Hits Iran Nuclear Site in What Appears to Be Israeli Sabotage, 11. April 2021, updated 13. April 2021, https://www.nytimes.com [abgerufen am 21.04.2021]

/PAR15w01/ Park, J., Cho, M., Reuters, South Korea blames North Korea for December hack on nuclear opera-tor, https://www.reuters.com/, 17.03.2015 [abgerufen am 21.12.2020]

/PKM20r01/ PK Mallick, Cyber Attack on Kudankulam Nuclear Power Plant – A Wake Up Call, Center for Land Warfare Studies India, 2020

/POL20w01/ Politico, Nuclear weapons agency breached amid massive cyber onslaught, N. Betrand and E. Wolff, 17 December 2020, https://www.politico.com [abgerufen am 19.4.2021]

/PRS22w01/ ProSec, Cyberangriffskampagne gegen deutsche Wirtschaftsunternehmen, Situationsbeschreibung zur aktuellen Lage, https://www.prosec-networks.com, [abgerufen am 02.09.2022]

/PRV17r01/ Pravda: Der Virusangriff betraf das Kernkraftwerk Tschernobyl, Kiev 2017

/PUS19w01/ Pukhraj Singh Tweet: So, it's public now. Domain controller-level access at Kudankulam Nuclear Power Plant.

/QNA22i01/ QNAP, Security Advisory, Vulnerability in QVR, CVE-2022-27588, May 6 2022

/QNA22i02/ QNAP, Security Advisory, Multiple Vulnerabilities in Samba, CVE-2021-44141 | CVE-2021-44142 | CVE-2022-0336, February 10 2022

/QNA22w01/ QNAP, QNAP-Webseite, Ueber QNAP, https://www.qnap.com/de-de/about-qnap/, [abgerufen am 01.09.2022]/REG16w01/The Register, Today the web was broken by countless hacked devices your 60-second summary, 21 October 2016, https.//www.theregister.com [abgerufen am 22.04.2021]

/REC22w02/ Recorded Future, WhisperGate Malware Corrupts Computers in Ukraine, January 2022, https://www.recordedfuture.com, [abgerufen am 02.02.2022]

/REU20w01/ Reuters, Microsoft says it found malicious software in its systems, 17 December 2020, https://www.reuters.com [abgerufen am 19.4.2021]

/REU21r01/ Brazil’s Eletrobras says nuclear unit hit with cyberattack, 2021

/SAN14r01/ SANS Institute, Robert M. Lee, Michael J. Assante, Tim Conway, German Steel Mill Cyber Attack, 30. Dezember 2014

/SAN16r01/ SANS Institute, Information Security Reading Room, The Impact of Dragonfly Malware on Industrial Control Computers, Nell Nelson, 18 January 2016

/SCH18w02/ Schneider Electric, Industry Keynote, PAS OptICS 2018, April 2018

/SEA17w01/ The Seattle Times, Boeing hit by WannaCry virus, but says attack caused little damage, 28 March 2018, https://www.seatletimes.com [abgerufen am 13.01.2021]

/SEA19w01/ "Seals, T., threat post, Solar, Wind Power Utility Disrupted in Rare Cyberattack, 01.11.2019[abgerufen am 08.05.2021]"

/SEC10w01/ SecureWorks, Joe Stewart, BlackEnergy Version 2 Threat Analysis, 03. März 2010, https://www.secureworks.com [abgerufen am 23.12.2020]

/SEC10w02/ Securelist, Kaspersky, Black DDoS, 15 July 2010, https://securelist.com [abgerufen am 10.05.2021]

/SEC12w01/ Seculert, Shamoon, a two-stage targeted attack, 16 August 2012, http://blog.seculert.com [abgerufen am 22.04.2021]

/SEC12w03/ Securelist, Kaspersky, Shamoon the Wiper in details, 22 August 2012, https://securelist.com [abgerufen am 22.04.2021]

/SEC12w04/ Securelist, Kaspersky, Shamoon The Wiper: Further Details (Part II), 11 September 2012, https://securelist.com [abgerufen am 28.04.2021]

/SEC14w01/ Securelist, BE2 custom plugins, router abuse, and target profiles, 03 Nov 2014, https://securelist.com [abgerufen am 21.01.2021]

/SEC17w01/ Securelist, Kaspersky, New(ish) Mirai Spreader Poses New Risks, 21 February 2017, https://securelist.com [abgerufen am 24.08.2020]

/SEC19w02/ Secureworks, Threat Analysis, Resurgent Iron Liberty Targeting Energy Sector, July 2019, https://www.secureworks.com [abgerufen am 13.11.2020]

/SEC21w05/ Security Week, Over 250 Organizations Breached via SolarWinds Supply Chain Hack: Report, 4 January 2021, https://www.securityweek.com [abgerufen am 19.04.2021]

/SEC21w06/ Security Week, AP: Iran Calls Natanz Atomic Site Blackout 'Nuclear Terrorism', 11. April 2021, https://www.securityweek.com [abgerufen am 21.04.2021]

/SEC21w07/ Security Week, Cyberattack Forces Shutdown of Major U.S. Pipeline, 8 May 2021, https://www.securityweek.com [abgerufen am 11.05.2021]

/SEC21w08/ Security Week, Colonial Pipeline Targets Recovery From Ransomware Attack by End of Week, 10 May 2021, https://www.securityweek.com [abgerufen am 11.05.2021]

/SEN19r01/ Sentionel One: ASUS ShadowHammer Episode A Custom-Made Supply Chain Attack

/SEN22w02/ Sentinel One, AcidRain – A modem wiper rains down on Europe, 31 March 2022 [abgerufen am 08.08.2022]

/SIE15f01/ Siemens, Program Rewitalizacji Bloków 200MW, Vortrag, Katowice, 2015

/SIE18w01/ Siemens, SPPA-T3000 Broschüre, Karlsruhe, 2018

/SIE19i05/ Siemens Security Advisory by Siemens ProductCERT: SSA-686531: Hardware based manufacturing access on S7-1200

/SIE19i06/ Siemens Security Advisory by Siemens ProductCERT: SSA-232418: Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families

/SIE19r01/ Siemens, SSA-451445: Multiple Vulnerabilities in SPPA-T3000, December 2019

/SIE20r02/ Siemens Security Advisory by Siemens Product CERT: SSA-780073: Denial-of-Service Vulnerability in PROFINET Devices via DCE-RPC Packets, CVE-2019-13946, 2020

/SIE20r12/ Siemens Security Advisory by Siemens ProductCERT: SSA-818183: Denial-of-Service Vulnerability in SIMATIC S7-300 CPU Family, CVE-2016-3949, 2020

/SIE20r13/ Siemens ProductCERT, Siemens Security Advisory, SSA-541017: Embedded TCP/IP Stack Vulnerabilities (AMNESIA:33) in SIRIUS 3RW5 Modbus TCP and SENTRON PAC Devices, 08.12.2020

/SOC20w01/ SOC Prime, Andrii Bezverkhyi, Black Energy Phase 2: From Media and Electric Companies to Darknet and TTPS, https://socprime.com, [abgerufen am 28.07.2020]

/SOP19r01/ SophosLabs Research Team: Emotet exposed, looking inside highly destructive malware, Network Security Volume 2019, Issue 6, June 2019

/SPI22w02/ Der Spiegel, Hacker greifen norwegische Behörden-Webseiten an, 29.06.2022 [abgerufen am 09.08.2022]

/SSL20w01/ The SSL Store, Re-Hash: The Largest DDoS Attacks in History, 25 June 2020, https://www.thesslstore.com [abgerufen am 22.04.2021]

/STA22w01/ Star Advertiser, Cyberattack on Hawaii undersea communications cable thwarted by Homeland Security, April 12 2022, https://www.staradvertiser.com/, [abgerufen am 29.08.2022]

/SUS22i01/ SUSE, CVE-2022-0336, Common Vulnerabilities and Exposures, https://www.suse.com/, [abgerufen am 01.09.2022]

/SYM12r01/ Symantec Enterprise, Broadcom, The Shamoon Attacks, 16 August 2012, https://www.community,broadcom.com [abgerufen am 22.04.2021]

/SYM14r01/ Symantec, Symantec Security Response, Dragonfly: Cyberespionage Attacks Against Energy Suppliers, Version 1.21, 7 July 2014

/SYM16w01/ Symantec Enterprise, Broadcom, TShamoon: Back from the dead and destructive as ever, 30 November 2016, https://www.community,broadcom.com [abgerufen am 28.04.2021]

/SYM17r01/ Symantec, Threat Intelligence, Dragonfly: Western energy sector targeted by sophisticated attack group, 27 October 2017, https://symantec-enterprise-blogs.security.com [abgerufen am 16.06.2020]

/TAG21w01/ Tagesspiegel, Cyberangriff auf Irans Atomanlage? – Wer hinter dem Blackout in Natans stecken könnte, 12.04.2021, https://www.tagesspiegel.de [abgerufen am 21.04.2021]

/TAR13w01/ Tarakanov, D., Securelist by Kaspersky, The Kimsuky Operation: A North Korean APT?, https://securelist.com/, 11.09.2013 [abgerufen am 21.12.2020]

/TER20r01/ Zerologon: Unauthenticated domain controller compromise by subverting Netlogon cryptography (CVE-2020-1472), Whitepaper, Tom Tervoort, September 2020

/THA20f01/ Thales, Report on Cyber Threats to Operational Technologies in the Energy Sector, January 2020

/THP21w01/ Threatpost, FamousSparrow APT Wings in to Spy on Hotels, Governments, September 23 2021, https://threatpost.com/, [abgerufen am 16.11.2021]

/THR22w01/ The Record by Recorded Future, Who tried to hack Hawaii’s undersea cable?, April 27 2022, https://therecord.media/who-tried-to-hack-hawaiis-undersea-cable/, [abgerufen am 29.08.2022]

/TON20r01/ T-online Portal: Gefährlicher Trojaner Emotet wieder aktiv, Dezember 2020

/TRE14w01/ Trend micro, Korean Nuclear Plant Faces Data Leak and Destruction, https://www.trendmicro.com/, 22.12.2014 [abgerufen am 21.12.2020]

/TRE17w01/ Trend Micro, Bad Rabbit Ransomware Spreads via Network, https://www.trendmicro.com/, 24.10.2017 [abgerufen am 09.05.2021]

/TRE17w02/ Trend Micro, Bad Rabbit Ransomware What is it and how to stay safe, https://news.trendmicro.com/, 27.10.2017 [abgerufen am 09.05.2021]

/TRE19w01/ Trend Micro, What You Need to Know About the LockerGoga Ransomware, 20.03.2019 [abgerufen am 07.05.2021]

/TRM18r02/ TrendMicro: A Look into the Lazarus Group's Operations, 2018

/TWP20w01/ The Washington Post, Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce, 14 December 2020 [abgerufen am 14.04.2021]

/UAG15r01/ Unwala, Azhar and Ghori, Shaheen "Brandishing the Cybered Bear: In-formation War and the RussiaUkraine Conflict," Military Cyber Affairs: Vol. 1 : Iss. 1 , Article 7, 2015, https://scholarcommons.usf.edu, [abgerufen am 05.10.2020]

/WAL20w01/ Walter, J., SentinelLabs, Blogpost "New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware", Januar 2020 [abgerufen am 05.05.2021]

/WIE19w01/ Wieler, H., Infopoint Security, Europäische Industriebetriebe weiterhin im Visier von Cyberattacken, https://www.infopoint-security.de/, 29.03.2019 [abgerufen am 07.05.2021]

/WIR18r01/ Wored, Lily Hay Newman, Inside the Unnerving Supply Chain Attack That Corrupted CCleaner, 2018

/WIR19w01/ Wired, Andy Greenberg, Russia's 'Sandworm' Hackers Also Targeted Android Phones, 21.11.2019, https://www.wired.com/ [abgerufen am 04.11.2020]

/WIR20w01/ Wired, Andy Greenberg, NASA: Russia's Sandworm Hackers Have Hijacked Mail Servers, 28.05.2020, https://www.wired.com/ [abgerufen am 04.11.2020]

/WIR22w02/ Wired, The Unsolved Mystery Attack on Internet Cables in Paris, July 22, 2022, https://www.wired.com/story/france-paris-internet-cable-cuts-attack/, [abgerufen am 26.07.2022]

/WOR21w01/ World Today News, Cyber-attack on Sogin, the company that conserves nuclear waste: 800 Gb of data on sale for 250 thousand dollars, 14.12.2022

/WSJ20w01/ The Wall Street Journal, SolarWinds Hack Victims: From Tech Companies to a Hospital and University, 21 December 2020 [abgerufen am 14.04.2021]

/ZND14w01/ Zero Day Net, Charlie Osborne, Russian hackers target NATO, Ukraine through Windows zero-day exploit, October 14, 2014, https://www.zdnet.com, [abgerufen am 28.07.2020]

/ZDN18w01/ ZDNet, Shamoon malware destroys data at Italian oil and gas company, 13 December 2018, https://www.zdnet.com [abgerufen am 28.04.2021]

/ZDN18w02/ ZDNet, GreyEnergy: New malware campaign targets critical infrastructure companies, 17 October 2018, https://www.zdnet.com [abgerufen am 07.05.2021]

/ZDN19r02/ ZDnet; Employees connect nuclear plant to the internet so they can mine cryptocurrency, 2019

/ZDN19w01/ ZDNet, Iranian hackers deploy new ZeroCleare data-wiping malware, 4 December 2019, https://www.zdnet.com [abgerufen am 28.04.2021]

/ZDN20w01/ ZDNet, New Iranian data wiper malware hits Bapco, Bahrain's national oil company, 9 January 2020, https://www.zdnet.com
[abgerufen am 28.04.2021

Abbildungsverzeichnis

Relevante Fachbegriffe

Begriff	Definition
Advanced Persistent Threat	Advanced Persistent Threat bezeichnet im Rahmen der allgemeinen Bedrohungslage in Bezug auf die Informationssicherheit einen komplexen, von langer Hand geplanten und effektiven Angriff. Solch ein Angriff erfolgt fast immer stufenweise und enthält oft sehr zielgerichtete, spezifische Komponenten. Eine APT-Gruppierung kann zumeist auf große zeitliche und personelle Ressourcen zurückgreifen und wird nicht selten von nationalstaatlicher Seite finanziell gefördert. Häufige Ziele sind kritische Infrastrukturen und vertrauliche Informationen. Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren. /BSI20w01/ An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender’s efforts to resist it, and with determination to Maintain the level of interaction needed to execute its objectives. /NIS12n01/
Angriff	Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen. /BSI20w01/
Angriffsvektor	Als Angriffsvektor wird die Kombination von Angriffsweg und -technik bezeichnet, mit der sich ein Angreifer Zugang zu IT- Systemen verschafft. /BSI20w01/
Anwendungssoftware	Teil der Software eines leittechnischen Systems, durch den Anwendungsfunktionen realisiert werden. /DIN13n01/
Attribution/Attribuierung	Attribution bezeichnet den Analyse-Vorgang, den Urheber eines Angriffs zu benennen. In der Regel werden Attributionsaussagen durch Einschätzungen der Belastbarkeit ergänzt. /BSI20w01/

Begriff	Definition
Authentifizierung	Bei der Authentifizierung wird der bei der Authentisierung vorgelegte Identitätsnachweis einer Person überprüft. Erst nach erfolgreicher Authentifizierung erfolgt dann eine Autorisierung. /BSI20w01/
Authentisierung	Bei der Authentisierung legt eine Person einen Nachweis über ihre Identität vor, um ihn von einem System überprüfen zu lassen. Dies kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen. /BSI20w01/
Authentizität	Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder -Anwendungen. /BSI20w01/
Autorisierung	Bei der Autorisierung werden für eine bereits erfolgreich authentifizierte Person die ihr auf einem System eingeräumten Rechte freigeschaltet. /BSI20w01/
Bedrohung	Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung. /BSI20w01/
Backdoor	Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang ("Hintertür") zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. /BSI20w01/
Bot / Bot-Netz	Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert. /BSI20w01/

Begriff	Definition
Brute Force Angriff	Wählen Nutzer ein schwaches Passwort und ist der Benutzername (z. B. die E-Mail-Adresse) bekannt, kann sich ein Angreifer unter Umständen auch durch wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken kann der Angreifer auch versuchen, kryptografisch geschützte Daten, z. B. eine verschlüsselte Passwort-Datei, zu entschlüsseln. /BSI20w01/
Command & Control Server (C&C Server)	Die meisten Schadprogramme nehmen nach der Infektion eines Systems Kontakt zu einem Kontrollserver (C&C-Server) der Angreifer im Internet auf, um von dort weiteren Schadcode nachzuladen, Instruktionen zu empfangen oder auf dem infizierten System ausgespähte Informationen (wie Benutzernamen und Passwörter) an diesen Server zu übermitteln. Die Kontaktaufnahme erfolgt häufig unter Verwendung von Domainnamen, welche von den Tätern speziell für diesen Zweck registriert wurden. /BSI20w01/
Credentials	Typische Beispiele für Credentials sind Passwörter, kryptografische Schlüssel und Zertifikate, sog. "Authentisierungs-Tickets" oder auch "Session-Cookies". Ein Diebstahl von Credentials kann z. B. Folge einer Attacke auf die Benutzerdatenbank von Webseiten oder Online-Diensten sein. Credentials können auch durch Schadsoftware-Infektionen auf Clients mitgeschnitten und so unbefugt an Dritte übermittelt werden. Es können aber auch gezielt Geräte wie Smartphones, Hardware-Tokens oder mobile Datenträger gestohlen werden, wenn ein Angreifer Zugangsdaten auf diesen Komponenten vermutet. Authentisierungs-Tickets oder Cookies können über unverschlüsselte Verbindungen mitgeschnitten werden. /BSI20w01/
Credential Harvesting	Credential Harvesting bezeichnet den Prozess zur Erbeutung von legitimen Benutzernamen, Passwörtern und Hashes (typischerweise mit Hilfe einer Schadsoftware oder Social Engineering Techniken wie Phishing) mit dem Ziel, sich innerhalb eines Cyberangriffs mit diesen Nutzerdaten einzuloggen und so von einem autorisierten Nutzer zunächst nicht unterscheidbar zu sein.
Common Vulnerabilities and Exposures (CVE)	Bei den Common Vulnerabilities and Exposures (Häufige Schwachstellen und Risiken) handelt es sich um eine Sammlung öffentlich bekannter Schwachstellen in IT-Systemen. Mit CVE wird in der Regel die CVE-Nummer gemeint, die einer bestimmten Schwachstelle eindeutig zugewiesen ist.
Cyberangriff	Siehe IT-Angriff

Begriff	Definition
Demilitarisierte Zone (DMZ)	Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. DMZ werden bei einfachen Sicherheitsgateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheitsgateway aus Paketfilter – Application-Level-Gateway – Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level-Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden. /BSI20w01/
DOS / DDoS-Angriffe	Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern. /BSI20w01/
Dropper	Als Dropper werden Schadsoftwarekomponenten bezeichnet, die mindestens eine weitere Payload enthalten und dafür verantwortlich sind, diese ggf. zu entschlüsseln und auszuführen.
Ethernet	Eine Technologie zur Vernetzung von Computern in lokalen Netzen (Local Area Networks, kurz LAN). /BSI20w01/
Exploit	Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden. /BSI20w01/
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. /BSI20w01/
Hashfunktion	Eine Hashfunktion ist ein kryptographischer Algorithmus, bei dem Nachrichten beliebiger Länge auf einen Hashwert fester Länge (z. B. 160 Bit) abgebildet werden. Bei kryptographisch geeigneten Hashfunktionen ist es praktisch unmöglich, zwei Nachrichten mit dem gleichen Hashwert zu finden (Kollisionsresistenz) und bei einem gegebenen Hashwert eine Nachricht zu finden, die durch die Hashfunktion auf den Hashwert abgebildet wird (Einwegeigenschaft). /BSI20w01/

Begriff	Definition
Hashwert	Ein Hashwert ist eine mathematische Prüfsumme, die durch Anwendung einer Hashfunktion aus einer elektronischen Nachricht erzeugt wird. Da es bei einer kryptographisch geeigneten Hashfunktion praktisch unmöglich ist, zwei Nachrichten zu finden, deren Hashwert identisch ist, bezeichnet man den Hashwert auch als "digitalen Fingerabdruck" einer Nachricht. Da man auf Grund des so genannten Geburtstagsparadoxon mit großer Wahrscheinlichkeit eine Kollision bei einer l-Bit-Hashfunktion findet, wenn man etwa 2l/2 zufällige Nachrichten wählt, sollte eine Hashfunktion, die für elektronische Signaturen eingesetzt werden soll, mindestens 160 Bit Hashwerte produzieren. /BSI20w01/
Host	Alternative Bezeichnung für Server. /BSI20w01/
Indicators of Compromise (IoCs)	Indicators of Compromise sind technische Informationen, die zur Detektion einer Infektion mit Schadsoftware oder einer anderweitigen Kompromittierung verwendet werden können. Häufig handelt es sich dabei um netzwerkbasierte Signaturen wie Domainnamen von Kontrollservern, oder um hostbasierte Signaturen, die auf den Endgeräten gesucht werden (wie Hashsummen von Schadprogrammen, Einträge in der Windows-Registry, o.ä.). /BSI20w01/
Industrial Control System (ICS)	ICS ist ein Oberbegriff für Automatisierungslösungen zur Steuerung technischer Prozesse. /BSI20w01/
Industrial Internet of Things (IIoT)	Industrielle Ausprägung des IoT.
Informationsinfrastruktur	Die Gesamtheit der IT-Anteile einer Infrastruktur. /BSI20w01/
Informationssicherheit	Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein. /BSI20w01/
Informationstechnik (IT)	Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen. /BSI20w01/

Begriff	Definition
Innentäter	Cyber-Angriffe durch Innentäter haben größere Aussicht auf Erfolg als Angriffe von außen, da der Angreifer bereits Zugang zu internen Ressourcen einer Organisation hat und so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren kann. Zusätzliche Vorteile genießen Innentäter durch das ihnen entgegengebrachte Vertrauen einer Organisation. Externe Dienstleister, die durch ihre Tätigkeit Einfluss oder direkten Zugang zur Organisation haben, werden hier ebenfalls zu den Innentätern gezählt. /BSI20w01/
Integrität	Sicherstellung der Korrektheit von Informationen und der korrekten Funktionsweise von Systemen. Zur Integrität von Informationen gehören auch deren Vollständigkeit und die Korrektheit von Angaben zu Sender und Empfänger sowie von Zeitangaben der Erstellung, Veränderung und des Empfangs. Zur Integrität von Systemen gehört auch die Korrektheit von Herkunft, Einsatzumgebung sowie von Zeitangaben der Erstellung und Änderung. /BMU13n03/
Internet of Things (IoT)	IoT steht für Internet of Thing, also das Internet der Dinge. Im Gegensatz zu "klassischen" IT-Systemen umfasst das Internet der Dinge "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden. /BSI20w01/
IT-Angriff	Bei einem IT-Angriff handelt es sich um eine vorsätzliche Einwirkung auf eines oder mehrere IT-Systeme der Anlage, die deren Kompromittierung (d. h. Beeinträchtigung von deren IT-Sicherheit) zum Ziel hat.
IT-Schutzziel	Schutzbedürftige IT-Systeme und die zugehörigen Prozesse sind entsprechend ihres Schutzbedarfes gestuft gegen SEWD zu schützen, sodass eine Verletzung der allgemeinen Schutzziele weder unmittelbar noch mittelbar herbeigeführt werden kann. /BMU13n03/

Begriff	Definition
IT-Sicherheit	IT-Sicherheit ist der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind. /BMU13n03/ Satz von Tätigkeiten und Maßnahmen, die darauf abzielen Folgendes zu verhindern, zu entdecken und darauf zu reagieren: – böswillige Veränderungen (Integrität) von Funktionen, die die Ausführung oder Unversehrtheit der durch programmierbare digitale leittechnische Systeme zu erbringenden Dienste beeinträchtigen können (einschließlich Kontrollverlust), was zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnte; – böswilliges Zurückhalten oder Verhindern von Zugriff auf oder Austausch von Informationen, Daten oder Ressourcen (einschließlich Anzeigeverlust), was die Ausführung der durch leittechnische Systeme zu erbringenden Dienste beeinträchtigen könnte (Verfügbarkeit), was zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnte; – böswillige Offenlegung von Informationen (Vertraulichkeit), was dazu benutzt werden könnte, böswillige Handlungen vorzunehmen, die zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnten; /DIN20n01/
IT-Sicherheitsvorfall	Ein IT-Sicherheitsvorfall ist ein Vorfall, der die IT-Sicherheit in einer Weise beeinträchtigt, dass Rückwirkungen auf die Sicherheit oder Sicherung der Anlage nicht ausgeschlossen werden können. Beispiele für IT-Sicherheitsvorfälle können erfolgreiche Cyberangriffe, Versagen von Sicherungsmaßnahmen, Verletzung von internen IT-Sicherheitsvorgaben und das Auftreten oder Bekanntwerden von Schwachstellen in IT-Produkten oder IT-Dienstleistungen sein, soweit Rückwirkungen auf die Sicherheit oder Sicherung der Anlage bestehen. /BMU13n03/
IT-System	System der Informationstechnik. IT-Systeme sind jegliche Art von programmgesteuerten Komponenten oder Systemen /BMU13n03/, insbesondere auch Automatisierungs-, Prozesssteuerungs- oder Leittechniksysteme. Hierzu zählen auch alle rechnerbasierten oder programmierbaren Komponenten oder Systeme, die durch externe Geräte konfiguriert oder parametriert werden können.

Begriff	Definition
IT-System, schutzbedürftiges	Als schutzbedürftige IT-Systeme im Sinne der SEWD-Richtlinie IT /BMU13n03/ gelten alle IT-Systeme, die vom Betreiber oder in seinem Auftrag betrieben werden und mit der Anlage in einem engen räumlichen, informationstechnischen oder betrieblichen Zusammenhang stehen und die unmittelbar oder mittelbare zur Herbeiführung einer Verletzung der allgemeinen Schutzziele verwendet werden können. Ein enger räumlicher Zusammenhang liegt vor, wenn das IT-System sich dauerhaft innerhalb der Umschließung der äußeren Sicherungsbereiche befindet. Ein enger informationstechnischer Zusammenhang liegt vor, wenn das IT-System über informationstechnische Systeme dauerhaft oder regelmäßig mit der Anlage verbunden ist. Ein enger betrieblicher Zusammenhang liegt vor, wenn das IT-System der Verarbeitung von Informationen für den Betrieb der Anlage dient. /BMU13n03/
Keylogger	Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern. /BSI20w01/
Living-off-the-Land	Living-off-the-Land bezeichnet ein Angreiferverhalten, bei dem die Angreifer auf Dateien, Skripte, Werkzeuge und Informationen zurückgegriffen wird, die auf den angegriffenen System bereits vorhanden sind, und diese maliziös einsetzen.
Loader	Als Loader werden Schadsoftwarekomponenten bezeichnet, die dafür verantwortlich sind, weitere Schadsoftwarekomponenten von einer angegebenen URL/IP-Adresse herunterzuladen, ggf. zu entschlüsseln und auszuführen.
Malware	Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben. /BSI20w01/

Begriff	Definition
Man-In-The-Middle-Angriff	Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer "in die Mitte" der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind. /BSI20w01/
Netzwerk	Verbund von Rechnern, die untereinander Daten austauschen. Netzwerk-Rechner können als Host bzw. Server Daten zur Verfügung stellen oder als Client auf diese zugreifen. In manchen Netzwerken üben die verbundenen Rechner auch beide Funktionen gleichzeitig aus. /BSI20w01/
Netzwerkstack	Bei einem Netzwerkstack oder auch Protokollstack handelt es sich um die Implementierung einer Reihe von zueinander in Beziehung stehenden Kommunikationsprotokollen.
Nichtabstreitbarkeit (englisch "non repudiation")	Hierbei liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann. Es wird unterschieden zwischen - Nichtabstreitbarkeit der Herkunft: Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten. - Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten. /BSI20w01/
Patch / Patch-Management	Ein Patch ("Flicken") ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren. Die Einspielung dieser Updates erleichtern viele Programme durch automatische Update-Funktionen. Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können. /BSI20w01/

Begriff	Definition
Payload	Payload („Nutzlast“ bzw. „Nutzdaten“) bezeichnet im Zusammenhang mit Cyberangriffen typischerweise diejenigen Schadsoftwarekomponenten, die maliziöse Aktivitäten (Manipulation von Daten oder Prozessen, Diebstahl von Nutzerdaten, Spionage etc.) ausführen. Ein Cyberangriff oder auch eine Schadsoftware kann daher mehrere Payloads enthalten, aber typischerweise besteht nicht die gesamte Schadsoftware aus Payloads, sondern enthält noch weitere Komponenten (z. B. Metadaten, Bibliotheken etc.).
Phishing	Das Wort setzt sich aus "Password" und "Fishing" zusammen, zu Deutsch "nach Passwörtern angeln". Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände. /BSI20w01/
Poisoning	Unter "Poisoning" versteht man das Einschleusen von manipulierten Daten in einen Zwischenspeicher (Cache), der dann von anderen Anwendungen oder Diensten genutzt wird. Beispiele sind Angriffe mittels Poisoning auf DNS-, BGP-, oder ARP-Caches. /BSI20w01/
Port	Ein Port spezifiziert einen Dienst, der von außen auf einem Server angesprochen werden kann. Dadurch ist es möglich, auf einem Server verschiedene Dienste (z. B. WWW und E-Mail) gleichzeitig anbieten zu können. /BSI20w01/
Port-Scan	Bei einem Port-Scan versucht ein Angreifer herauszufinden, welche Dienste ein Rechner nach außen anbietet, in dem er alle nacheinander "anspricht". Ein Port-Scan dient in der Regel dazu einen Angriff vorzubereiten. /BSI20w01/
Protokoll	Beschreibung (Spezifikation) des Datenformats für die Kommunikation zwischen elektronischen Geräten. /BSI20w01/
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch "ransom") wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung. /BSI20w0/
Remote Access Trojan	Schadsoftware, die den Angreifern durch Etablierung einer Backdoor Zugriff auf das infizierte IT-System verschafft.
Rootkit	Ein Rootkit ist ein Schadprogramm, das manipulierte Versionen von Systemprogrammen enthält. Unter Unix sind dies typischerweise Programme wie login, ps, who, netstat etc. Die manipulierten Systemprogramme sollen es einem Angreifer ermöglichen, zu verbergen, dass er sich erfolgreich einen Zugriff mit Administratorenrechten verschafft hat, so dass er diesen Zugang später erneut benutzen kann. /BSI20w01/

Begriff	Definition
Sandbox	Eine Sandbox ist ein isolierter Bereich innerhalb einer Anwendung oder eines Betriebssystems. Sie verhindert, dass unerwünschte Aktionen außerhalb des kontrollierten Umfelds ausgeführt werden können. Dadurch werden die Gefahren und Auswirkungen von Schadprogrammen abgewehrt. /BSI20w01/
Schadsoftware	Siehe Malware
Schutzziele, allgemeine	Laut SEWD-RL IT /BMU13n03/ dient die Einhaltung der folgenden allgemeinen Schutzziele der Gewährleistung des erforderlichen Schutzes gegen SEWD: - Eine Gefährdung von Leben und Gesundheit infolge erheblicher Direktstrahlung oder infolge der Freisetzung einer erheblichen Menge radioaktiver Stoffe aus Kernbrennstoffen vor Ort muss verhindert werden können. - Eine einmalige oder wiederholte Entwendung von Kernbrennstoff in Mengen, mit denen ohne Wiederaufbereitung und Anreicherung die Möglichkeit der unmittelbaren Herstellung einer kritischen Anordnung gegeben ist, muss verhindert werden können. - Eine einmalige oder wiederholte Entwendung von Kernbrennstoff in Mengen, mit denen eine Gefährdung von Leben und Gesundheit infolge erheblicher Direktstrahlung oder Freisetzung einer erheblichen Menge radioaktiver Stoffe aus Kernbrennstoffen an einem anderen Ort möglich ist, muss verhindert werden können.
Schutzziel, IT	Siehe IT-Schutzziel
Schwachstelle (englisch "vulnerability")	Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen. /BSI20w01/
Shellcode	In Bezug auf Cyberangriffe bezeichnet Shellcode eine typischerweise sehr kleine Schadsoftwarekomponente, die für den Angreifer auf dem kompromittierten System eine Kommandozeile (Shell) öffnet.
Spear-Phishing	Spear-Phishing ist eine Spezialform eines Phishing-Angriffs, bei dem nicht breitflächig, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträger auf Leitungsebene) attackiert wird. Voraussetzung für einen erfolgreichen Angriff ist eine gute Vorbereitung und die Einbettung des Angriffs in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich in der Regel nicht gegen allgemein nutzbare Dienste wie Online-Banking, sondern gegen Dienste, die für Angreifer einen besonderen Wert haben. /BSI20w01/

Begriff	Definition
Verfügbarkeit	Eigenschaft, auf Anforderung durch eine berechtigte Instanz zugänglich und benutzbar zu sein. /DIN20n01/ Sicherstellung, dass Informationen und Systemfunktionen wie vorgesehen bereitstehen. /BMU13n03/
Vertraulichkeit	Eigenschaft, dass Informationen nichtautorisierten Personen, Instanzen oder Prozessen nicht verfügbar gemacht oder offengelegt werden. /DIN20n1/ Sicherstellung, dass Informationen unbefugten Personen nicht zugänglich werden können. /BMU13n03/
Watering-Hole-Angriff	Bei einem Watering-Hole-Angriff kompromittieren die Angreifer gezielt eine von den potenziellen Opfern häufig oder immer wieder aufgesuchte Webseite. Je nach Absicht der Angreifer infizieren sie beispielsweise die Webseite mit Spionage-Software oder injizieren Schadcode in zum Download bereitstehende Dateien.
Wiper	Als Wiper bezeichnet man einen Typ von Schadsoftware, deren Zweck die Zerstörung von Daten von Festplatten und anderen Datenträgern ist. Hierzu werden die entsprechenden Daten entweder gelöscht oder mit anderen Daten überschrieben.
Zero-Day-Exploit	Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff Zero-Day-Exploit. Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Begriff Zero-Day leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch den Hersteller existierte – also an einem fiktiven "Tag Null". Der Hersteller hat somit keine Zeit, die Nutzer vor den ersten Angriffen zu schützen. /BSI20w01/
Zugang	Mit Zugang wird die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet. Zugangsberechtigungen erlauben somit einer Person, bestimmte Ressourcen wie IT-Systeme bzw. System-Komponenten und Netze zu nutzen. /BSI20w01/
Zugriff	Mit Zugriff wird die Nutzung von Informationen bzw. Daten bezeichnet. Über Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen. /BSI20w01/

Begriff	Definition
Zutritt	Mit Zutritt wird das Betreten von abgegrenzten Bereichen wie z. B. Räumen oder geschützten Arealen in einem Gelände bezeichnet. Zutrittsberechtigungen erlauben somit Personen, bestimmte Umgebungen zu betreten, also beispielsweise ein Gelände, ein Gebäude oder definierte Räume eines Gebäudes. /BSI20w01/

Abkürzungsverzeichnis

APT	Advanced Persistent Threat
BSI	Bundesamt für Sicherheit in der Informationstechnik
CISA	Cybersecurity and Infrastructure Security Agency
CNMF	Cyber National Mission Force
CPU	Central Processor Unit
CVE	Common Vulnerabilities and Exposures
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DMZ	Demilitarisierte Zone
DoS	Denial of Service
EWS	Engineering Work Station
HMI	Human Machine Interface
ICS	Industrial Control System
IIoT	Industrial Internet of Things
IoT	Internet of Things
IT	Information Technology
MBR	Master Boot Record
OT	Operational Technology
PLC	Programmable Logic Controller
RAT	Remote Access Trojan
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition system
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SPS	Speicherprogrammierbare Steuerungen

Anhang

In den folgenden Abschnitten werden nach Jahren sortiert ausgewählte Schwachstellen und Angriffswerkzeuge, IT-Sicherheitsvorfälle und Cyberangriffe der vergangenen Jahre vorgestellt. Hierbei handelt es sich nur um einen relevanten Ausschnitt der Gesamt-Bedrohungslage, der keinerlei Anspruch auf Vollständigkeit erhebt.

A Schwachstellen und Angriffswerkzeuge

In den folgenden Abschnitten werden für industrielle Steuerungssysteme und kritische Infrastrukturen besonders relevante und weitere herausragende Schwachstellen beschrieben. Den Beginn in Bezug auf Schwachstellen machen hierbei zwei im Jahr 2018 bekannt gewordene Schwachstellen in gängigen Prozessoren. In den Jahren 2019 und 2020 wurden mehrere Schwachstellen bekannt, welche industrielle Steuerungssysteme oder dabei eingesetzte leittechnische Komponenten betreffen. Zusätzlich waren auch immer wieder Kommunikationsstandards und Netzwerkstacks von teils schwer-wiegenden Schwachstellen betroffen, zuletzt im Jahr 2021.

Darüber hinaus werden in den folgenden Abschnitten auch Angriffswerkzeuge beschrieben, deren Einsatz zunächst keinem bekannt gewordenen Cyberangriff zugeordnet werden kann. Das erste beschriebene, bei einem Cyberangriff eingesetzte Angriffswerkzeug, welches bereits im Jahr 2017 bekannt wurde, dient dem Aufbau einer Kommunikation über Air-Gaps hinweg, beim zweiten Angriffswerkzeug, das im Jahr 2020 bekannt wurde, handelt es sich um ein klassisches Spionagewerkzeug.

A.1 2017

A.1.1 Brutal Kangaroo – Angriffswerkzeug der CIA

Übersicht

Am 22.07.2017 veröffentlichte WikiLeaks interne Dokumente des US-amerikanischen Nachrichtendienstes CIA /CIA12r01, CIA13r01, CIA13r02, CIA16r01/ zu einem Set von Angriffswerkzeugen bzw. Schadsoftwarekomponenten, die von der CIA unter dem Projektnamen Brutal Kangaroo (in früheren Versionen EZCheese) entwickelt

wurden /WIK17w01/. Die darin beschriebenen Schadsoftwarekomponenten dienen der Infektion von Systemen und Netzwerken über Air-Gaps hinweg /BSI17i06/.

Beschreibung

Die unter Brutal Kangaroo zusammengefassten Schadsoftwarekomponenten ermöglichen in mehreren Angriffsstufen zunächst die Infektion eines an das Internet angebundenen Rechners (Primary Host) der Zielorganisation, von dort aus die Infektion von dedizierten USB-Sticks, die an diesen ersten Rechner angeschlossen werden, zum Über-springen des Air-Gaps und schließlich über einen der so manipulierten USB-Sticks die Infektion des durch ein Air-Gap getrennten Systems oder Netzwerks. Der dort installierte Schadcode dient der gezielten Ausspähung von Informationen. Diese werden gesammelt und im weiteren Verlauf auf jeden manipulierten USB-Stick geschrieben, der mit einem infizierten System verbunden wird. Hierbei wird auf verschiedene Techniken zu-rückgegriffen, um die Dateien zu verstecken und den Datenabfluss vor dem Nutzer zu verbergen. Analog zum Infektionsweg realisiert Brutal Kangaroo den Exfiltrationsweg für die auf dem Zielsystem oder im Zielnetzwerk ausgespähten Informationen über einen der infizierten USB-Sticks zurück zu einem der ursprünglich infizierten, an das Internet angebundenen Rechner und letztlich von dort aus zu einem Rechner der Angreifer. /BSI17i06/

Brutal Kangaroo stellt so mit der Zeit Kommunikationskanäle nicht nur zwischen dem Rechner der Angreifer und einem durch ein Air-Gap getrennten System oder Netzwerk her, sondern auch zwischen den verschiedenen, typischerweise ebenfalls nicht miteinander verbundenen infizierten Systemen innerhalb der Zielorganisation. Damit wird asynchroner Informationsaustausch nicht nur zwischen den Angreifern und einem durch ein Air-Gap getrennten System ermöglicht, sondern auch der Informationsaustausch beispielsweise zwischen verschiedenen, jeweils durch ein Air-Gap getrennten Systemen. De facto wird dadurch ein ursprünglich nicht vorgesehenes Netzwerk über Air-Gaps hinweg realisiert. /BSI17i06/

Brutal Kangaroo deckt keinen vollständigen Cyberangriff ab, sondern kann als Teil eines komplexen, mehrstufigen Angriffs eingesetzt werden. So fällt die Infektion des Primary Host mit Brutal Kangaroo nicht in den Aufgabenbereich von Brutal Kangaroo, sondern muss unter Einsatz anderer Angriffswerkzeuge und -techniken erreicht werden. Brutal Kangaroo selbst, besteht aus mehreren Schadsoftwarekomponenten:

- Shattered Assurance (ersetzt Teile der älteren Schadsoftwarekomponente Emotional Simian) /CIA13r02, CIA16r01/: Schadsoftwarekomponente, die für die Infektion von USB-Sticks sorgt, welche mit dem infizierten Rechner verbunden werden.
- Drifting Deadline (ersetzt die ältere Schadsoftwarekomponente EZCheese und Teile der älteren Schadsoftwarekomponente Emotional Simian) /CIA13r01, CIA13r02, CIA16r01/: Individuell konfigurierbare Schadsoftwarekomponente zur Infektion der USB-Sticks. Diese Komponente wird ausgeführt, sobald der USB-Stick mit einem weiteren Rechner verbunden wird, was zum einen zur Infektion dieses Rechners führt und zum anderen zu dessen Ausspähung.
- Broken Promise /CIA16r01/: Schadsoftwarekomponente zur Auswertung und Analyse der gesammelten Informationen.
- Shadow /CIA12r01, CIA16r01/: Schadsoftwarekomponente, welche die Persistenz der Angreifer und den unbemerkten Transport der ausgespähten Informationen sicherstellt. Auf jedem infizierten Rechner wird eine Shadow-Instanz installiert. Sobald es mehrere Shadow-Instanzen gibt, die sich USB-Sticks teilen, können Informationen, Aufgaben und weitere Schadsoftwarekomponenten in dem so aufgespannten Netzwerk verteilt werden.

Bei der Infektion der Rechner werden unter anderem verschiedene LNK-basierte Schwachstellen im Windows-Betriebssystem ausgenutzt und entsprechende CIA Exploits eingesetzt /CIA16r01/. Die Ausnutzung LNK-basierter Schwachstellen in Verbindung mit dem Überspringen der Barriere Air-Gap über manipulierte USB-Sticks erinnern an die Vorgehensweise bei den Cyberangriffen im Zusammenhang mit der Schadsoftware Stuxnet (siehe Abschnitt B.1.1).

Laut Cyber-Sicherheitswarnung des BSI /BSI17i06/ zu diesem Sachverhalt ist über die in den Dokumenten der CIA beschriebene Nutzung von Brutal Kangaroo auch „eine Abstraktion der beschriebenen Netzwerkbildung grundsätzlich denkbar“, anstelle der Erstinfektion eines ans Internet angebundenen Rechners in der Zielorganisation „könnte der Angriff auch – entsprechenden Austausch von USB-Wechseldatenträgern vorausgesetzt – auch vollständig ohne Netzwerkverbindungen, auch zum Internet, durchgeführt werden“.

Das als Brutal Kangaroo zusammengefasste Set von Angriffswerkzeugen zeigt laut BSI, dass die Realisierung eines Air-Gaps zur physikalischen Trennung schützenswerter

Systeme von Netzwerken als alleinige Schutzmaßnahme „unzureichend“ ist. Des Weiteren geht das BSI davon aus „dass weltweit zahlreiche weitere Nachrichtendienste oder kriminelle Organisationen entsprechende Werkzeuge gegen durch Isolation besonders geschützte Systeme entwickelt haben und für zielgerichtete Angriffe einsetzen“. /BSI17i06/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.2 2018

A.2.1 Meltdown – Schwachstellen in CPUs

Übersicht

Im Januar 2018 veröffentlichten Forscher von Googles Project Zero, Cyberus Technology und der TU Graz mit dem Paper „Meltdown: Reading Kernel Memory from User Space“ /LIP18r01/ erstmalig Informationen zu einer Hardware-Sicherheitslücke in modernen Prozessoren, durch die ein unautorisierter Zugriff auf den Speicher des Systems, in dem der Prozessor eingebaut, ist bzw. ein unautorisierter Zugriff auf andere Prozesse und auch Prozesse anderer Nutzer (fremde Prozesse) erfolgen kann. Die Schwachstelle entstand bei der Entwicklung von Prozessoren (CPUs) und betrifft den überwiegenden Teil heutiger Modelle der Prozessoren unabhängig vom Betriebssystem. Betroffen sein können entsprechend alle Geräte, die eine bzw. mehrere CPUs besitzen, wie beispielsweise Notebooks, Desktop-Computer, Cloud-Computing Geräte und Smartphones. Dabei ist hauptsächlich der marktführende Hersteller Intel betroffen, aber auch andere Hersteller wie beispielweise ARM oder IBM. Bereits vor der Veröffentlichung der Schwach-stelle mit der CVE-Nummer CVE-2017-5754 wurden betroffene Hard- und Software-Hersteller von den Forschern im Jahr 2017 informiert.

Beschreibung

Die folgenden Ausführungen beschreiben die Ursachen der Schwachstelle und Möglichkeiten diese auszunutzen. In diesem Zusammenhang gibt es weiterhin die Schwachstelle Spectre, deren Entdeckung zusammen mit Meltdown veröffentlicht wurde und auf ähnlichen Prinzipien basiert (siehe dazu das folgende Abschnitt A.2.2).

Die Schwachstelle Meltdown ist hauptsächlich in der Eigenschaft moderner Prozessoren begründet, Befehle potenziell nicht in der festgelegten, sondern einer beliebigen Reihenfolge durchzuführen (Out-of-Order-Execution). Dazu kommt die sogenannte Speculative Execution, bei der die CPU nicht erst einen Befehl komplett ausführt, bevor sie mit dem nächsten beginnt, sondern möglichst mehrere Befehle parallel bearbeitet, die dann verschiedene Stufen durchlaufen. Dies dient der schnelleren Verarbeitung von Befehlen und erhöht die Rechengeschwindigkeit von Prozessoren, da die Auslastung optimiert wird.

Dieses Vorgehen führt zu Komplikationen, wenn beispielsweise Befehle Abhängigkeiten untereinander haben oder es zu Verzweigungen (Branches) im Code kommt. In diesem Fall führt die Speculative Execution dazu, dass die CPU eine Vorhersage trifft, ob eine bestimmte Verzweigung im Code genommen wird (sogenannte Branch Prediction) und die weiteren Befehle ausführt. Falls sich die Vorhersage als richtig herausstellt, setzt die CPU die Ausführung der nachfolgenden Befehle fort. Für den Fall, dass die Vorhersage falsch war, werden die falsch ausgeführten Aktionen verworfen und der Zeitverlust gleicht höchstens dem Warten der CPU, wenn er keine Vorhersage getroffen hätte. Dies führt im Zusammenhang mit der Speicherarchitektur und dem Zugriff der CPU auf den Speicher zu der als Meltdown bekannten Schwachstelle.

In der heutigen Zeit laufen unterschiedliche Programme und Prozesse in einer isolierten Umgebung (Sandbox) mit virtuellem Speicher ab, sodass einzelne Prozesse keinen Zugriff auf das Gesamtsystem oder den gesamten physikalischen Speicher, sondern nur auf den jeweils zugewiesenen Speicherbereich haben. Da einzelne Prozesse jedoch auch Betriebssystemfunktionen benötigen, haben sie einen definierten Zugriff auf den Kernel (zentraler Bestandteil des Betriebssystems) des Systems, der mit einer Zugriffskontrolle durch die CPU verbunden ist, sodass nur definierte und erlaubte Zugriffe durch die Prozesse möglich sind. Zugriffe auf nicht erlaubte Speicherbereiche werden durch die CPU unterbunden. Außerdem können bestimmte Bereiche des Speichers, die

beispielsweise Passwörter enthalten, speziell geschützt sein. Die Abbildung des virtuellen auf den physikalischen Speicher erfolgt durch die CPU und das Betriebssystem.

Die Schwachstelle Meltdown nutzt in diesem Zusammenhang aus, dass die CPU im Fall einer falschen Vorhersage (Branch Misprediction) ggf. Befehle ausführt, die beispielsweise aufgrund fehlender Berechtigungen nicht hätten ausgeführt werden dürfen. Obwohl die CPU diesen Umstand bemerkt und die durchgeführten Aktionen anschließend verwirft, können bei der Ausführung der spekulativ ausgeführten Befehle Informationen aus dem (physikalischen) Speicher in den internen Speicher (Cache) der CPU übertragen werden. Der Zugriff auf die Informationen im Cache des CPU ist nicht trivial, kann jedoch durch entsprechend gestaltete Programme durchgeführt werden. Somit kann der Cache dazu verwendet werden, Daten zu erhalten, auf die unter normalen Umständen aufgrund fehlender Berechtigungen nicht zugegriffen werden könnte.

Um diese Schwachstelle auszunutzen, werden keine weiteren Hilfsmittel benötigt. Angreifer brauchen lediglich eine Zugriffsmöglichkeit auf das System, die es erlaubt, Code auszuführen. Da es sich um eine Hardware-Schwachstelle handelt, kann eine direkte Ausnutzung nicht durch Antivirus-Software verhindert werden. Diese schützt ggf. lediglich vor Malware oder Viren, die dazu entwickelt wurden, die Schwachstelle auszunutzen. Entwickler der drei Betriebssysteme Windows, Linux und macOS haben Anfang 2018 bereits Patches veröffentlicht, die die Ausnutzung der Schwachstelle verhindern sollen. Dementsprechend ist auf den von der Schwachstelle betroffenen Systemen die Installation entsprechender Patches die einzige verfügbare Schutzmaßnahme.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.2.2 Spectre – Schwachstellen in CPUs

Übersicht

Im Januar 2018 veröffentlichten Forscher von verschiedenen Universitäten in Australien, Österreich und den Vereinigten Staaten von Amerika sowie von Googles Project Zero, mit dem Paper „Spectre Attacks: Exploiting Speculative Execution“ /KOC18r01/,

Informationen zur Sicherheitslücke Spectre, die eng mit der Schwachstelle Meltdown (siehe Abschnitt A.2.1) verknüpft ist und auf den gleichen Prinzipien moderner Prozessoren basiert. Spectre nutzt dabei ebenfalls Out-of-Order-Execution, Speculative Execution und Branch-Prediction aus, um unberechtigt Informationen beispielsweise aus dem Speicher anderer ablaufender Prozesse bzw. Programme auszulesen.

Beschreibung

Im Gegensatz zu Meltdown, bei dem potenzielle Angreifer Informationen beliebig aus dem gesamten Speicher des Systems extrahieren können, ist unter Ausnutzung der Spectre-Schwachstelle kein Zugriff auf den gesamten Speicher möglich, sondern nur auf den Speicher anderer ausgeführter Programme. Technische Hintergründe der drei genannten Prozesse Out-of-Order-Execution, Speculative Execution und Branch-Prediction sind in Abschnitt A.2.1 beschrieben.

Die Schwachstelle betrifft den überwiegenden Teil heutiger Modelle der Prozessoren, unabhängig vom Betriebssystem und neben den bereits von Meltdown betroffenen Herstellern (insbesondere der Marktführers Intel sowie ARM und IBM) ist auch der Hersteller AMD betroffen. Somit ist auch von Spectre eine Vielzahl an Privat- oder Firmengeräten, die CPUs besitzen, betroffen und potenziell ist die große Mehrzahl der Computer weltweit für die Schwachstelle anfällig. Vor der Veröffentlichung der ursprünglichen zwei Spectre-Schwachstellen mit den CVE-Nummern CVE-2017-5715 und CVE-2017-5753, die sich jeweils in Details unterscheiden, wurden betroffene Hard- und Software-Hersteller bereits im Jahr 2017 von den Forschern informiert.

Um diese Schwachstelle auszunutzen, werden wie bei Meltdown keine weiteren Hilfsmittel benötigt. Angreifer brauchen lediglich eine Zugriffsmöglichkeit auf das System, die es erlaubt, Code auszuführen. Da es sich um eine Hardware-Schwachstelle handelt, kann eine direkte Ausnutzung nicht durch Antivirus-Software verhindert werden. Diese schützt ggf. lediglich vor Malware oder Viren, die dazu entwickelt wurden, die Schwachstelle auszunutzen. Auch für Spectre haben Entwickler der drei Betriebssysteme Windows, Linux und macOS Anfang 2018 bereits Patches veröffentlicht, die die Ausnutzung der Schwachstelle verhindern sollten. Die Installation der entsprechenden Patches ist auf den von der Schwachstelle betroffenen Systemen die einzige verfügbare Schutzmaßnahme.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.3 2019

A.3.1 SPPA-T3000 – Schwachstellen in ICS

Übersicht

Im Rahmen eines Vortrages stellte das Unternehmen Kaspersky Lab Security Services im Dezember 2019 zahlreiche Schwachstellen des Leittechniksystems SPPA-T3000 des Unternehmens Siemens vor /KAS19f01/. Bei SPPA-T3000 handelt es sich um ein weltweit eingesetztes Distributed Control System (DCS), welches insbesondere in konventionellen Kraftwerken und Turbinensteuerungssystemen eingesetzt wird, wobei SPPA-T3000 keine Sicherheitsleittechnik direkt integriert unterstützt. Die Schwachstellen sind als äußerst schwerwiegend eingeschätzt worden und ermöglichen Angreifern umfassende Kontrollübernahme über das betroffene Leittechniksystem.

Beschreibung

Bei dem System des Herstellers Siemens mit der Typenbezeichnung SPPA-T3000 handelt es sich um ein betriebliches Leittechniksystem bzw. Prozessleitsystem (Distributed Control System, DCS), welches häufig zur Turbinensteuerung in Kraftwerken aber auch für verschiedene andere Aufgaben zur Steuerung verfahrenstechnischer Prozesse eingesetzt wird /SIE18w01/. SPPA-T3000 wird in einer Vielzahl von konventionellen Kraftwerken eingesetzt, z. B. im Kraftwerk Eemshaven in den Niederlanden sowie fossilen Kraftwerken in Deutschland, beispielsweise Westfalen D&E, Neurath F&G, GKM 9, Schwarze Pumpe, Altbach, Heilbronn, Lippendorf, Niederaußem K, RDK 8. /SIE15f01/

Die Mitarbeiter von Kaspersky legten im Rahmen ihres Vortrages und des von ihnen veröffentlichten Whitepapers dar, wie unautorisierte Personen sowohl remote als auch direkt Zugriff auf die zentralen Komponenten des SPPA-T3000 Systems erlangen und weitere Schwachstellen ausnutzen können, darunter die Eskalation von Rechten /KAS19f01/.

Dabei gingen sie auf die Schwachstellen der eingesetzten Softwarelösungen ein und zeigten auf, wie sich die verschiedenen Schwachstellen auszunutzen lassen um Zugriff mit privilegierten Rechten, d. h. Administratorrechten, auf alle entscheidenden Systemkomponenten zu erhalten.

Eigenen Angaben zufolge /KAS19f01/ setzte Kaspersky den Hersteller Siemens bereits Ende 2018 über ihre Untersuchungsergebnisse einschließlich der mehr als 50 gefundenen Schwachstellen in Kenntnis, um dem Hersteller des SPPA-T3000 Systems so aus-reichend Zeit für die Erstellung von Patches und die Information der betroffenen Anlagen zu geben. Siemens arbeitete daraufhin gemeinsam mit Kaspersky an Patches, Software-Updates und mitigativen Lösungen. Ende 2019 veröffentlichte Siemens einen CERT-Report zu den bekannt gewordenen Schwachstellen in SPPA-T3000, verfügbaren Updates und Mitigationsmöglichkeiten. /SIE19r01/ Dieser CERT Report wurde im März 2020 nach der Veröffentlichung eines weiteren Updates überarbeitet.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS20r07/

A.3.2 S7 und PCS7 – Schwachstellen in ICS

Übersicht

In den vergangenen Monaten bzw. Jahren wurden zahlreiche Anfälligkeiten in den SIMATIC-Produkten S7 und PCS 7 identifiziert und öffentlich gemacht. Hervorzuheben sind hierbei zwei umfangreich dokumentierte Schwachstellen, die einerseits von Forschern der Ruhr Universität Bochum und andererseits von Forschern des Technion in Haifa, Israel, im letzten Jahr veröffentlicht und auf IT-Sicherheitskonferenzen /ABB19w01, MAL19w01/ vorgestellt wurden. Die Forscher der Technion veröffentlichten außerdem ein Whitepaper /BIH19r01/, in dem verschiedene Angriffsmöglichkeiten auf die neueste Gerätegeneration S7-1500 detailliert beschrieben werden.

Der Hersteller der SIMATIC-Systeme S7 und PCS 7, Siemens, veröffentlichte u. a. bezüglich der zwei öffentlich gemachten Schwachstellen jeweils einen Sicherheitshinweis /SIE19i05/, /SIE19i06/ und außerdem eine Vielzahl weiterer Sicherheitshinweise für S7- und PCS 7-Systeme.

Beschreibung

Forscher der Ruhr Universität Bochum fanden eine hardwarebasierte Schwachstelle im Bootloader der Siemens SPS S7-1200, die ihnen Zugriff auf das System und das unerkannte Platzieren eigener Software ermöglichte. Der Bootloader prüft unter anderem beim Systemstart über Checksummen die Integrität der SPS Firmware. Diese Integritätsprüfung kann durch die Nutzung der Schwachstelle umgangen werden, sodass potenzielle Angreifer beliebigen Code auf die SPS übertragen können, ohne dass dies durch die Integritätsprüfung erkannt wird. Dies geschieht über die Universal Asynchronous Receiver Transmitter (UART) Schnittstelle der S7-1200, was einen physischen Zugang zum System voraussetzt.

In einem Whitepaper /BIH19r01/ beschreiben Forscher der Technischen Universität Israels (Technion), wie sie mit Hilfe einer selbst entwickelten, maliziösen Engineering Station auf die Siemens SPS 7-1500 zugreifen konnten. Neben der Möglichkeit des remote--Zugriffs und der Steuerung der SPS ist es Ihnen gelungen, eigenen Code auf dem Gerät zu platzieren. Außerdem könnten Angreifer mit den im Paper dargestellten Methoden die SPS so manipulieren, dass der auf der SPS ausgeführte Code sich vom angezeigte Code unterscheidet. In diesem Fall könnte vom Angreifer potenziell platzierter Schadcode unerkannt auf dem System ausgeführt werden, ohne dass dies beim Anzeigen des auf der SPS gespeicherten Codes auffallen würde.

Beide Forschungsgruppen informierten Siemens vor der Veröffentlichung der Schwach-stellen über ihre Erkenntnisse, um dem Hersteller der S7-SPS-Systeme ausreichend Zeit für die Erstellung von Updates und die Information der betroffenen Anlagen zu geben. Am 12.11.2019 veröffentlichte Siemens einen Sicherheitshinweis bezüglich der Schwachstelle des unautorisierten Zugriffs über den Bootloader. /SIE19i05/ Der Sicherheitshinweis bezüglich der Schwachstelle, die es ermöglichte, dass der angezeigte Code und der tatsächlich ausgeführte Code nicht identisch sind, wurde am 13.08.2019 veröffentlicht. Für beide Schwachstellen bietet Siemens Softwareupdates zu deren Behebung an. /SIE19i06/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r09/.

A.4 2020

A.4.1 Profinet – Schwachstellen in einem Kommunikationsstandard

Übersicht

Im Februar 2020 veröffentlichte die Firma Siemens IT-Sicherheitshinweise zum Kommunikationsstandard Profinet, welcher weltweit für die Kommunikation leittechnischer Systeme eingesetzt wird /SIE20r02/. Bei Profinet handelt es sich um einen für die in der Leittechnik notwendige Echtzeitkommunikation entwickelten Kommunikationsstandard, welcher auf der Ethernet-Technik basiert und weltweit von mehreren Millionen leittechnischer Geräte verschiedener Hersteller unterstützt wird. Die IT-Sicherheitshinweise, die in Teilen als schwerwiegend eingeschätzt werden, betreffen hierbei neben einer hohen Anzahl an leittechnischen IT-Systemen, welche Profinet unterstützen, auch leittechnische Systeme, welche grundsätzlich auf Ethernet basierende Kommunikation unterstützen. Profinet, ebenfalls wie sein Vorgänger Profibus, unterstützen die Kommunikation von Sicherheitsleittechnik bis zu einem Sicherheitsintegritätslevel SIL 3.

Beschreibung

Im Februar 2020 veröffentlichte die Firma Siemens IT-Sicherheitshinweise zu einer großen Anzahl von Leittechniksystemen, welche den Kommunikationsstandard Profinet unterstützen und von Schwachstellen des Kommunikationsstandards Profinet betroffen sind. Im Zuge dessen veröffentlichte Siemens weitere Sicherheitshinweise und aktualisierte ältere Sicherheitshinweise zu Schwachstellen in der Profinet-Kommunikation und genereller Ethernetkommunikation von Siemens Leittechniksystemen.

Die von Siemens veröffentlichten Schwachstellen sind in ihren Auswirkungen sehr ähnlich, lassen sich jedoch unabhängig voneinander ausführen: Bei Netzwerkzugriff auf die Kommunikation mittels Profinet bzw. auf die generelle Ethernetkommunikation können Angreifer ohne Authentifizierung spezielle Nachrichten an die mit Profinet bzw. Ethernet kommunizierenden Leittechniksysteme versenden, wodurch es bei den betroffenen Leittechniksystemen zu einem Denial-of-Service Zustand kommt. Infolgedessen wird die Verfügbarkeit der betroffenen Leittechniksysteme beeinträchtigt, die Systeme schalten sich ab bzw. reagieren nicht mehr auf legitime datentechnische Anfragen und senden keine eigenen Signale mehr aus, sodass die leittechnischen Funktionen der Systeme nicht mehr ausgeführt werden. Hierbei ist zu beachten, dass von potenziellen Angreifern nicht alle der genannten Schwachstellen ausgenutzt werden müssen, sondern die Ausnutzung jeweils einer der beschriebenen Schwachstellen für die Hervorrufung eines Denial-of-Service-Zustandes ausreicht. /SIE20r02 bis SIE20r12/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r06/

A.4.2 ABB 800xA – Schwachstellen in ICS

Übersicht

Im März 2020 veröffentlichte das Unternehmen ABB, ein international tätiger Hersteller für Leittechnik- und Sicherheitsleittechniklösungen, mehrere IT-Sicherheitshinweise zu teilweise schwerwiegenden bekanntgewordenen Schwachstellen im Leittechniksystem ABB 800xA /ABB20r01, ABB20r02, ABB20r03/. Mit ABB 800xA ist ein weltweit eingesetztes DCS mit Sicherheitsleittechnikunterstützung von Schwachstellen betroffen, die potenziell Angreifern die Möglichkeit bieten, die Integrität und Verfügbarkeit des gesamten Systems zu beeinflussen.

Beschreibung

Bei dem genannten System des Herstellers ABB mit der Typenbezeichnung 800xA handelt es sich um ein betriebliches Leittechniksystem bzw. Prozessleitsystem (Distributed Control System, DCS), welches für eine Vielzahl verschiedener Großprozesse, unter anderem Kraftwerksprozesse, eingesetzt wird /ABB14r01/. Dabei unterscheidet sich das 800xA-System von den DCS-Systemen anderer Hersteller grundlegend dadurch, dass neben betrieblichen Leittechnikfunktionen nach Wunsch auch umfassende Sicherheitsleittechnikfunktionen integriert werden können /ABB14r01/. Das 800xA-System von ABB wird in einer Vielzahl von Industrie- und Kraftwerksanlagen in Deutschland und Europa verwendet, z. B. im Müllverbrennungskraftwerk Höchst, im Stahlwerk Dillinger Hüttenwerk, im DOMO Chemiewerk in Leuna, in einer Aluminiumhütte von Alunorf sowie einer Papierfabrik in Fulda. /ABB20w01/

Mit den drei initial von ABB veröffentlichten IT-Sicherheitshinweisen werden insgesamt vier bekannt gewordene Schwachstellen des 800xA-Systems beschrieben. Mit Hilfe der vorgestellten Schwachstellen ist es nach Angaben von ABB möglich, dass Angreifer einerseits innerhalb des 800xA-Systems auf bestimmten Teilsystemen ihre Rechte eskalieren können, andererseits besteht durch eine Schwachstelle die Möglichkeit, dass Angreifer unautorisiert beliebigen Code ausführen können, bei bestehendem Netzwerk- und Internetzugriff auch aus der Ferne. /ABB20r01/, /ABB20r02/, /ABB20r03/

Mit später veröffentlichten Sicherheitshinweisen wurden mehrere weitere Schwachstellen bekannt, welche ABB 800xA betreffen. Unter anderem ist das zentrale Lizenzmanagementsystem der ABB betroffen, welches in den meisten ABB Leittechniklösungen, darunter 800xA, verwendet wird sowie die Intersystemkommunikation von 800xA. /ABB20r08/, /ABB20r09/, /ABB20r10/

Die IT-Sicherheitshinweise von ABB zum 800xA-System wurden nach der Veröffentlichung mehrfach aktualisiert und ergänzt. ABB veröffentlichte seit dem Bekanntwerden der Schwachstellen Updates für die Versionen 5.1, 6.0 und 6.1 von 800xA, welche verschiedene Schwachstellen beheben. Je nach Versionsstand sind jedoch Stand Oktober 2020 noch nicht alle bekannt gewordenen Schwachstellen behoben worden. /ABB20r04/, /ABB20r05/, /ABB20r06/, /ABB20r08/, /ABB20r09/, /ABB20r10/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r07/

A.4.3 Zerologon – Schwachstelle im Windows Netlogon Remote Protocol

Übersicht

Das Bundesamt für Sicherheit in der Informationstechnik hat eine BSI-Cyber-Sicherheitswarnung in Bezug auf eine kritische Schwachstelle im Windows Netlogon Remote Protocol mit dem Namen Zerologon veröffentlicht /BSI20i02/. Microsoft veröffentlichte bereits im August 2020 ein Update in Bezug auf diese Schwachstelle /MIC20w01/, die von der auf digitale Sicherheit spezialisierten, niederländischen Firma Secura entdeckt und im September 2020 unter anderem in Form eines Whitepapers /TER20r01/ der Öffentlichkeit bekannt gemacht wurde. Durch Microsoft wurden bereits in diesem Zusammenhang Vorfälle unter Ausnutzung dieser Schwachstelle beobachtet /MIC20w02/. Mittlerweile wurde außerdem Code zur Ausnutzung der Schwachstelle veröffentlicht /GIT20w01/ und diverse einschlägige Werkzeuge im Bereich der Cyber-Kriminalität wie beispielsweise Mimikatz /GIT20w02/ wurden um Funktionalitäten zur Ausnutzung der Schwachstelle erweitert. Es ist daher davon auszugehen, dass Angriffe auf ungepatchte Systeme durchgeführt werden.

Beschreibung

Von der Schwachstelle betroffen ist das sogenannte Netlogon-Protokoll, ein RPC-Interface (Remote Procedure Call) für Windows Domänencontroller, das u. a. beim Zugriff und bei der Authentifizierung von Nutzern auf entsprechenden Servern verwendet wird. Der Domänencontroller ist dabei ein Server zur Authentifizierung von Rechnern und Nutzern in einem Netzwerk. Unter Ausnutzung der Schwachstelle erhält ein potenzieller Angreifer Kontrolle über den Verzeichnisdienst Active Directory, der in Windows Server Systemen implementiert ist.

Laut dem Whitepaper von Secura ist es einem Angreifer bei der Authentifizierung gegenüber dem Domänencontroller weiterhin möglich, die Identität einer beliebigen Maschine in einem Netzwerk vorzutäuschen. Dies ermöglicht weiteres Vorgehen, wie einen Denial-of-Service Angriff, bei dem die Verfügbarkeit des Systems beeinträchtigt wird oder letztendlich auch eine vollständige Übernahme des Domänencontrollers, indem das Passwort geändert wird und der Angreifer sich selbst Administratorrechte verleihen kann. Die Schwachstelle ermöglicht somit eine Rechteausweitung.

Zur Ausnutzung der Schwachstelle ist eine Verbindung zum Netzwerk erforderlich, die entweder lokal (z. B. über einen Innentäter) oder über das Internet (z. B. durch global agierende Angreifer) erfolgen kann. Das BSI hebt in der Sicherheitswarnung die Kritikalität der Schwachstelle hervor, da es eine große Anzahl über das Internet erreichbarer Domänencontroller gibt, die möglicherweise auch nach Veröffentlichung des Updates nicht aktualisiert wurden und somit ungeschützt sind. Außerdem werden die weitreichenden Auswirkungen im Falle einer Kompromittierung herausgestellt. Dass bereits Code-Beispiele zur Ausnutzung der Schwachstelle veröffentlicht wurden, wodurch die Anwendung auch durch nicht spezialisierte Angreifer ermöglicht wird, dass der Code vergleichsweise einfach anzuwenden ist und dass entsprechende Teile des Codes bereits in einschlägige Werkzeuge im Bereich der Cyber-Kriminalität integriert wurden, unterstreicht die Kritikalität. Microsoft beobachtete in diesem Zusammenhang bereits eine Zunahme an Aktivitäten der u. a. bereits in Deutschland agierenden Gruppierung TA505. Außerdem wurden vom Federal Bureau of Investigation (FBI) und der Cybersecurity and Infrastructure Security Agency (CISA) der Vereinigten Staaten von Amerika mehrere Warnmeldungen in Bezug auf die Schwachstelle veröffentlicht. Demnach wurden Angriffe von Advanced Persistent Threat (APT)-Gruppierungen unter Ausnutzung von Vulnerability-Chaining-Techniken, bei dem mehrere Schwachstellen im Verlauf eines einzigen Angriffs ausgenutzt werden, um ein Netzwerk oder ein System zu kompromittieren, beobachtet, wobei auch die hier genannte Schwachstelle Zerologon verwendet wurde. /CIS20r02/ Laut einer weiteren CISA-Warnmeldung wird die Schwachstelle auch von der APT-Gruppierung Dragonfly/Energetic Bear benutzt, die in der Vergangenheit u. a. bereits Organisationen, Firmen und Anlagen im Energiesektor angegriffen hat. /CIS20r01/ Windows Server werden branchenübergreifend in einer Vielzahl von Firmen, Organisationen und Institutionen eingesetzt. Dem BSI liegen Informationen über die Betroffenheit von sich im Einsatz befindlichen, nicht gepatchten Altsystemen bei Betreibern kritischer Infrastrukturen vor.

Auch kerntechnische Anlagen und Einrichtungen, national und international, verwenden Windows Server Systeme, die ungepatched von der Schwachstelle betroffen sind.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r10/.

A.4.4 Amnesia:33 – Schwachstellen in Netzwerkstacks

Übersicht

Anfang Dezember 2020 veröffentlichte das BSI zwei Cyber-Sicherheitswarnungen /BSI20r03/ zu Schwachstellen in Open Source Netzwerkstacks. Zuvor wurde bereits ein ICS Advisory zu dieser Thematik veröffentlicht /CIS20r03/. Die insgesamt 33 bekannt gewordenen Schwachstellen werden mit dem Namen Amnesia:33 zusammengefasst. Entdeckt wurden die Schwachstellen vom IT-Sicherheitsunternehmen Forescout bei der Untersuchung von Open Source TCP/IP-Stacks.

Beschreibung

Im Rahmen der Untersuchungen fand Forescout in vier von sieben untersuchten Stacks Schwachstellen, von denen die Forscher einige als kritisch einstuften. Die betroffenen Netzwerkstacks werden in einer Vielzahl von IT-, IoT- und OT-Umgebungen eingesetzt und betreffen daher eine ganze Reihe Hersteller, darunter auch den Leittechnikhersteller Siemens. Die Schwachstellen sind unabhängig von der herstellerspezifischen Anwendungssoftware ausnutzbar. Heise /HEI20w01/ nennt unter Berufung auf Forescout folgende Beispiele für potenziell betroffene Gerätetypen:

- IoT (Internet of Things): Kameras, Umgebungssensoren (z. B. Temperatur, Luftfeuchtigkeit), intelligente Beleuchtung, intelligente Stecker, Strichcodelesegeräte, Spezialdrucker, Audiosysteme für den Einzelhandel, Geräte in Krankenhäusern, Sensoren

- OT (Operational Technology): Gebäudeautomationssysteme (GA) wie physische Zugangskontrolle, Feuer- und Rauchmelder, Stromzähler, HVAC (Heating, Ventilation and Air Conditioning (dt. Heizung, Lüftung, Klimatechnik)) und industrielle Steuerungssysteme (ICS) einschließlich beispielsweise PLCs, RTUs, Protokoll-Gateways und Seriell-Ethernet-Gateways, IP Kameras
- IT: Drucker, Switches und WLAN-Access-Points, Server

Forescout veröffentlichte am 7.12.2020 einen detaillierten Forschungsbericht zu Amne-sia:33 /FOR20r01/ und gab am 9.12.2020 weitere Details auf der IT-Sicherheitskonferenz Blackhack Europe 2020 bekannt /FOR20f01/. Forescout schätzt die Zahl der von Amnesia:33 betroffenen Hersteller auf über 150 und die Zahl der letztlich betroffenen Geräte auf mehrere Millionen. Bei geeigneter Ausnutzung der bekannt gewordenen Schwachstellen können potenzielle Angreifer beispielsweise Denial-of-Service-Angriffe durchführen oder sensible Informationen auslesen, bei den kritischen Schwachstellen sogar per Fernzugriff und ohne Authentifizierung beliebigen Schadcode auf betroffenen Geräten ausführen /BSI20r03/. Die CISA nennt als konkrete Handlungsmöglichkeiten die Korrumpierung von Speicher, das Auslösen von Endlosschleifen, unautorisierten Zugriff auf Daten und Durchführung von DNS-Cache-Vergiftungsangriffen[6] /CIS20r03/.

Das BSI berichtet, die Ausnutzung der Schwachstellen basiere in allen Fällen auf manipulierten Netzwerkpaketen, die zwischen betroffenem Gerät und Angreifer ausgetauscht werden /BSI20r03/. Die CISA veröffentlichte bereits kurz zuvor ein speziell auf Siemens-Produkte ausgerichtetes ICS Advisory /CIS20r04/ zu den entdeckten Amne-sia:33 Schwachstellen. Auch Siemens selbst veröffentlichte ein entsprechendes Security Advisory /SIE20r13/. Eine der 33 bekannt gewordenen Schwachstellen (CVE-2020-13988) betrifft die folgenden Siemens Produkte:

- SENTRON PAC3200: Version 2.4.5 und frühere Versionen
- SENTRON PAC4200: Version 2.0.1 und frühere Versionen
- SIRIUS 3RW5 Kommunikationsmodul Modbus TCP: Alle Versionen

[6] Mit DNS Cache Poisoning ändert der Angreifer im Prinzip die Regeln, nach denen der Netzwerkverkehr erfolgt.

Bei erfolgreicher Ausnutzung dieser Schwachstelle würde dem Angreifer die Durchführung eines Denial-of-Service-Angriffes auf die genannten Geräte ermöglichen. Der Schwachstelle wurde ein CVSS v3 Base Score von 6.5 zugeordnet. Bei der für Sie-mens-Produkte relevanten Schwachstelle handelt es sich jedoch um keine der vier als kritisch eingestuften Amnesia:33-Schwachstellen. Siemens hat für die SENTRON PAC Geräte sowie für das SIRIUS 3RW5 Kommunikationsmodul im ersten Quartal 2021 bereits Updates veröffentlicht, welche die Schwachstellen beheben.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r08/

A.4.5 Ramsay – Angriffswerkzeug für Cyberspionage

Übersicht

Im Jahr 2020 entdeckten Forscher von ESET ein Toolkit für Cyberspionage, das speziell auf die Ausspähung von Air-Gap Netzwerken und die Exfiltration von Informationen über Air Gaps hinweg zugeschnitten ist. Die Analyse der aufgefundenen Instanz der Schad-software lieferte Hinweise darauf, dass sich das Angriffswerkzeug derzeit noch im Entwicklungsprozess befindet /ESE20w01/.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.4.6 Schwachstelle in Hirschmann Switchen

Übersicht

Am 14. Februar 2020 veröffentlichte der Hersteller von IT-Technik Belden mit dem Bel-den Security Bulletin BSECV-2020-01 /BEL20r01/ einen Bericht zur kritischen Schwachstelle CVE-2020-6994 in Netzwerkswitchen der Marke Hirschmann. Die gefundene kritische Schwachstelle betraf mehrere Produktreihen sogenannter Managed-Switche und wurde mit einem CVSS Score von 9,8 von 10 Punkten als kritisch bewertet. Im Juli 2022 wurde darüber hinaus bekannt, die gleiche Schwachstelle auch industrielle Firewalls der Produktreihen AFF66X des Herstellers Hitachi Energy von der Schwachstelle betroffen sind. /BEL20r01/, /BSI22r13/

Beschreibung

Netzwerkswitche sind zentrale Baugruppen zur Leitung- und Verteilung des Datenverkehrs in lokalen Netzwerken (LAN) und dienen hierbei der Verteilung und Weiterleitung des eingehenden und ausgehenden Datenverkehrs angebundener IT-Systeme. Switches werden mittlerweile häufig als sogenannte Managed Switches mit ihrer eigenen integrierten Software in Form eines Betriebssystems ausgeliefert, welches zusätzliche Funktionen im Bereich des Netzwerkmanagement und des Sicherheitsmanagement der Switche bietet. Hirschmann Switche der Produktreihen RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS und RED nutzen als Betriebssystem das HiOS, Switche der Baureihen Eagle20/30 das Betriebssystem HiSecOS. Die Schwachstelle CVE-2020-6994 betrifft die HiOS Versionen 07.0.02 oder älter sowie die HiSecOS Versionen 03.2.00 oder älter. Über eine http- bzw. HTTPS-Anfrage können Angreifer unter Ausnutzung der Schwachstelle einen vollständigen Systemzugriff auf die betroffenen Switche erreichen und entsprechend die Verfügbarkeit, Vertraulichkeit und Integrität der Systeme beeinträchtigen. Die Schwachstelle wurde am 14.02.2020 für Hirschmann Switche bekannt, am 26.02.2020 veröffentlichte Belden mit der HiOS Version 07.0.03 sowie der HiSecOS Version 03.3.00 Updates für alle betroffenen unterstützten Produkte, welche die Schwachstelle behebt. /BEL20r01/, /BSI22r13/

Im Juli 2022 wurde bekannt, dass zwei industrielle Firewallprodukte der Produktreihen AFF66X des Unternehmens Hitachi Energy ebenfalls von der Schwachstelle CVE-2020-6994 betroffen sind. Für diese Systeme bestehen bisher keine Updates zur Verfügung.

Für diesen Fall wie auch für die Fälle, dass Hirschmann Switche nicht auf den neusten Stand gebracht werden können, wird die Deaktivierung der HTTP- und HTTPS-Zugriffsfunktionen auf die Systeme empfohlen. Es liegen keine Informationen vor, dass die Schwachstelle CVE-2020-6994 bisher von Angreifenden ausgenutzt wurde. /BSI22r13/, /HIT22r01/

Switche und Firewalls sind zentrale Komponenten in Netzwerken und daher von besonderer Bedeutung bei der Sicherung entsprechender Netzwerke vor Einwirkungen von außen.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer kurzfristigen Ersteinschätzung ausgewertet.

A.5 2021

A.5.1 Microsoft Exchange – Schwachstelle des Microsoft Exchange Servers

Übersicht

Im ersten Quartal 2021 wurde eine schwerwiegende Sicherheitslücke bekannt, welche dazu genutzt werden kann, dass Microsoft Exchange Server, welche unter anderem für das weltweit verbreitete E-Mail und Organisationsprogramm Outlook genutzt werden, von Angreifern vollständig kontrolliert werden können. Zum Zeitpunkt des Bekanntwerdens wurde die Schwachstelle aktiv von Angreifern ausgenutzt, wodurch potenziell eine hohe Anzahl von Unternehmen, Behörden und Betreibern kritischer Infrastruktur betroffen sein können.

Beschreibung

Schwachstellen in Microsoft Exchange ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware, sowie die Übernahme des gesamten Systems aus der Ferne durch Angreifer /BSI21i05/. Nach den Angaben von Microsoft wurden über die Schwachstellen bereits Angriffe gegen amerikanische Einrichtungen durchgeführt. Zu den Angriffszielen gehören Forschungseinrichtungen mit dem Schwerpunkt Pandemie, Hochschulen, Anwaltsfirmen, der Rüstungssektor, Think Tanks und nichtstaatliche Organisationen. Nach Volexity wurden die Schwachstellen bereits im November 2020 für gezielte Angriffe genutzt und laut der Server-Suchmaschine Shodan waren von den Schwachstellen im März 2021 in Deutschland etwa 57.000 Server potenziell betroffen /BSI21i04/. Die Angreifer verschafften sich Zugang über die E-Mail-Accounts und installierten danach weitere Schadsoftware zur Herstellung einer persistenten Verbindung. /BSI21i03/

Vier Schwachstellen sind seit dem 02.03.2021 unter dem Namen ProxyLogon bekannt. Sie ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware. Davon ausgenommen ist Exchange-Online. Für die Durchführung von Angriffen über diese Schwachstellen muss die Möglichkeit bestehen eine nichtvertrauenswürdige Verbindung zu Port 443 des Exchange-Servers aufzubauen. Server ohne nichtvertrauenswürdige Verbindungen oder mit VPN-Verbindung sind zwar gegen einen initialen Angriff geschützt, haben die Angreifer aber bereits Zugriff auf den Server oder führt ein Administrator eine schadhafte Datei aus, so bieten auch diese Maßnahmen keinen Schutz mehr. Angriffe, bei denen die vier Schwachstellen ausgenutzt wurden, wurden vermutlich von der APT-Gruppierung HAFNIUM durchgeführt, welche im Auftrag der chinesischen Regierung arbeitet. Nachstehend werden die Schwachstellen aufgelistet und ihre Auswirkungen beschrieben /BSI21i03/:

- **CVE-2021-26855**: Diese Schwachstelle ermöglicht einem Angreifer das Senden ei-er HTTP-Anfrage sowie die Authentifizierung am Exchange-Server. Am 11. März 2021 berichtete Bleeping Computer über eine Ausbreitung der Ransomware DearCry unter Ausnutzung dieser Schwachstelle /BSI21i04/. CVSS-Score: CVSS:3.0 9.1 / 8.4 /MIC21w09/.
- **CVE-2021-26857**: Ermöglicht die Ausführung beliebigen Programmcodes als SYSTEM auf dem Exchange-Server. Dafür werden vom Angreifer Administratorrechte benötigt oder er muss eine weitere, geeignete Schwachstelle ausnutzen. CVSS-Score: CVSS:3.0 7.8 / 7.2 /MIC21w10/.

- **CVE-2021-26858 und CVE-2021-27065**: Über diese Schwachstellen können nach erfolgreicher Authentifizierung Dateien auf den Exchange-Server geschrieben wer-den. Die Authentifizierung kann über die oben beschriebene Schwachstelle CVE-2021-26855 oder gestohlene Administratorrechte erfolgen. Beide Schwachstellen besitzen den CVSS-Score CVSS:3.0 7.8 / 7.2 /MIC21w11, MIC21w12/.

Drei weitere Schwachstellen werden unter dem Namen ProxyShell zusammengefasst und ermöglichen die Übernahme des gesamten Systems aus der Ferne. Nach Cisco Ta-los wurden diese bei Angriffen im Oktober 2021 mit der Ransomware Babuk eingesetzt, für die gemäß dem IT-Sicherheitsunternehmen Huntress die APT-Gruppierung Tortilla verantwortlich sein soll /BSI21i05/. Nachstehend werden die Schwachstellen aufgelistet und ihre Auswirkungen beschrieben /MAL21w02/:

- **CVE-2021-31207**: Diese Schwachstelle ermöglicht es einem Angreifer per Fernzugriff den Authentifizierungsprozess zu umgehen. CVSS-Score: CVSS:3.0 6.6 / 5.8 /MIC21w13/.
- **CVE-2021-34523**: Ermöglicht einem Angreifer die Erhöhung von Zugriffsrechten. CVSS-Score: CVSS:3.0 9.0 / 7.8 /MIC21w14/.
- **CVE-2021-34473**: Die Schwachstelle erlaubt einem Angreifer die Ausführung beliebigen Programmcodes im SYSTEM-Kontext. Der Angreifer benötigt dazu eine Authentifizierung. CVSS-Score: CVSS:3.0 9.1 / 7.9 /MIC21w15/.

Darüber hinaus ist noch die folgende Schwachstelle seit dem 13.07.2021 bekannt /BAR21w01/:

- **CVE-2021-31206**: Ein Angreifer kann über einen von ihm kompromittierten Systemnutzer beliebigen Programmcode ausführen. Die Ausnutzung dieser Schwachstelle setzt die Kompromittierung eines authentifizierten Benutzers in einer bestimmten Vermittlungsfunktion voraus. CVSS-Score: CVSS:3.0 7.6 / 7.1 /MIC21w16/.

Darüber hinaus gibt es eine Vielzahl weiterer Schwachstellen. Zurzeit sind 31 Schwachstellen bekannt /CVE21w01/. Microsoft hat entsprechende Updates für den Exchange-Server veröffentlicht. Die amerikanische Cybersecurity and Infrastructure Agency hat entsprechende Angriffsindikatoren angegeben. Die Indikatoren werden auch von Microsoft, Volexity und Rapid 7 bereitgestellt. /BSI21i03/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.5.2 NAME:WRECK – Schwachstellen in Netzwerkstacks

Übersicht

Das IT-Unternehmen Forescout hat nach der Aufdeckung der Amnesia:33 Schwachstellen die Erforschung und Aufdeckung von Schwachstellen von TCP/IP Stacks weiter fortgesetzt und 2021 unter dem Titel NAME:WRECK insgesamt 9 weitere Schwachstellen in vier TCP/IP Stacks veröffentlicht. Betroffen sind die TCP/IP Stacks FreeBSD, NetX, IPnet sowie Nucleus NET, wobei letzterer vom Hersteller Siemens entwickelt wurde.

Beschreibung

Forescout geht von insgesamt mehr als 100 Millionen betroffenen Systemen aus, wobei eine große Anzahl betroffener Siemensprodukte in der Leittechnik der kritischen Infrastruktur anzunehmen ist. Die Schwachstellen selbst betreffen insbesondere das Domain Name System (DNS) der TCP/IP Kommunikation, welches als Adresssystem beschrieben werden kann. Die Schwachstellen ermöglichen Angreifern die Auslösung von DoS-Bedingungen und auch die Ausführung beliebigen Codes und werden damit als schwerwiegend eingeschätzt. /FOR21r01/

Forescout veröffentlichte ein quelloffenes Script, mit welchem jeder Anwender innerhalb seines Netzwerks herausfinden kann, ob Systeme mit betroffenen TCP/IP Stacks genutzt werden. Die Anbieter der TCP/IP Stacks, insbesondere Siemens, haben im Vorfeld der Veröffentlichung mit Forescout zusammengearbeitet, sodass für alle Nucleus NET Versionen Sicherheitsupdates bereitstehen. Ob und welche Siemensprodukte betroffen sind und bereits produktspezifische Sicherheitsupdates verfügbar sind, ist zum Zeitpunkt der Berichtserstellung noch nicht bekannt.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen.

Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r08/

A.5.3 Schwachstellen in Bachmann Controllern

Übersicht

Zwei Schwachstellen betreffen die M1-Hardware-Controller von Bachmann. Diese wer-den in den Bereichen Energie und Automatisierung eingesetzt. Informationen über eine Ausnutzung der Schwachstellen liegen derzeit nicht vor.

Beschreibung

Die gefundenen Schwachstellen betreffen die M1-Hardware-Controller von Bachmann, die bezüglich des Betriebssystems und der Middleware alle M-Base-Versionen seit MSYS V1.06.14 verwenden. Das M1-Automatisierungssystem ist das Herzstück aller Systemlösungen von Bachmann, die in den Bereichen erneuerbare Energien wie z. B. Windkraft, Energieverteilung sowie zur Automatisierung im Maschinenbau und Anlagen-bau eingesetzt werden. Nachfolgend werden die gefundenen Schwachstellen angegeben und beschrieben: /BSI21i09, BAC22w01/

- **CVE-2020-16321**: Die Speicherung von Passwörtern erfolgt über ein unsicheres, kryptographisches Verfahren. Zum Einsatz kommt der Verschlüsselungsalgorithmus MD5. Dieser wird nicht mehr als sicher betrachtet, da moderne leistungsfähige Rechner eine Rückrechnung auf das Originalpasswort ermöglichen. Ein nicht authentifizierter Angreifer kann unter Ausnutzung der Schwachstelle per Fernzugriff die Hashwerte der Passwörter auslesen und entschlüsseln. Mit den gewonnenen Informationen können dann weitere Angriffe durchgeführt werden. CVSS Base Score: CVSS v3 7.2. /BSI21i09, BAC22w01, CIS21i06/
- **CVE-2020-1971**: In der OpenSSL-Bibliothek kann ein Angreifer über ein manipuliertes Zertifikat unter bestimmten Bedingungen einen Denial-of-Service-Angriff durch-führen und damit den Controller zum Absturz bringen. CVSS Base Score: CVSS v3 5.9. /NVD22w01/, /RED20w01/

Bei fehlerhafter Konfiguration des Sicherheitslevels oder bei Nutzung unsicherer Dienste wie z. B. Telenet oder FTP, kann dies zur Ausnutzung weiterer Schwachstellen für die Durchführung nicht authentifizierter Zugriffe oder für den Diebstahl von sensiblen Informationen führen. Unsicher sind die Sicherheitslevel 0 bis 3. Ist dagegen das Sicherheitslevel 4 konfiguriert, ist die Kommunikation mit dem Gerät auf TLS-abgesicherte Dienste beschränkt und Passwort-Hashes können dann nur durch einen authentisierten Benutzer ausgelesen werden. /CIS21i06/

Derzeit liegen keine Informationen über eine erfolgte Ausnutzung der Schwachstellen vor. Die Schwachstellen werden mit dem am 11.01.2021 veröffentlichen Patch M-Base V4.49-P1 bzw. dem am 18.01.2021 veröffentlichten Patch M-Base V3.95R-P8 behoben. Bachmann empfiehlt eine Prüfung der Schutzbedürfnisse und Gefährdungsszenarien. Ausgehend von dieser Prüfung sollten entsprechende Software-Updates durchgeführt oder das jeweilige Patch mit nachfolgender Aktivierung des neuen Ablageverfahrens für Passwörter (SHA-512) angewendet werden. /BSI21i09/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.5.4 INFRA:HALT – Schwachstellen in Netzwerkstacks

Übersicht

Das IT-Unternehmen Forescout setzt die Arbeit zur Untersuchung von TCP/IP Stacks auf Schwachstellen kontinuierlich fort. Unter dem Titel INFRA:HALT veröffentlichte Forescout einen umfassenden Bericht zu insgesamt 14 neu entdeckten Schwachstellen im NicheStack (auch bekannt als Interniche) TCP/IP Stack. Die Bedeutung des NicheStacks ergibt sich insbesondere aus seiner Verbreitung, mehr als 200 verschiedene Anbieter von OT Systemen werden zu den Kunden des NicheStacks gezählt. /FOR21r02/

Beschreibung

Seit mehreren Jahren analysiert Forescout verschiedene TCP/IP Stacks auf Schwach-stellen und stellt die Veröffentlichungen in umfassenden Berichten der

Öffentlichkeit vor. Diesmal wurde ausschließlich der NicheStack des Unternehmens HCC Embedded untersucht, da dieser Stack insbesondere in Embedded Systems eingesetzt wird und damit bei OT Systemen eine hohe Verbreitung hat. Insgesamt 14 Schwachstellen wurden hierbei aufgedeckt. Die Schwachstellen können nur bei Netzwerkzugriff ausgenutzt werden und ermöglichen zum einen das Auslösen von Denial-of-Service-Zuständen auf betroffenen Systemen sowie bei zwei kritischen Schwachstellen das Ausführen beliebigen Codes /FOR21r02/.

Forescout gibt in /FOR21r02/ als prominentestes Beispiel für betroffene Systeme die weit verbreitete speicherprogrammierbare Steuerung des Typs S7 von Siemens an, da diese den NicheStack für ihre TCP/IP basierte Kommunikation nutzt. Siemens hat diese Betroffenheit im eigenen Sicherheitshinweis /SIE21r02/ nicht bestätigt, lediglich einige Kommunikationsmodule spezifischer Leistungsschalter von Siemens sind betroffen. Weitere bestätigte betroffene Unternehmen sind Phoenix Contact, Rockwell Automation und Schneider Electric.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r08/

A.5.5 Nucleus:13 – Schwachstellen in Netzwerkstacks

Übersicht

Forescout hat im Laufe des Jahres 2021 die Arbeiten an der Erforschung von Schwach-stellen von TCP/IP Stacks kontinuierlich fortgesetzt und veröffentlichte im November 2021 gemeinsam mit Medigate Labs einen Report über insgesamt weitere 13 neue Schwachstellen im TCP/IP Stack Nucleus, welcher von Siemens entwickelt wird. Nucleus ist ein seit 2018 zu Siemens gehörender TCP/IP Stack, welcher zum einen einzeln innerhalb von Software angeboten wird und zum anderen als Nucleus ROTS Echtzeitbetriebssystem Verbreitung in medizinischen, automobilen und industriellen Anwendungen findet. /FOR21r04/

Beschreibung

Aufgrund der Verbreitung von TCP/IP Stacks in jedem über TCP/IP kommunizierendem IT-System fokussiert sich die Forescout Forschung zu Schwachstellen auf verschiedene weit verbreitete open source und kommerzielle TCP/IP Stacks. Der Nucleus TCP/IP Stack war bereits von den NAME:WRECK Schwachstellen und wurde auch aufgrund seiner industriellen Anwendung noch einmal spezifisch untersucht. Die neu entdeckten Schwachstellen besitzen einen CVSS Score zwischen 5,3 und 9,8 und ermöglichen Denial-of-Service Angriffe, die Ausführung beliebigen Codes sowie Informationsabflüsse.

Siemens veröffentlichte zum selben Zeitpunkt wie Forescout ein Security Advisory, welches die Schwachstellen darstellt. Für alle betroffenen Nucleus Versionen sowie das Nucleus RTOS hat Siemens Updates veröffentlicht, welche die Schwachstellen beseitigen. Die Hersteller von Systemen, welche Nucleus Produkte nutzen (gemäß Siemens mehr als 3 Milliarden IT-Systeme), müssen nun die Updates des Nucleus TCP/IP Stack oder des Nucleus RTOS mittels eigenen Updates an die Kunden ausliefern. Analog zu den NAME:WRECK Schwachstellen sind weder die genauen betroffenen IT-Systeme noch der aktuelle Stand der individuellen Systemupdates. /FOR21r04/, /SIE21r03/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r08/

A.5.6 Schwachstellen im DDS Protocol

Übersicht

Data Distribution Service (DDS) ist ein von der Object Management Group (OMG) entwickeltes Protokoll für die Verteilung von Daten in Netzwerken von Echtzeit bearbeiten-den IT-Systemen. Es erlaubt den in den Echtzeitnetzwerken verbundenen IT-Systemen Daten zu senden, zu empfangen und Kommandos auszusenden und Ereignisse zu verarbeiten und wurde gezielt für industrielle Steuerungssysteme mit Echtzeitanforderungen entwickelt. Auf der IT-Sicherheitskonferenz Black Head Europe 2021

im Dezember 2021 zeigte ein Team von Forschern ihr Forschungsergebnis im Bereich der DDS Schwachstellen und veröffentlichte einen Bericht mit insgesamt 13 Schwachstellen in 6 von 10 angebotenen DDS Lösungen. /CIS22r02/

Beschreibung

Data Distribution Service (DDS) ist eine sogenannte Middleware, im Schichtsystem der Kommunikation (ISO-OSI Modell) übernimmt Middleware die Aufgabe einer Verteilungsplattform oder eines Protokolls und verteilt bereitgestellte Daten zwischen unterschiedlichen Anwendungen. Industrielle Steuerungssysteme benötigen in den meisten Fällen eine Form von Echtzeitkommunikation, welche sich von der normalen TCP/IP Kommunikation abweichend durch höhere Reaktionsgeschwindigkeiten und Zeitgenauigkeiten auszeichnet. Mehr als 10 verschiedene Anbieter führen DDS Lösungen zur Implementierung im Echtzeitkommunikationsumfeld an. Es ist daher anzunehmen, dass DDS Lösungen in mehreren Milliarden echtzeitfähigen Geräten in industriellen Steuerungssystemen zur Anwendung kommen. Die 13 Schwachstellen teilen sich auf die DDS Lösungen Fast-DDS, OpenDDS, Connext DDS, CoreDX DDS, Gurum DDS und CycloneDDS und wurden mit einem CVSS Base Score von 6,6 bis 8,7 bewertet. Die Schwachstellen ermöglichen Angreifern unterschiedliche Einwirkungsmöglichkeiten wie das Schreiben von beliebigen Werten in spezifische XML-Dokumente, die Auslösung von Denial-of-Service Bedingungen und die Ausführung beliebigen Codes. Die Anbieter der DDS Lösungen veröffentlichten in Folge des Bekanntwerdens der Schwachstellen Updates, als Supply-Chain Softwareelemente müssen diese Updates jedoch von Anbietern der tatsächlich betroffenen IT-Systeme verarbeitet und schließlich mit eigenen Updates verbreitet werden. Die CISA hat daher eine Reihe von Mitigationsmaßnahmen veröffentlicht, wie der minimalen Zugriffsmöglichkeit im Anlagennetzwerk, der Isolation des leittechnischen Echtzeitnetzes von anderen Netzwerken und Schutzmaßnahmen für Remotezugriffe wie VPNs. /CIS22r02/

Aufgrund der industriell weiten Verbreitung von Echtzeitnetzwerken und damit DDS nutzenden IT-Systemen, ist von einer hohen Verbreitung der Schwachstellen bei gleichzeitig nicht optimalen Updateverläufen aufgrund der Lieferkettenthematik auszugehen. Eine letztendliche Abschätzung des Umfangs der Betroffenheit ist aufgrund dieser Unwägbarkeiten nicht möglich.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.5.7 BadAlloc – Schwachstellen in echtzeitfähigen OT- und IoT-Geräten

Übersicht

Unter dem Namen BadAlloc werden eine Serie von mehr als 25 Schwachstellen in ins-besondere bei Echtzeitbetriebssystemen für OT-, IoT- und IIoT-Systeme zusammengefasst. Der Name leitet sich daraus ab, dass die Schwachstellen verschiedene Speicherfunktionen ausnutzen, welche als „Bad Allocation of Memory“ (kurz BadAlloc) bezeichnet werden. Werden die Schwachstellen ausgenutzt, können Angreifer zum einen Denial-of-Service-Zustände bei betroffenen Geräten auslösen, zum anderen ermöglichen ein Teil der BadAlloc Schwachstellen das Ausführen beliebigen Codes durch Angreifer. /CIS21i01/

Beschreibung

Fehlerhaftes Speichermanagement und damit einhergehende Schwachstellen waren bereits vor den Veröffentlichungen zu BadAlloc ein bekanntes Problem. So basieren mehrere TCP/IP Schwachstellen aus Sammlungen wie AMNESIA:33 auf fehlerhaftem Speichermanagement der betroffenen TCP/IP Stacks. Ende April 2021 veröffentlichte die Sektion 52 von Microsoft, die Azur Defender for IoT Security Research Group, einen um-fassenden Bericht zu Schwachstellen in verschiedenen Echtzeitbetriebssystemen. Solche Betriebssysteme werden zum einen in OT- und IIoT-Systemen verwenden, in denen zeitgenaue Signale und Datenverarbeitungen notwendig sind sowie in IoT-Systemen, welche einfache und günstige Betriebssysteme benötigen. Viele dieser Echtzeitbetriebssysteme sind hierbei keine Neuentwicklungen der Entwickler der IoT-, OT- und IIoT-Systeme, sondern werden entweder vollständig oder als SDK (Software Development Kit) eingekauft und angepasst. /MIC21r01/

Die Schwachstellen basieren darauf, dass bei schlecht implementierter Allokation von Speicherraum Daten unvorhergesehen gespeichert oder verarbeitet werden. Hierbei kann bei einer Datenanfrage an den Speicher des Systems der tatsächlich abzurufende Speicher von dem innerhalb des Kopfes der Datenanfrage angegebenen Speicherbedarfs abweichen.

Das System antwortet auf eine solche Anfrage mit einem zugeordneten, zu kleinen Speicherbereich. Die dann mit der Datenanfrage mitgelieferten Informationen, z. B. Teile einer Schadsoftware, überragen dann den zugeordneten Speicherbereich, was zu einem sogenannten Overflow führt. Infolgedessen kann Schadsoftware außerhalb des zugewiesenen Speichers ausgeführt werden, was zu der Möglichkeit des Ausführens von beliebigem Code führt. /MIC21r01/

Unsichere Allokationen von Speichern sind weit verbreitete Schwachstellen, welche seit Jahrzehnten zu den Hauptgründen für gefundene Softwareschwachstellen zählen. Neu-artig an BadAlloc war die von Microsoft gesammelte Untersuchung von verschiedenen Echtzeitbetriebssystemen und SDKs, welche insbesondere bei IoT-, aber auch bei OT- und IIoT-Systemen Anwendung finden. Zu den betroffenen Echtzeitbetriebssystemen und SDKs gehören sowohl freie als auch kommerzielle Versionen namhafter Anbieter wie Amazon, ARM, BlackBerry, Samsung, Tencent, Texas Instruments, Windriver und viele weitere. Für die meisten betroffenen Betriebssysteme und SDKs stehen Updates bereit, welche die Schwachstellen beheben. Einige betroffene Systeme wie das ARM mbed-ualloc oder das Texas Instruments SimpleLink MSP432E4 erhalten als veraltete Systeme keine weiteren Updates. /CIS21i01/

Da keine spezifischen IoT-, OT- oder IIoT-Systeme von den Schwachstellen betroffen sind, sondern eine hohe Anzahl an auf IoT-, OT- und IIoT-Systemen angewendeten Betriebssystemen bzw. deren Ausgangs-SDKs ist eine vollständige Abschätzung welche und wie viele Systeme betroffen sind zum aktuellen Zeitpunkt nicht möglich. Hersteller, welche die betroffenen Betriebssysteme bzw. SDKs nutzen, sind aufgerufen für ihre Produkte entsprechende Updates bereitzustellen.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.5.8 Siemens SIPROTEC 4

Übersicht

Zwei Schwachstellen gefährden SIPROTEC 4-Schutzrelais von Siemens. Diese Geräte werden häufig in Umspannwerken eingesetzt.

Über die DIGSI4- und EN100-Ethernet-Kommunikationsmodule können unter Ausnutzung der Schwachstellen Autorisierungspasswörter rekonstruiert oder überschrieben werden. /SIE18i03/

Beschreibung

Siemens berichtete erstmals am 08.03.2018 in seinem Sicherheits-Advisory SSA-203306: Password Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact Relay Families // von zwei Schwachstellen, die SIPROTEC 4-Schutzrelais betreffen. Das Advisory wurde am 13.07.2021 zuletzt aktualisiert. Darin wird beschrieben, dass Angreifer über die beiden nachfolgend erläuterten Schwachstellen und über die DIGSI4- und EN100-Ethernet-Kommunikationsmodule der Geräte Autorisierungspasswörter rekonstruieren oder überschreiben können: /SIE18i03/

- **CVE-2018-4839**: Ein Angreifer mit lokalem Zugriff auf das Engineering-System oder in einer privilegierten Netzwerkposition mit der Möglichkeit auf den Datenverkehr des Netzwerks zuzugreifen, kann Zugriffs-Autorisierungspasswörter rekonstruieren. CVSS Base Score: CVSS v3.1 4.0.
- **CVE-2018-4840**: Der Engineering-Mechanismus erlaubt einem unautorisierten Nutzer per Fernzugriff eine modifizierte Gerätekonfiguration auf das Gerät zu laden und dabei Zugriffs-Autorisierungspasswörter zu überschreiben. CVSS Base Score: CVSS v3.1 7.5.

Siemens hat entsprechende Firmware-Updates veröffentlicht. Darüber hinaus empfiehlt Siemens ihr Sicherheitskonzept für Umspannwerke und das Defense-in-Depth-Konzept umzusetzen. Darüber hinaus sollte das Risiko eines möglichen Angriffs durch ein angemessenes Netzdesign und durch geeignete Schutzmaßnahmen für den Netzwerkzugriff wie Firewalls, Segmentation und VPN-Verbindung minimiert werden. /SIE18i03/

Die Cybersecurity & Infrastracture Security Agency (CISA) der USA berichtete in ihrem ICS Advisory (ICSA-18-067-01) /CIS21i02/ ebenfalls über die Schwachstellen. Sie empfiehlt zusätzlich sicherzustellen, dass über das Internet nicht auf die Geräte zugegriffen werden kann, indem das ICS, in dem sich die Geräte befinden, vom Firmennetzwerk getrennt ist. Es müsse beachtet werden, dass auch VPN-Verbindungen Schwachstellen aufweisen können und nur so sicher wie die miteinander verbundenen Geräte sind. VPN-Server sind regelmäßigen Updates zu unterziehen. /CIS21i02/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

A.5.9 Kameras Geutebrück

Übersicht

Am 08.07.2021 wurden 12 Schwachstellen in der IP-Kamera Firmware des Herstellers UPD Technology bekannt. Von den Schwachstellen sind verschiedene Hersteller von IP-Kameras betroffen, die die Firmware in ihren Geräten einsetzen, darunter Geutebrück.

Beschreibung

Am 08.07.2021 berichtete der IT-Sicherheitsdienstleister RandoriSec über mehrere Schwachstellen in der IP-Kamera Firmware des Herstellers UPD Technology. Die Cybersecurity and Infrastructure Security Agency (CISA) der USA veröffentlichte im Juli 2021 einen Bericht über die Schwachstellen. Die Firmware wird von mehreren Herstellern von IP-Kameras wie Geutebrück, Ganz, Visualint, Cap, THRIVE Intelligence, Sophus, VCA, TripCorps, Sprinx Technologies, Smartec und Riva eingesetzt. Über die Schwachstellen kann ein Angreifer den Authentifizierungsprozess umgehen und per Internetverbindung, LAN oder WLAN beliebigen Programmcode auf dem Gerät ausführen. Dies kann zum Kontrollverlust über das System, einen Teil seiner Komponenten und / oder zum Diebstahl sensibler Daten führen. Beim Hersteller Geutebrück sind die Kameras der E2 Serie G-CAM EBC-21xx, EFD-22xx, ETHC-22xx und EWPC-22xx so-wie die A/D Signalkonvertor für Video- und Audiosignale Encoder G-Code der Firmwareversionen <= 1.12.027, 1.12.13.2 und 1.12.14.5 von den Schwachstellen betroffen. /BSI21i11/, /IND21w01/

Zurzeit sind 12 Schwachstellen bekannt: /MAL21w05, CIS21i09/:

- **CVE-2021-33543**: Fehlende Authentifizierung: Die Schwachstelle erlaubt nicht authentifizierten Remote-Zugriff auf sensible Dateien durch Voreinstellungen bei der Benutzerauthentifizierung. CVSS v3 Base Score: 9.8.

- Bei den sieben Schwachstellen CVE-2021-33544, CVE-2021-33548 und CVE-2021-33550 bis CVE-2021-33554 handelt es sich um Remote Code Execution (RCE) Schwachstellen. Sie ermöglichen einem Angreifer per Remote-Zugriff die Ausführung von beliebigem Programmcode und besitzen jeweils den CVSS v3 Base Score 7.2.
- Die verbleibenden vier Schwachstellen sind ebenfalls RCE-Schwachstellen. Sie er-möglichen einen speicherbezogenen Pufferüberlauf in einem von der jeweiligen Schwachstelle abhängigen Parameter: CVE-2021-33545 (Zähler-Parameter), CVE-2021-33546 (Namens-Parameter), CVE-2021-33547 (Profil-Parameter) und CVE-2021-33549 (Aktions-Parameter). Dadurch ist ein Angreifer in der Lage beliebigen Programmcode per Remote-Zugriff auszuführen. Alle vier Schwachstellen besitzen den CVSS v3 Base Score 7.2.

Nachdem der Firmware-Hersteller UPD Technology nicht reagierte, arbeiteten Rand-ori-Sec und Geutebrück zusammen, um die Schwachstellen zu schließen. Geutebrück hat für seine betroffenen Geräte eine aktualisierte Firmware auf seiner Webseite veröffentlicht. Der Hersteller empfiehlt die Firmware auf die Version 1.12.14.7 oder höher upzudaten. Falls die Firmwareupdates nicht installiert werden können, rät Geutebrück Nutzern die Standardpasswörter der Kameras zu ändern und die Geräte vom Internet zu trennen. Ob die anderen genannten Hersteller ebenfalls Updates zur Behebung der Schwachstellen zur Verfügung stellen, ist nicht bekannt. /BSI21i11, IND21w01/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.5.10 DIAEnergie

Übersicht

Im Jahr 2021 wurde bekannt, dass das industrielle Energiemanagementsystem (EMS) DIAEnergie des Herstellers Delta Electronics mehrere kritische Sicherheitslücken auf-weist. DIAEnergie ermöglicht Unternehmen unter anderem die Visualisierung von elektrischen und energetischen Systemen sowie die Überwachung und Steuerung durch manuelle und automatisierte Systeme.

Im letzten Jahr wurde von insgesamt acht Sicherheitslücken berichtet, wobei sechs der acht Sicherheitslücken mit einem CVSS-Score von 9,8 bewertet wurden. Die sich aus den Sicherheitslücken ergebenden Angriffsmöglichkeiten umfassen das Abfangen von Passwörtern im Klartext, das Hinzufügen neuer Benutzer mit Admin-Rechten und das Ausführen beliebigen Codes auf Basis von SQL-Injections bzw. Dateiupload-Möglichkeiten. /HEI21w12/ Im März 2022 veröffentlichte die CISA einen aktualisierten Sicherheitshinweis DIAEnergie betreffend mit einer Übersicht über diverse Schwachstellen. /CIS22i04/

Beschreibung

Das industrielle Energiemanagementsystem DIAEnergie dient Unternehmen in vielfältigen Bereichen der Überwachung und Steuerung von Anlagen, beispielsweise zur Echtzeitüberwachung und Analyse des Energieverbrauchs, der Optimierung der Anlagenleistung und zur Maximierung der Energieeffizienz. Dazu erstreckt sich das System über weite Anlagenteile und kann über industrielle Netzwerk bis hin zur Feldebene mit einzelnen Komponenten kommunizieren. DIAEnergie kann unter anderem auch für die Fernwartung verwendet werden und lässt sich in verschiedene industrielle Steuerungssysteme (ICS) integrieren. Die Kommunikation findet dabei generell über Modbus bzw. OPC statt. Eine Vielzahl der öffentlich gewordenen Schwachstellen basiert auf sogenannten SQL-Injections, bei denen Sicherheitslücken im Zusammenhang mit SQL-Datenbanken ausgenutzt werden. Eine Sicherheitslücke entsteht dabei durch einen Programmierfehler in einem Programm, das auf die Datenbank zugreift. Dadurch können potenzielle Angreifer zum Beispiel Befehle einschleusen, Daten aus der Datenbank aus-lesen, Daten unberechtigt ändern oder löschen und ggf. die Kontrolle über den kompletten Datenbankserver übernehmen. /SEC21w16/

Ursprünglich wurde im August 2021 von insgesamt 8 Sicherheitslücken berichtet, woraufhin die CISA eine entsprechende Meldung veröffentlichte. /CIS22i04/ Diese wurde mittlerweile mehrfach aktualisiert und es wurde eine weitere Warnmeldung durch die CISA veröffentlicht, die ebenfalls mehrfach aktualisiert wurde /CIS22r02/. Darin wird berichtet, dass etwa 30 Sicherheitslücken DIAEnergie betreffend gefunden wurden, wobei mittlerweile mit Hilfe von Softwareupdates einige Sicherheitslücken behoben werden konnten. Eine Ausnutzung der Schwachstellen erfordert keine Authentifizierung und ermöglicht es einem Angreifer unter Umständen die vollständige Kontrolle über DIAEnergie und die Systeme zu übernehmen, auf denen es eingesetzt wird. Betroffen sind dabei verschiedene Versionen von DIAEnergie. /SEC21w16/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

A.5.11 Schwachstelle in Johnson Controls Videoüberwachungs- und Zugangskontrollsystem

Übersicht

Am 26.08.2021 veröffentlichte die Cybersecurity & Infrastructue Security Agency (CISA) der USA Informationen zu einer Schwachstelle im Zugangskontroll- und Sicherungssystem CEM Systems AC2000 von Johnson Controls. Zwei weitere Schwachstellen, die das Videoüberwachungssystem ExacqVision von Johnson Controls betreffen, wurden am 07.10.2021 bekannt. Auch über diese Schwachstellen wurde vom CISA berichtet. /BSI21i07/, /CIS21i03/, /CIS21i04/, /CIS21i05/

Beschreibung

CEM-Systems ist ein Anbieter von Zugangskontrollsystemen und vollständig integrierten Sicherheitsmanagementsystemen. Die folgende Schwachstelle hat Auswirkungen auf das Unternehmens-Zugriffskontroll- und integriertes Sicherheitsmanagementsystem AC2000 von CEM Systems, welches von Johnson Controls vertrieben wird. AC200 wird in den USA in den Bereichen kommerzielle Einrichtungen, Petrochemie, Flugzeugverkehr, Bildungswesen und Kritische Fertigung eingesetzt. /BSI21i07/, /JCC20t01/, /JCI21i01/

- **CVE-2021-27663:**

Unter bestimmten Bedingungen wird für Funktionen, die eine prüfbare Nutzeridentifizierung benötigen, keine angemessene Autorisierungsprüfung durchgeführt. Diese Schwachstelle betrifft nur Nutzer, die die Single Sign On (SSO)-Funktion implementiert und das Application Programming Interface (API) des AC2000 installiert haben und die Programmversionen 10.1 bis 10.5 verwenden. Betroffene sollten sich an den technischen Support des CEM wenden, um das erforderliche Patch zu erhalten. CVSS Base Score: CVSS v3 8.2. /JCI21i01/, /CIS21i03/

ExacqVision ist eine Videoüberwachungslösung von Exacq Technologies, ein Unter-nehmen, das zu Johnson Controls gehört. Das Produkt umfasst Videomanagement-software (VMS), Netzwerk-Videorekorder (NVR) und Speicher-Server. Die beiden folgenden Schwachstellen haben Auswirkungen auf den exacqVision-Internetdienst und den exacqVision-Server. Der Internetdienst erlaubt Nutzern Videodateien und andere Daten über einen Browser oder über das Mobiltelefon vom exacqVision-Server abzurufen. Durch die Ausnutzung der Schwachstellen können Zugangsdaten gestohlen und das Videoüberwachungssystem außer Funktion gesetzt werden. ExacqVision wird im Bildungs- und Gesundheitswesen, in Unternehmen und im Einzelhandel eingesetzt. /HEI21w05, JCI21i02, JCI21i03/

- **CVE-2021-27664**:

Wenn die Passthrough-Funktion bzw. der nicht authentifizierte Zugriff aktiviert sind, können über den Internetdienst Anmeldeinformationen für andere mit exacqVision verbundene Systeme offengelegt werden. Einem nicht authentifizierten, per Fernzugriff agierenden Nutzer kann auf diese Weise Zugang zu Berechtigungen gewährt werden, welche auf dem exacqVision-Server gespeichert sind. Betroffen sind die Version 21.06.11.0 des exacqVision-Servers und ältere Versionen. Johnson Controls empfiehlt den exacqVision-Server auf Version 21.09. upzugraden. CVSS Base Score: CVSS v3 9.8. /JCI21i02, CIS21i04/

- **CVE-2021-27665**:

Unter bestimmten Einstellungen kann ein nicht authentifizierter, per Fernzugriff agierender Nutzer eine potenzielle Integer-Overflow-Bedingung des exacqVision-Servers in Verbindung mit einem speziell angefertigten Skript ausnutzen, um einen DoS-Angriff durchzuführen. Betroffen sind die 32-Bit-Version 21.06.11.0 des exacqVision-Servers und ältere Versionen. Johnson Controls empfiehlt die 32-Bit-Version des exacqVision-Servers auf Version 21.09. oder auf 64-Bit-Versionen upzugraden. CVSS Base Score: CVSS v3 7.5. /JCI21i03/, /CIS21i05/

Das CISA berichtet in seinen ICS Advisories ICSA-21-238-01, ICSA-21-280-01 und ICSA-21-280-03 über die Schwachstellen und empfiehlt vorbeugende Maßnahmen. Steuerungssysteme, Systeme und Geräte sollten vom Internet getrennt sein, durch Firewalls abgesichert und vom Firmennetzwerk getrennt werden. Bei Fernzugriff auf Systeme sollten Virtuelle Private Netzwerke (VPNs) eingesetzt werden.

Dabei ist zu beachten, dass auch VPN-Verbindungen Schwachstellen aufweisen können und daher immer auf die neueste Version aktualisiert werden müssen. Darüber hinaus sind VPN-Verbindungen nur so sicher wie die über sie verbundenen Geräte. /CIS21i03, CIS21i04, CIS21i05/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

A.5.12 Log4Shell: Kritische Zero-Day Schwachstelle in der Java Bibliothek log4j

Übersicht

Am 09. Dezember 2021 wurden auf der Code-Sharing Plattform GitHub Informationen zur Schwachstelle Log4Shell für die Java Logging-Bibliothek Log4j veröffentlicht. Da die Programmiersprache Java keine eigenen Logging-Funktionen besitzt und Log4j sich in der Vergangenheit als die zentrale Logging-Bibliothek für Java etablierte, besitzt Log4j eine sehr hohe Verbreitung bei Java-basierten Softwaren sowie Systemen. Java selbst ist auf Milliarden von IT-Systemen installiert, neben Bürosystemen auch insbesondere auf Linux-basierten Industriellen PCs (IPCs), (industrial) Internet of Things (IoT/IIoT) Anwendungen und leittechnischen Systeme. /CIS21w03, /APA21w01/

Beschreibung

Log4j wurde im Januar 2001 erstmal vom Entwickler Ceki Gülcü veröffentlicht und seit-dem als Open-Source Software von der Apache Software Fondation weiterentwickelt. Da die Programmiersprache Java bzw. das Java Development Kit für Entwickler keine eigenen Logging-Funktionen besitzt, haben sich im Laufe der Zeit eine Reihe von speziellen Frameworks[7] etabliert, mit welchen Logging-Funktionen in auf Java basierender Software und Betriebssystemen integriert werden können.

[7] Frameworks, wörtlich übersetzt Rahmenstruktur, beschreiben in der Softwareentwicklung sogenannte Programmiergerüste. Frameworks sind keine allein lauffähigen Softwareprogramme, sondern ermöglichen Programmierern mit Hilfe des Frameworks Anwendungen zu schaffen oder in bestehenden Anwendungen Funktionen zu integrieren.

Log4j ist das weiteste verbreitete Logging-Framework für Java und wird von einer sehr hohen Anzahl an auf Java basierenden Software-Pakete, Firmware und Betriebssystemen verwendet. Java selbst ist eine von Oracle entwickelt und vertriebene objektorientierte Programmiersprache, welche zu den drei meistverbreiteten Programmiersprachen der Welt gehört. Logger wie Log4j übernehmen bei Implementierung in auf Java basierender Software die Aufgabe der Sammlung und Verarbeitung von auflaufenden Meldungen der Software. /CIS21w03, /APA21w01, NVD21w01/

Auf Java basierende Programme senden Nachrichten verschiedener Level an den Logger. Der Logger greift auf sogenannte Levelklassen zurück, mit welchen die aufgelaufenen Meldungen bewertet werden. Eingesetzte Filter ermöglicht eine weitergehende Kontrolle über den Umgang mit Meldungen, mit einem ResourceBundle können optional Meldetexte und andere Informationen mit den Meldungen verknüpft werden. Niederstufig definierte Meldungen und solche Meldungen, die über den Filter definiert werden, werden vom Logger verworfen, alle anderen Meldungen werden an den LogRecorder weitergeleitet, welcher die Meldungen in ein Objekt bindet und an den Handler weiterleitet. Der Handler kann weitere Logik abhängig von den Loglevel und anderen angewendeten Filtern verwenden. Der Handler wird anhand dieser Logik weitere Nachrichten verwerfen und die übrigen entsprechend den Vorgaben des Formatters in ein bestimmtes Format überführen und über eine Console, einen Bildschirm, eine Datei oder eine andere Ausgabemöglichkeit ausgeben. Die so herausgegebenen Logging-Nachrichten können dann von Nutzern oder Administratoren gelesen werden. /CIS21w03, APA21w01/

Die Log4j Ausgabe ermöglicht die Einbeziehung von Java-Variablen. Die Schwachstelle Log4Shell ermöglicht, dass diese Einbeziehung praktisch unbegrenzt und ohne Rechteabfrage genutzt werden kann, sodass auch externe Java-Bibliotheken über Log4j aufgerufen werden können. In diesen Bibliotheken kann sogenannter Shell-Code[8] integriert werden, welcher dann zur Ausführung beliebigen Codes auf dem betroffenen System führen kann, woher der Name der Schwachstelle Log4Shell stammt. Betroffen sind die Log4j Versionen 2.0 bis 2.14 mit Ausnahme der Version 2.12.2.

[8] Shell-Code beschreibt in der Programmierung eine bestimmte Sorte getarnten Codes. Dieser Code wird erst geschrieben, kompiliert, zurückübersetzt und anschließend nachprogrammiert. Man erhält hierdurch einen getarnten Code, welcher in andere Programme integriert werden kann. Ziel ist es mittels dieses Codes ein Kommandozeilensystem wie die Windows-Konsole oder Linux Bash zu starten und schadhaften Code hiermit auszuführen.

Mit dem Update auf Log4j 2.15 wurde am 06. Dezember 2021 die Möglichkeit zur Deaktivierung der der Schwachstelle Log4Shell zugrunde liegenden Befehlsreihen etabliert. Mit dem Update Log4j 2.16 wurden die zugrunde liegenden Befehlsreihen aus dem Code von Log4j voll-ständig entfernt. In Log4j 2.16 wurden weitere Fehler entdeckt, die mit der Version Log4j 2.17 und anschließend 2.17.1 vollständig behoben wurden. Die Version Log4j 2.17.1, veröffentlicht am 28. Dezember 2021, ist nach bisherigen Erkenntnissen frei von allen bekannten Log4j Schwachstellen. /HIS21r01, CIS21w03, /CIS21w04/

Java ist neben dem Consumerbereich auch umfassend in Servern und im leittechnischen Bereich verbreitet, die Verbreitung von Log4j ist durch die umfassende Nutzung von Log4j in Java analog anzusehen. Zu den betroffenen Systemen gehören darüber hinaus Java nutzende Systeme mit eingeschränkter Programmierfähigkeit wie industriel-le Steuerungen, SCADA oder DCS Systeme, Systeme im Internet of Things (IoT und IIoT), Netzwerksysteme wie Router und weitere Systeme wie Kameras, Scanner, RFID-gesteuerte Systeme usw.. In einer aktuelle Übersichtsliste werden mehr als 2800 betroffene IT-Systeme von mehr als 100 betroffenen Herstellern von der amerikanischen CISA aufgeführt. Zu den betroffenen Herstellern gehören große und weit verbreitete Hersteller wie ABB /ABB21r01/ Cisco /CIS21w01/ Citrix /CIT21w01/ Emerson /EME21r01/ Phoenix Contact /PHO21r02/ Rockwell Automation /GIT21w02/ Schneider Electric /GIT21w02/ Siemens /SIE21r04/ oder VMware /VMW21r01/.

Die ersten Angriffe über die Schwachstelle fingen spätestens mit dem 01. Dezember 2021 an, die Anzahl der Angriffe hat sich mit der Veröffentlichung am 09. Dezember 2021 drastisch zugenommen. Da die Schwachstelle vollautomatisiert direkt über das Internet angegriffen werden kann, ist ein großer Teil der Angriffslast auf automatisierte Angriffe zurückzuführen. Innerhalb von Netzwerken kann die Schwachstelle zur lateralen Bewegung ausgenutzt werden. Log4Shell ermöglicht damit mit einfachsten Cyberangriffen die vollständige IT-Systemübernahme und wird daher mit einem CVSS Base Score von 10 von 10 Punkten als hoch kritisch bewertet. /AQU21w01/

Zur Mitigation besteht mittlerweile das schwachstellenfreie Update Log4j 2.17.1 bereit. Anbieter müssen für ihre Produkte eigene Patches entwickeln und bereitstellen. Alternativ kann Log4j deaktiviert werden, was zu Funktionseinschränkungen führt. Das ältere Log4j 1 ist nicht von Log4Shell betroffen, jedoch von anderen schwerwiegenden Schwachstellen, für welche keine Updates mehr erscheinen. /HIS21r01, CIS21w03/

Kerntechnischer Bezug

Die GRS ist bekannt, dass Log4J aufgrund seiner enormen Verbreitung u. a. auch in Servern und im leittechnischen Bereich in IT-Systemen kerntechnischer Anlagen eingesetzt wird. Der kerntechnische Bezug der gefundenen Schwachstellen ist dennoch zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wird der Sachverhalt von der GRS aktuell detailliert ausgewertet. /GRS22r01/

A.6 2022

A.6.1 Incontroller/Pipedream – Set aus ICS-spezifischen Angriffswerkzeugen

Übersicht

Am 13.04.2022 veröffentlichte die US-amerikanische CISA in Zusammenarbeit mit dem FBI, der NSA und dem DoE eine Warnmeldung zu einem ICS-spezifischen Set aus Angriffswerkzeugen „APT Cyber Tools Targeting ICS/SCADA Devices“. /CIS22r01/ Zu-dem gibt es entsprechende Berichte und Analysen dieses Sets von den IT-Analysten der Firmen Dragos („Pipedream“) /DRA22w01/ und Mandiant („Incontroller“) /MAN22w01/. Es folgten kurze Zeit später Warnmeldungen des BSI /BSI22i02/ sowie weiterer ausländischer CERT-Behörden zu diesem Thema. Dieses Set aus Angriffswerkzeugen ist inzwischen unter den Namen Incontroller und Pipedream bekannt. Es handelt sich um ein hochkomplexes, maßgeschneidertes und sehr breit aufgestelltes Set aus Angriffswerkzeugen, die zum Einsatz gegen industrielle Steuerungssysteme entwickelt wurden. Dragos und Mandiant geben an, ein Sample von Incontroller/Pipedream bereits seit Anfang 2022 untersucht zu haben. Es gibt bisher keine Informationen zu einem aktiven Einsatz von Incontroller/Pipedream. Aus Sicht des BSI erhöht unabhängig vom bisherigen Einsatz die bloße „Existenz von Incontroller/Pipedream das Bedrohungsszenario für ICS-Systeme“. /BSI22i02/ Nach Einschätzung von Dragos wurde Incontroller/Pipedream von staatlich geförderten Angreifern entwickelt. Die verantwortliche Angreifergruppierung, die Dragos unter dem Namen „Chernovite“ (siehe Abschnitt B.2.10.4) führt, zielt vor allem auf die Manipulation von industriellen Steuerungssystemen.

Beschreibung

Bei Incontroller/Pipedream handelt es sich um ein Set aus maßgeschneiderten Angriffswerkzeugen, die auf industrielle Steuerungssysteme zugeschnitten sind. Incontroller/Pipedream ist in der Lage, ein breites Spektrum von PLCs und im industriellen Umfeld gebräuchlicher Software zu beeinflussen. Hierzu zählen insbesondere ausgewählte Controller von Schneider Electric und Omron. Der modulare Aufbau von Incontroller/Pipedream erlaubt es Angreifern, weitere Komponenten zu entwickeln, um das Set für andere leittechnische Komponenten einsetzbar zu machen und PLCs diverser anderer Hersteller anzugreifen. Incontroller/Pipedream nutzt häufige Industrieprotokolle, sodass auch eine potenzielle Interaktion mit anderen leittechnischen Komponenten, die diese Protokolle nutzen, denkbar ist. Zudem erlaubt es Incontroller/Pipedream Angreifern, Cyberangriffe mit hohem Automatisierungsgrad auf die anvisierten Controller durchzuführen, sodass auch weniger spezialisierte bzw. weniger befähigte Angreifer prinzipiell die Kenntnisse und Fähigkeiten hochqualifizierter Angreifer nachahmen können.

Mit Incontroller/Pipedream demonstrieren die dafür verantwortlichen Angreifer signifikante Kenntnisse und Fähigkeiten zur Unterbrechung, Schwächung und potenziell auch Zerstörung von Industrieanlagen und verfahrenstechnischen Prozessen. Die Möglichkeiten, die Incontroller/Pipedream potenziellen Angreifern bietet, stellen eine Bedrohung für die Verfügbarkeit, die Funktion und die Sicherheit von industriellen Steuerungssystemen und verfahrenstechnischen Prozessen dar. Denkbare Szenarien bei einem Einsatz von Incontroller/Pipedream beinhalten beispielsweise:

- Störungen von Controllern in der betrieblichen Leittechnik zur Unterbrechung verfahrenstechnischer Prozesse,
- die Umprogrammierung von Controllern in der betrieblichen Leittechnik zur Sabotage verfahrenstechnischer Prozesse und
- die Deaktivierung von Controllern in der Sicherheitsleittechnik zur Hervorrufung physischer Schäden.

Konkret ist beispielsweise die Manipulation von Drehgeschwindigkeit und Drehmoment von Omron Motoren möglich. Incontroller/Pipedream erlaubt zudem die schnelle Auskundschaftung von industriellen Netzwerken über eine Vielzahl von Mechanismen, die

beispielsweise auf MAC-Adressen, Ports, Modbus oder proprietäre Protokolle von Omron bzw. Schneider Elektrik abzielen.

Insgesamt kann Incontroller/Pipedream auch zu Cyberangriffen auf Codesys (Integrierte Entwicklungsumgebung für Speicherprogrammierbare Steuerungen), Modbus (eines der am häufigsten genutzten Industrieprotokolle, De-facto-Standard bei der Kommunikation mit PLCs), Windows-basierte Engineering Work Stations (über eine bekannte Schwachstelle CVS2020-15368 in der weit verbreiteten ASRock Motherboard Utility für BIOS- und System-Updates) sowie Open Platform Communications Unified Architecture (OPC-UA, Standard für Datenaustausch) Server eingesetzt werden. Mit Hilfe von Incontroller/Pipedream sind Angreifer unter anderem in der Lage, ein Anlagennetzwerk auszuspähen, Exchange Web Services (EWS) zu infiltrieren, Controller zu deaktivieren und ihre Programmierung zu manipulieren. Die Angriffswerkzeuge sind zudem deutlich auf das Maskieren als „Trusted Processes“ aus-gerichtet und nutzen bei den ICS-spezifischen Modulen keine spezifischen Schwach-stellen aus, sondern verwenden legitime Funktionen wie eine legitime Programmierstation. Vor dem Einsatz von Incontroller/Pipedream ist eine Modifikation oder individuelle Anpassung an die anvisierte Umgebung sehr wahrscheinlich, sodass eine spezifische Detektion schwierig ist. Der von Incontroller/Pipedream auf den PLCs platzierte maliziöse Schadcode ist nach Einschätzung von Dragos für normales Monitoring nicht detektierbar. Dragos geht davon aus, dass solcher Schadcode nur durch eine forensische Analyse der Firmware der Controller detektierbar wäre, und sich daher jahrelang unentdeckt auf PLCs befinden kann.

In der untersuchten Version enthält Incontroller/Pipedream die folgenden Komponenten (die meisten Angriffswerkzeuge enthalten, wie auch das gesamte Set zwei Namen, wobei einer von Mandiant und der andere von Dragos stammt):

- Codecall/Evilscholar: Angriffswerkzeug für Erkennung von, Zugriff auf, Manipulation von und Abschaltung von Schneider Electric PLCs. Das Modul enthält Modbus und CODESYS Funktionalitäten.
- Omshell/Badomen: Angriffswerkzeug zur Auffindung von, Identifikation von und Interaktion mit OMRON PLCs.
- Tagrun/Mousehole: Angriffswerkzeug zur Interaktion mit OPC-UA Servern.
- Icecore/Dusttunnel: Angriffswerkzeug für Aufklärung und Command-and-Control.

- Lazycargo: Angriffswerkzeug zur Ausnutzung der CVS2020-15368 Schwachstelle in einem Treiber für ASRock Motherboards.

Das Ausmaß der Fähigkeiten von Incontroller/Pipedream deckt eine große Mehrheit der aufgeführten Angriffstaktiken der MITRE ATT&CK ICS Matrix ab, wobei lediglich zur Erlangung des Erstzugriffs andere bzw. weitere Angriffswerkzeuge benötigt werden. Derzeit ist nicht bekannt, welche Angriffswerkzeuge die Angreifer für die initiale Infektion vorgesehen haben. Anhand der Controller-spezifischen Module von Incontroller/Pipedream lässt sich momentan auf eine Ausrichtung auf Anlagen zur Energieversorgung sowie LNG-Anlagen (Liquified Natural Gas) schließen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische An-lagen und Einrichtungen. Daher wird der Sachverhalt von der GRS im Rahmen einer Stellungnahme detailliert ausgewertet.

A.6.2 ICEFALL

Übersicht

Im Juni 2022 veröffentlichten Forscher des Unternehmens ForeScout unter dem Namen OT:ICEFALL einen Bericht über insgesamt 56 Schwachstellen, die Geräte von zehn Anbietern von OT betreffen. Die Schwachstellen werden in dem Bericht in vier Kategorien eingeteilt: unsichere technische Protokolle, schwache Verschlüsselung oder fehlerhafte Authentifizierungsverfahren, Fehler in Firmware-Updates und Remote-Code-Ausführung über native Funktionen. Angreifern mit Netzwerkzugriff zu einem betroffenem Gerät ermöglichen diese Schwachstellen unter anderem die Remote-Ausführung von Code, Veränderungen an der Logik, an Daten oder der Firmware von OT-Geräten und Denial-of-Service-Angriffe. Die betroffenen Geräte sind für ihren Einsatz in kritischen Infrastrukturen wie beispielsweise der Öl-, Gas, Chemie- und Nuklearindustrie sowie Stromerzeugung bekannt und werden als „Secure by Design“ bzw. zertifiziert mit entsprechenden OT-Sicherheitsstandards angesehen. Das BSI wurde vor der Veröffentlichung des Berichts über die Schwachstellen informiert und veröffentlichte

diesbezüglich Informationen am 23.06.2022. Die CISA veröffentlichte einen entsprechenden Sicherheitshinweis am 22.06.2022. /BSI22r13/, /CIS22r03/, /FOR22r01/

Beschreibung

Ein wesentlicher Aspekt, der im OT:ICEFALL-Bericht aufgegriffen wird, ist die Tatsache, dass für Operational Technology in der Vergangenheit oftmals wesentliche Grundzüge der Praxis „Security by Design“ nicht angewendet bzw. vernachlässigt wurden, was da-zu geführt hat, dass es diverse Schwachstellen in OT-Geräten gibt, die beispielsweise mit sehr alten Protokollen kommunizieren, keine Schutzmechanismen besitzen und generell eine schlechte allgemeine Sicherheit aufweisen. Demnach gab es bisher t in der Regel für OT-Schwachstellen keine Common Vulnerabilities and Exposures (CVE) Meldungen, da allgemein bekannt war, dass OT-Protokolle und Kommunikation entsprechend unsicher sind. Aufgrund dieses Sachverhalts ist nach Einschätzung des BSI die Gefahr groß, dass ein Angreifer, der Zugriff auf ein Prozesssteuerungsnetz (SCADA-Netz) hat, beliebige Befehle ausführen kann, wodurch es beispielsweise zu einem temporären Ausfall kritischer Dienstleistungen kommen kann. Das BSI geht davon aus, dass eine dauerhafte, physische Schädigung schwieriger zu realisieren ist, da diese genaue Kenntnisse des Prozesses voraussetzt und oft zusätzlich analoge Schutzmaßnahmen etabliert sind. Nach Angaben des BSI haben bereits einige der betroffenen Hersteller auf den Bericht reagiert und Patches bereitgestellt. Die im Bericht genannten Geräte stammen von den Herstellern Bently Nevada, Emerson, Honeywell, JTEKT, Motorola, Omron, Phoenix Contact, Siemens und Yokogawa und entsprechend verwundbare Geräte wurden in Deutschland mit Hilfe der Suchmaschine Shodan gefunden worden (Honeywell Saia Burgess, Phoenix Contact DDI und ProConOS SOCOMM). Neben der Veröffentlichung der entsprechenden CVEs wurden von der CISA außerdem diverse Industrial Control Systems Advisories (ICSAs, Sicherheitshinweise zu industriellen Steuerungssystemen) bezüglich der Schwachstellen veröffentlicht. Die genauen Auswirkungen der einzelnen Schwachstellen hängen maßgeblich von den jeweiligen Funktionalitäten und genauen Einsatzbedingungen ab. Im Bericht sind fünf allgemeine Angriffsmöglichkeiten durch Ausnutzung der Schwachstellen angegeben:

- Remote Code Execution, bei der Angreifer beliebigen Code auf das betroffene Gerät aufspielen und ausführen können (für die Erlangung der vollständigen Kontrolle über das Gerät ist darüber hinaus ein Überschreiben der Firmware erforderlich),
- Denial-of-Service, wobei ein Angreifer den Zugriff auf die Funktion eines Geräts blockiert bzw. dessen Verfügbarkeit einschränkt,

- Datei-/Firmware-/Konfigurationsmanipulation, bei der ein Angreifer wichtige Komponenten bzw. gespeicherte Daten oder die Firmware manipuliert,
- Kompromittierung von Anmeldeinformationen, wobei Angreifer Anmeldeinformationen erlangen, da diese ungesichert gespeichert sind oder übertragen werden und
- Umgehung der Authentifizierung, bei der Angreifer in der Lage sind, bestehende Authentifizierungsmaßnahmen zu umgehen.

Als Mitigationsmaßnahmen werden Im Bericht unter anderem Updates der betroffenen Geräte mit entsprechenden Patches und die Einhaltung gängiger, elementarer Sicherungsmaßnahmen im Bereich Cybersicherheit empfohlen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

A.6.3 Retbleed – Schwachstellen in CPUs

Übersicht

Forscher der Eidgenössischen Technischen Hochschule Zürich haben Informationen zu einer Schwachstelle in Intel- und AMD-Prozessoren veröffentlicht, die ähnlich wie die Spectre-Schwachstellen (siehe Abschnitt A.1.4) auf spekulativer Codeausführung (sie-he Abschnitte A.1.3 undA.1.4) beruht. Bei Ausnutzung der „Retbleed“ genannten Schwachstellen können Daten bzw. Datenfragmente von Angreifern unberechtigt aus dem Speicher ausgelesen werden. Den Retbleed-Schwachstellen wurden die CVE-Einträge CVE-2022-29900 bzw. CVE-2022-29901 (für AMD- und Intel- Prozessoren) zugeteilt. Google entwickelte 2019 die Kompiliertechnik „Retpoline“ zum Schutz vor Spectre-artigen Angriffen, was unter anderem Teil der Windows 10 Sicherheitsupdates im Mai 2019 war. Mit Retbleed ist es möglich, die Sicherheitsmaßnahmen der zum Schutz vor Spectre entwickelten Sicherheitsupdates zu umgehen. Das BSI sieht in Retbleed ein Gefährdungspotenzial vergleichbar mit den Spectre-Schwachstellen. /HEI22w13/, /BSI22r14/

Beschreibung

Retbleed umgeht die Sicherheitsmaßnahmen, die im Zusammenhang mit Spectre-artigen Angriffen entwickelt wurden, durch die geschickte Gestaltung von Return-Kommandos. Dadurch können Datenfragmente aus vermeintlich geschützten RAM-Speicherbereichen ausgelesen werden. Dies ist bei Retbleed mit sehr geringen Geschwindigkeiten von 219 Bytes pro Sekunde für Intel-Prozessoren und 3,9 KByte pro Sekunde für AMD-Prozessoren möglich. Die Forscher haben die Funktionalität für die AMD-Prozessoren AMD Zen1, Zen1+ und Zen 2 und für die Intel-Prozessoren der Generation 6, 7 und 8 erfolgreich getestet. Dabei griffen die Forscher auf Linux-Systeme zurück, wobei angemerkt wurde, dass das grundlegende Problem auf der Hardware-Ebene der betroffenen Prozessoren liegt und auch Microsoft Windows und Apple bzw. MacOS Systeme betroffen sind. Nach Ansicht der Forscher ist Retbleed insbesondere für virtuelle Maschinen mit geteilter Hardware, zum Beispiel bei Cloud-Systemen, relevant. Es wurden bereits mitigative Maßnahmen entwickelt, die jedoch zu Performance-Einbußen im Bereich von 14% bis 39% führen. /COM22w02/, /WAT22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.4 SpringShell – Schwachstelle in der Java Bibliothek Spring

Übersicht

Am 31. März 2022 wurde durch VMware die kritische Schwachstelle SpringShell (häufig Spring4Shell) in der Java Bibliothek Spring MVC und Spring WebFlux öffentlich gemacht. Die als CVE-2022-22965 bekannt gewordene Schwachstelle betrifft analog zu Log4Shell eine weit verbreitete Bibliothek der Programmiersprache Java. Das Spring Framework ist eine umfassende unterstützende Bibliothek, um grundlegende programmiertechnische Infrastruktur in Java-Applikationen zu integrieren, wodurch Java-Programmierer Zeit und Aufwand im Rahmen der Programmierung sparen können. Java selbst ist auf Milliarden von IT-Systemen installiert, neben Bürosystemen auch insbesondere auf Linux-basierten Industriellen PCs (IPCs), auf Systemen im (industrial) Internet of Things (IoT/IIoT) und leittechnischen Systemen. /VMW22w01/, /SPR22W01/

Beschreibung

Das Framework Spring wurde erstmalig im Oktober 2002 in seiner ursprünglichen Version von Rod Johnson entwickelt und wird mittlerweile als Open-Source Software von VMware verwaltet. Als Framework zur Unterstützung der Programmierung in Java bietet Spring eine Vielzahl von Funktionalitäten an und ist gemäß VMware Millionenfach in Endnutzergeräten verbreitet. Im März 2022 kamen Gerüchte zu einer kritischen Schwachstelle in einer Java Bibliothek auf. Tatsächlich analysierten Sicherheitsforscher bereits länger eine kritische Schwachstelle in der Bibliothek Spring für Java, welche dann kurzzeitig über einen Proof of Concept Bekanntheit gewann und dann am 31. März 2022 offiziell als CVE-2022-22965 vom Hersteller veröffentlicht wurde. SpringShell wird aufgrund der Analogien zu Log4Shell auch Spring4Shell genannt und betrifft die Spring Versionen 5.3.0 bis 5.3.17, 5.2.0 bis 5.2.19 sowie ältere Versionen. Unter bestimmten Umständen kann SpringShell auf betroffenen Systemen insoweit ausgenutzt werden, dass beliebiger Code in Form von Shellcode ausgeführt werden kann und damit Vertraulichkeit, Verfügbarkeit und Integrität der Systeme beeinflusst werden kann. Zur Nutzung der Schwachstelle muss das betroffene Java Programm auf dem System im Java Development Kit 9 oder höher entwickelt worden sein, es muss eine bestimmte seltenere Form von Java Container für das Programm angewendet werden und es müssen die Abhängigkeiten spring-webmvc oder spring-webflux angewendet werden. Mit den Spring Versionen 5.3.18 sowie 5.2.20 stehen seit dem 31.März 2022 aktualisierte Versionen von Spring zur Verfügung. /VMW22w01/, /SPR22W01/

Hauptbetroffene Software ist Apache Tomcat, ein Open-Source Webserver mit hoher Verbreitung. Apache Tomcat wird vielfältig in IT- und auch OT Umgebungen eingesetzt, mit der Version 10.0.20 steht eine Version ohne SpringShell Schwachstelle bereit. /SPR22w01/

Besondere Aufmerksamkeit erfuhr SpringShell durch die Ähnlichkeit zur wenige Monate früher bekannt gewordenen Log4Shell Schwachstelle. Beide Schwachstellen betreffen populäre Java Bibliotheken, beide Schwachstellen werden als kritisch angesehen (Log4Shell mit einem CVSS Score von 10 von 10 Punkten, SpringShell mit einem CVSS Score von 9,8 von 10 Punkten) und beide Schwachstellen ermögliche die Ausführung beliebigen Codes bei geringem Aufwand durch die Angreifer. Analog zu Log4Shell wurde auch SpringShell als Schwachstelle noch vor der offiziellen Warnung des Herstellers bekannt, jedoch nicht in der Intensität wie die von Log4Shell.

Der große Unterschied zwischen beiden Schwachstellen ist, dass die SpringShell Schwachstelle nur beim Zusammenkommen von mehreren Bedingungen ausgenutzt werden kann und nicht wie Log4Shell grundsätzlich bei jedem betroffenen System. Bisher sind keine um-fassenden Angriffsserien auf Java Systeme mit Spring Bibliothek bekannt geworden. /VIA22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.5 Schwachstelle in Schneider Electric Easergy P3 und P5

Übersicht

Vier Schwachstellen betreffen die Mittelspannungsschutzrelais Easergy P3 und P5 von Schneider Electric. Sie ermöglichen Angreifern den Datenverkehr in ICS-Netzwerken zu beobachten und Schadsoftware in die Netzwerke einzuschleusen.

Beschreibung

Im Januar 2022 informierte Schneider Electric seine Kunden über Schwachstellen in Mittelspannungsschutzrelais. Bezüglich der Schwachstellen erfolgte im März 2022 eine Warnmeldung der Cybersecurity & Infrastructure Security Agency (CISA) der USA. Sie betreffen die Schutzrelais Easergy P3 und P5 und werden mit dem Bedrohungsgrad „hoch“ eingestuft. Erhalten IT-Angreifer Zugriff auf den fest codierten SSH-Schlüssel des Geräts, können sie auf das mit dem Gerät verbundene ICS-Netzwerk zugreifen und dessen Datenverkehr beobachten sowie Schadsoftware in das Netzwerk laden. Die Schwachstellen werden nachstehend angegeben. /HEI22w11, SEC22w10/

Die folgenden drei Schwachstellen betreffen die Schutzrelais Easergy P5 /SCH22i01, CIS22i03/:

- **CVE-2022-22722**: Hart codierte Anmeldeinformationen können zur Offenlegung von Informationen führen. Ein Angreifer, der den kryptografischen SSH-Schlüssel für das Gerät und die Kontrolle über das lokale Betriebsnetzwerk erhält, kann den mit der Produktkonfiguration verbundenen Datenverkehr beobachten und manipulieren. CVSS v3.1 Base Score: 7.5

- **CVE-2022-22723**: Kopien des Speicherpuffers ohne Überprüfung der Speichergröße können zu einem Überlauf des Puffers führen, der Programmabstürze und die Ausführung beliebigen Codes verursacht, falls speziell gestaltete Datenpakete an das Gerät gesendet werden. Schutz- und Auslösefunktionen über GOOSE[9] können beeinträchtigt werden. CVSS v3.1 Base Score: 8.8

- **CVE-2022-34758**: Eine fehlerhafte Eingabevalidierung kann dazu führen, dass die Watchdog-Funktion des Gerätes deaktiviert wird, falls ein Angreifer Zugriff auf privilegierte Benutzeranmeldeinformationen hatte. CVSS v3 Base Score: 5.1

Die drei Schwachstellen können durch Updates der Firmware auf die Versionen 01.401.101 und 01.303.202 geschlossen werden. Auf welche der beiden Versionen die Firmware zu aktualisieren ist, hängt von der auf dem Gerät installierten Firmware ab. Um das geeignete Firmwareupdate zu erhalten, ist eine Anfrage bei Schneider Electric erforderlich. Falls Kunden nicht das Firmwareupdate für die Schwachstelle CVE-2022-22723 nutzen möchten, können sie die GOOSE-Anwendung des Gerätes deaktivieren, um das Risiko zu minimieren. Ist dies nicht möglich, sollte das Gerät nur in einem sicheren lokalen Netzwerk eingesetzt werden. /SCH22i01/

Die folgende Schwachstelle betrifft Easergy P3 Schutzrelais /SCH22i02/:

- **CVE-2022-22725**: Kopien des Speicherpuffers ohne Überprüfung der Speichergröße können zu einem Überlauf des Puffers führen, der Programmabstürze und die Ausführung beliebigen Codes verursacht, falls speziell gestaltete Datenpakete an das Gerät gesendet werden. Schutz- und Auslösefunktionen über GOOSE können beeinträchtigt werden. CVSS v3.1 Base Score: 8.8

Die Schwachstelle wird durch ein Update der Firmware auf Version 30.205 geschlossen. Um das Update zu erhalten, ist eine entsprechende Anfrage an Schneider Electric zu stellen. Für die GOOSE-Anwendung gelten die gleichen Empfehlungen wie für die Schwachstelle CVE-2022-22723. /SCH22i02/

Die betroffenen Schutzrelais werden in Kraftwerken und im elektrischen Stromnetz ein-gesetzt.

---

[9] GOOSE steht für Generic Object Oriented System-Wide Events. Ziel von GOOSE ist es, die herkömmliche festverdrahtete Logik, die für die Koordination innerhalb der Relais erforderlich ist, durch die Kommunikation zwischen Station und Bus zu ersetzen. /SCH11w01/

Angreifer können Schutzrelais käuflich erwerben und auf die Schwachstellen untersuchen. Über Spear-Phishing-E-Mails können sie Zugriff auf das Büronetzwerk eines Unternehmens erhalten, das die Relais in seinen ICS-Netzwerken einsetzt. Bei ungünstiger Netzwerkarchitektur können die Angreifer den Zugriff vom Büronetzwerk auf das ICS-Netzwerk ausweiten. Sie haben dann die Möglichkeit Spannungsversorgungen von Geräten und Schutzeinrichtungen abzuschalten, so dass auch physische Schäden an anderen Geräten entstehen können. /SEC22w010/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.6 TL Storm 2.0, Schwachstelle in Aruba und Avaya Switches

Übersicht

Aruba und Avaya sind Anbieter von Netzwerktechnologien für Unternehmen und bieten insbesondere Switches und andere Komponenten zum Aufbau von LAN, Wide Area LANs und VLANs an. Am 03.05.2022 wurden von Sicherheitsforschern des Unternehmens ARMIS mit einem unter TLStorm 2.0 genannten Whitepaper insgesamt fünf Schwachstellen in verschiedenen Netzwerktechnologien der Unternehmen Aruba und Avaya der Öffentlichkeit bekannt gemacht. Die auf der Supply-Chain basierenden Schwachstellen werden durch die Nutzung von spezifischen externen Bibliotheken ermöglicht und wurde von ARMIS als schwerwiegend bis kritisch eingestuft. /ARM22r01/

Beschreibung

Im März 2022 veröffentlichte ARMIS einen Bericht zu kritischen Schwachstellen in SMART-UPS™ unterbrechungsfreien Stromversorgungen (USV) des Unternehmens APC (Tochter von Schneider Electric). Die TLStorm genannten Schwachstellen betrafen mit Cloud-Funktionen ausgestattete USV und ermöglichten die Ausführung beliebigen Codes durch IT-Angreifer.

Die Schwachstellen basierten auf einer fehlerhaften Implementierung der TLS[10] Bibliothek Mocana nanoSSL, welche zur Sicherung der Anbindung der USVs an die APC Cloud dient. Mittels der Schwachstellen ist es den Angreifern möglich, die USVs bis zur physischen Zerstörung zu manipulieren. Am 03. Mai 2022 veröffentlichte ARMIS mit TLStorm 2.0 einen Bericht zu Netzwerksystemen, welche ebenfalls die Bibliothek Mocana nanoSSL für TSL Verschlüsselungen nutzen. Zur Implementierung der Mocana nanoSSL Bibliothek müssen die Anwender einer genauen Dokumentation folgen. Ein Beispiel für die Folgen solcher Fehlimplementierungen ist ein schwerer Fehler, der zur Ausführung beliebigen Codes durch Angreifer führen kann, wenn Anwender bei der Implementierung von nanoSSL einen Codezeilenkommando missachten. In den Netzwerkswitchen von Aruba wurden die Schwachstellen CVE-2022-23677 und CVE-2022-23676 entdeckt, welche mit einer CVSS Base Score von 9,0 und 9,1 als schwerwiegend bewertet wurden. Die Schwachstellen betreffen mehrere Interfaces der Aruba-Geräte und ermöglichen Angreifern die Ausführung beliebigen Codes. In Netzwerkswitchen von Avaya wurden die kritischen Schwachstellen CVE-2022-29860 und CVE-2022-29861 mit je einem CVSS Base Score von 9,8 und eine kritische, nicht nummerierte Schwachstelle von nicht mehr unterstützten Baugruppen (legacy Systemen) entdeckt. Mithilfe der bekannt gewordenen Schwachstellen können die genannten Netzwerkkomponenten vollständig übernommen werden und es kann Einfluss auf den Netzwerkverkehr genommen werden wie auch die Ausbreitung in Netz-werken ermöglicht werden. Für alle betroffenen, noch von den Herstellern unterstützten IT-Systeme wurde von Aruba und Avaya Updates bereitgestellt. Die Geräte sind weltweit in Unternehmen und Behörden im Einsatz, eine Ausnutzung der Schwachstellen ist jedoch nicht bekannt geworden. /ARM22r01, ARM22r02/

Schwachstellen in Softwarebibliotheken sind in den letzten Jahren vermehrt festgestellt worden, wobei die TLStorm Schwachstellen der nanoSSL Bibliothek insbesondere wegen der hohen Verbreitung von nanoSSL auf Interesse stießen. TLStorm basiert jedoch nicht auf direkten Schwachstellen der Softwarebibliothek, sondern ausschließlich auf einer nicht vollständig korrekten Implementierung, wodurch Schwachstellen entstehen. Im Gegensatz zu Log4Shell sind daher nur eine geringe Anzahl von Herstellern betroffen. /ARM22r01/, /ARM22r02/

[10] TLS steht für Transport Layer Security und ist der Nachfolger von SSL, dem Secure Sockets Layer. TLS ist ein Verschlüsselungsprotokoll für Datenübertragungen und dient der sicheren Kommunikation in Netzwerken wie auch dem Internet.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.7 SATAn

Übersicht

Im Juli 2022 veröffentlichten Forscher der Ben-Gurion-Universität in Israel ein Konzeptpapier, in dem eine Methode vorgestellt wird, mit der es möglich ist, Informationen aus einem mit Hilfe eines AirGaps gesicherten IT-Systems durch die Verwendung von Radiosignalen über SATA-Kabel zu extrahieren. Bei Serial ATA (SATA) handelt es sich um eine Schnittstelle für den Datenaustausch mit Festplatten und anderen Speichergeräten, die weit verbreitet ist. Die Forschergruppe hat neben der in dem Konzeptpapier vorgestellten Methode in der Vergangenheit weitere Veröffentlichungen publiziert, die sich mit der Überwindung von AirGaps durch verschiedene Methoden (USB-Kabel, Monitor-Kabel oder Ethernet-Kabel als Antennen, Geräusche von Festplatten, Temperaturschwankungen eines PC-Systems usw.) befassen. Der Schwerpunkt der Forschungsarbeiten liegt dabei nicht auf der Überwindung von AirGaps zur Erlangung des Zugriffs oder Platzierung von Schadsoftware, sondern auf der Extraktion von Daten über AirGaps. /HEI22w14/, /HEI21w13/

Beschreibung

Die Forscher zeigen in dem veröffentlichten Konzeptpapier, wie ein SATA-Kabel als Funkantenne missbraucht werden kann, um Informationen zu übertragen. Dazu wurde auf einem präpariertem System eine entsprechende Schadsoftware installiert, sodass das SATA-Kabel, während Lese- und Schreiboperationen Daten im Bereich von 5.9995 und 5.996 GHz übertragen hat und somit als Antenne zweckentfremdet wurde. Es wurde eine Datenübertragungsrate von 1 Bit/s erreicht, wobei die erzielte Sendeleistung so gering war, dass sich der Empfänger in einem Abstand von maximal 1,2 m befinden musste. Auch wenn sich die Reichweite eines derartigen Angriffs vermutlich durch Verbesserungen der Empfangstechnik erhöhen lässt, schätzt das BSI die praktische Anwendbarkeit des Angriffs als gering ein, da dazu zunächst eine entsprechende Software auf das über ein AirGap abgeschottete System platziert werden muss.

Zudem werden in Anbetracht der Tatsache, dass kompromittierende Abstrahlungen von Computersystemen seit längerem bekannt sind, durch das BSI entsprechende Vorgaben für d kritische Computersystemen erstellt. Dennoch zeigt unter anderem diese Veröffentlichung, dass es Möglichkeiten zur Überwindung von AirGaps gibt und dass es Forschungsarbeiten und auch erste erfolgreiche praktische Demonstrationen diesbezüglich gibt. /BSI22r15/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS besteht derzeit keine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen, diese kann zukünftig jedoch nicht ausgeschlossen werden.

A.6.8 Schwachstellen in GPS-Trackern

Übersicht

Im Juli 2022 veröffentlichte das BSI einen Tageslagebericht mit Informationen zu sechs teilweise kritischen Schwachstellen in GPS-Trackern der Firma MiCODUS /BSI22r12/. Zuvor wurde bereits ein ICS-Advisory zu dieser Thematik veröffentlicht /CIS22i01/, welches sich auf einen Untersuchungsbericht der IT-Sicherheitsfirma BitSight /BIT22r01/ bezieht, von welcher die Schwachstellen entdeckt worden sind.

Beschreibung

Im Rahmen der Untersuchungen fand BitSight sechs teilweise kritische Schwachstellen im GPS-Tracker mit der Typenbezeichnung MV720 des chinesischen Herstellers MiCODUS. Dieser GPS-Tracker wird festverdrahtet in Fahrzeugen eingebaut und hat neben einer Ortungsfunktion die Fähigkeit zur Fernsteuerung, zum Geofencing oder zum Aktivieren einer Kraftstoffsperre. Hauptsächlich wird der GPS-Tracker als Fahrzeugortungsgerät für Flottenmanagement und Diebstahlschutz eingesetzt. Der GPS-Tracker kann über ein Webinterface oder eine Handy-App gesteuert werden. Die Kommunikation mit dem GPS-Tracker erfolgt über einen dedizierten TCP-Port (7700) oder via SMS.

Die verfügbaren Dienste für den GPS-Tracker werden von einem einzigen Webserver gehostet, wobei die Kommunikation zwischen dem Browser und diesem Webserver verschlüsselt erfolgt, alle anderen Verbindungen wie z. B. für die Handy-App aber im Klartext erfolgen. /BSI22r12/, /BIT22r01/

In dem von BitSight veröffentlichten Forschungsbericht /BIT22r01/ werden folgende Schwachstellen genannt:

- Verwendung eines hartkodierten Masterpasswortes (kritische Schwachstelle): Es wird ein hartkodiertes Masterpasswort für die Kommunikation zwischen der Handy-App und dem Webserver verwendet, welches es einem Angreifer ermöglicht, sich auf dem Webserver anzumelden und sich als Benutzer auszugeben. Somit könnte ein Angreifer direkte SMS-Befehle an den GPS-Tracker senden, die so aussehen, als kämen sie von der Handynummer des legitimen Besitzers. Unter Ausnutzung dieser Schwachstelle hätte ein Angreifer die Möglichkeit, vollständige Kontrolle über den GPS-Tracker zu erlangen, inklusive Zugriff auf Standortinformationen, Routen, Tracking-Standorte sowie z. B. die Möglichkeit des Aktivierens der Kraftstoffsperre.

- Möglichkeit, SMS-basierte Befehle ohne Authentifizierung zu senden (kritische Schwachstelle): Es besteht die Möglichkeit des Servers, SMS-Befehle direkt an den GPS-Tracker zu senden. Damit sieht es so aus, als ob diese Nachricht direkt vom mobilen Gerät des Administrators kommt. Befehle können dabei zum Teil ohne Eingabe eines Passwortes gesendet werden, wodurch beispielsweise die IP-Adresse des Administrator-Webservers geändert werden kann. Unter Ausnutzung dieser Schwachstelle könnten Angreifer beispielsweise die volle Kontrolle über den Datenverkehr erlangen.

- Alle Geräte sind mit einem Standardpasswort „123456“ vorkonfiguriert (hoch eingestufte Schwachstelle). Während der Installation erfolgt keine verbindliche Forderung, dass dieses Passwort geändert werden muss. Bei den Untersuchungen hat BitSight festgestellt, dass viele Nutzer ihr Passwort nicht geändert haben, da Sie im Installationsprozess nicht dazu gezwungen werden. Unter Ausnutzung dieser Schwachstelle könnten Angreifer einfach auf GPS-Tracker zugreifen.

- Cross-Site-Scripting-(XSS)-Schwachstelle des Webservers (hoch eingestufte Schwachstelle): Aufgrund dieser XSS-Schwachstelle werden Daten in unsicherer Weise in die Antwort auf eine Anfrage eingefügt. Bei einer Kontrolle des Skriptes

durch einen Angreifer kann dies dazu führen, dass der GPS-Tracker kompromittiert werden kann. Unter Ausnutzung dieser Schwachstelle könnten Angreifer die voll-ständige Kontrolle über den GPS-Tracker und die verschickten Informationen erlangen.

- Insecure Direct Object Reference (IDOR) Schwachstelle des Webservers (hoch ein-gestufte Schwachstelle): Der Webserver hat eine authentifizierte IDOR-Schwachstelle im Parameter „Device ID“. Es handelt sich um eine Schwach-stelle in der Zugriffskontrolle, die auftritt, wenn eine Anwendung vom Benutzer be-reitgestellte Eingaben verwendet, um direkt auf Objekte zuzugreifen. Aufgrund dieser Schwach-stelle werden beliebige Geräte-IDs ohne weitere Überprüfung akzeptiert. Unter Ausnutzung dieser Schwachstelle könnten Angreifer auf Daten von jeder Ge-räte-ID in der Server-Datenbank zugreifen, unabhängig vom angemeldeten Nutzer.
- IDOR-Schwachstelle für POST-Parameter (mittel eingestufte Schwachstelle): Für den Parameter „Device ID“ ist es möglich, dass nicht authentifizierte Nutzer Excel-Berichte über die Geräteaktivität erstellen. Aus diesen geht beispielsweise her-vor, wo und wie lange ein Fahrzeug angehalten hat.

Laut /BSI22r12, BIT22r01, CIS22i01/ könnten Angreifer durch ein erfolgreiches Ausnut-zen dieser Schwachstellen die Kontrolle über jeden MV720 GPS-Tracker erlangen und damit beispielsweise Zugriff auf Standorte und Routen sowie die Möglichkeit zum Ab-sperren des Kraftstoffs und dem Entschärfen von Alarmen erhalten. Potenziell kann ein Ausnutzen dieser Schwachstellen katastrophale, mitunter lebensbedrohliche Folgen ha-ben. Beispielsweise könnte einer kompletten Flotte der Kraftstoff entzogen oder die Fahrzeuge überwacht und abrupt gestoppt werden. Außerdem besteht die Möglichkeit einer Forderung nach Lösegeld für die Wiederherstellung der Betriebsbereitschaft.

Laut /BIT22r01/ werden die betroffenen GPS-Tracker in 169 Ländern neben Privatper-sonen auch von diversen Organisationen genutzt. Insgesamt sind ca. 1,5 Millionen Ge-räte bei ca. 420.000 Kunden installiert, u. a. in Fortune-50-Energieunternehmen, beim nationalen Militär in Südamerika, nationalen Regierungen und Strafverfolgungsbehörden in Westeuropa sowie einem ausländischen Kernkraftwerksbetreiber. Die Auswertung der ca. 2 Millionen hergestellten Verbindungen zwischen dem Webserver und den GPS-Trackern für den Zeitraum Mai 2021 bis Februar 2022 hat ergeben, dass die meis-ten Verbindungen in den GUS-Staaten hergestellt wurden. In Deutschland wurden we-niger als 5.000 dieser Verbindungen hergestellt. Deshalb kommt /BSI22r12/ zu dem

Schluss, dass die Schwachstellen zwar grundsätzlich als kritisch einzuordnen sind, dass sie aber keine besondere Relevanz in Deutschland haben.

Es ist allerdings aus den Unterlagen nicht zu entnehmen, welche Organisationen konkret betroffen sind. Laut /CIS22i01/ wird empfohlen, die Verwendung der betroffenen GPS-Tracker zu deaktivieren, bis eine Behebung der Schwachstellen erfolgt ist. Ob und wann diese erfolgt, ist momentan nicht absehbar, da der Hersteller trotz mehrfacher Kontaktversuche nicht in ausreichendem Maße reagiert hat. Laut /BIT22r01/ ist es zudem wahrscheinlich, dass auch andere GPS-Tracker des Herstellers MiCODUS von den Schwachstellen betroffen sind.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Es besteht die Möglichkeit, dass GPS-Tracker beispielsweise in Fahrzeugen zum Transport von kerntechnischem Material eingesetzt werden können und diese damit gezielt angegriffen werden können.

A.6.9 Schwachstellen in Videoüberwachungssystemen und Network Attached Storage von QNAP

Übersicht

Im Jahr 2022 wurden vier Schwachstellen bekannt, die die Videoüberwachungssysteme und NAS (Network Attached Storage[11]) der Firma QNAP betreffen und von QNAP als kritisch eingestuft wurden. Sie ermöglichen einem Angreifer die Ausführung von beliebigem Programmcode sowie die Durchführung von DoD-Angriffen und können zu Vertraulichkeits- und Integritätsverlust führen.

[11] NAS (Network-Attached Storage) Systeme sind IT-Systeme, welche eine hohe Festplattenkapazität an ein Netzwerk anschließen, um so einen von verschiedenen IT-Systemen zugreifbaren Speicherort zu bieten. NAS-Systeme können rein in lokalen Netzwerken betrieben werden, aber je nach Einsatzgebiet auch über das Internet angesteuert werden. Zugriffe auf NAS-Systeme erfolgen entweder über direkten Netzwerkzugriff auf die Speicher der Systeme oder aber über HTML-Anwendungen.

Beschreibung

QNAP (Quality Network Appliance Provider) ist ein Unternehmen mit Hauptsitz in Taipeh, welches Hardware- und Softwarelösungen im Bereich Speicher, Netzwerke und Smart Videoüberwachung anbietet.

Zudem stellt QNAP für seine Nutzer eine Cloud basierte NAS Lösung zur Verfügung. Im Jahr 2022 wurden vier von QNAP als kritisch ein-gestufte Schwachstellen bekannt, die die Videoüberwachungssysteme und NAS von QNAP betreffen. Sie werden nachfolgend aufgelistet. /QNA22w01, HEI22w15/

Eine kritische Schwachstelle betrifft Netzwerk Videorecorder, die QVR Videoüberwachungssysteme verwenden /QNA22w01, QNA22i01, NIS22i01/:

- **CVE-2022-27588**: Die Schwachstelle ermöglicht einem Angreifer per Fernzugriff beliebige Befehle auszuführen. Sie besitzt einen Base Score CVSS v3.1 von 9.8. Durch ein Update des Systems auf die Firmwareversion QVR 5.1.6 build 20220401 oder höher, wird die Schwachstelle geschlossen.

Drei weitere kritische Schwachstellen betreffen das Netzwerkprotokoll Samba (SMB), das den Zugriff auf Daten über ein Computernetzwerk ermöglicht und Datei- und Druck-dienste für Windows-Clients bereitstellt /QNA22w01, QNA22i02, NIS22i02, SUS22i01/:

- **CVE-2021-44141**: Von dieser Schwachstelle sind alle Samba-Versionen vor 4.15.5 betroffen. Ein böswilliger Nutzer kann einen Server-Symlink[12] verwenden, um fest-zustellen ob eine Datei oder ein Verzeichnis in einem Bereich des Server-Dateisystems vorliegt, der nicht unter der Freigabefunktion exportiert wurde und so ein Informationsleck herbeiführen. Dafür muss SMB1 mit Unix-Erweiterungen aktiviert sein. Base Score CVSS v3.1: 4.3.
- **CVE-2021-44142**: Betroffen sind die Samba-Versionen vor 4.13.17, 4.14.12 und 4.15.5 mit konfiguriertem vfs_fruit. Ein Angreifer mit Schreibzugriff auf erweitere Dateiattribute kann aus der Ferne beliebigen Programmcode ausführen. Base Score CVSS v3.1: 8.8.

[12] Ein Symlink ist ein symbolischer Link. Es handelt sich um eine Verknüpfungsdatei, die sich auf eine physische Datei oder einen physischen Ordner bezieht. /JOE22w01/

- **CVE-2022-0336**: Samba AD DC überprüft beim Hinzufügen von Service Principal Names (SPNs) zu einem Benutzerkonto, dass diese nicht mit den SPNs über-ein-stimmen, die bereits in der Datenbank existieren. Diese Überprüfung kann umgangen werden, wenn durch eine Kontoänderung ein SPN erneut hinzugefügt wird, der zuvor bereits auf diesem Konto vorhanden war. Ein Angreifer kann dies für einen DoD-Angriff ausnutzen, indem er einen SPN hinzufügt, der einem vorhandenen Dienst entspricht. Darüber hinaus kann ein Angreifer sich als bestehender Dienst ausgeben, was zu einem Vertraulichkeits- und Integritätsverlust führt. Base Score CVSS v3.1: 8.8.

Um NAS bezüglich der drei Schwachstellen abzusichern, empfiehlt QNAP die Deaktivierung von SMB1 und ein Update der Firmware des Systems auf die aktuelle Version /QNA22i02/.

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.10 TLStorm-Schwachstellen in UPS-Notstromgeräten von APC betreffen kritische Infrastrukturen

Übersicht

Cyberangriffe können auf Geräte für die unterbrechungsfreie Stromversorgung (Uninterruptible Power Supply UPS) abzielen, welche mit dem Internet verbunden sind. Ermöglicht wird dies durch die Ausnutzung von Schwachstellen, darunter drei Schwachstellen in smarten UPS-Geräten des Herstellers APC, die als TLStorm bezeichnet werden. APC ist ein Tochterunternehmen von Schneider Electric. UPS-Geräte werden auch in kritischen Infrastrukturen eingesetzt.

Beschreibung

Die US Cybersecurity & Infrastructure Security Agency (CISA) und das US Department of Energy haben festgestellt, dass sich IT-Angreifer Zugriff auf eine Vielzahl von UPS-Geräte verschaffen können, die zwecks Energieüberwachung und routinemäßiger Wartung mit dem Internet verbunden sind. UPS steht für Uninterruptible Power Supply. Die

Geräte stellen also die unterbrechungsfreie Stromversorgung von elektrischen Verbrauchern sicher, falls die reguläre Stromversorgung nicht mehr zur Verfügung steht. Deshalb werden sie in Rechenzentren, Krankenhäusern, Industrieanlagen und speziell in kritischen Infrastrukturen eingesetzt. Oft ermöglichen vom Hersteller vergebene Standard-Benutzernamen und -Passwörter, welche vom Anwender nicht abgeändert wurden, den unautorisierten Zugriff auf die UPS-Geräte. Armis, der Anbieter einer Plattform für Asset Visibility und IT-Sicherheit, hat im März 2022 drei Sicherheitslücken CVE-2022-22805, CVE-2022-22806 und CVE-2022-0715 mit Namen TLStorm entdeckt, über die sich Angreifer Fernzugriff auf smarte UPS-Geräte von APC verschaffen können /ARM22w01/. APC ist ein Tochterunternehmen von Schneider Electric. Armis untersucht die Sicherheit verschiedenartiger Geräte mit dem Ziel Sicherheitsmanager dabei zu unterstützen ihre Unternehmen vor Bedrohungen zu schützen. Da viele Kunden von Armis smarte UPS-Geräte von APC verwenden, analysierte das Sicherheitsunternehmen deren Fernverwaltungs- und Überwachungsdienste und stieß dabei auf die drei Schwachstellen. Angreifer können die TLStrom-Schwachstellen ausnutzen, um die von ihnen betroffenen UPS-Geräte ohne Benutzerinteraktion über das Internet fernzusteuern. Die UPS-Geräte und die an diesen angeschlossenen Verbraucher können von Angreifern deaktiviert, beeinträchtigt oder zerstört werden. /CIS22i05, ITA22w01/

Die TLStorm-Sicherheitslücken CVE-2022-22805 und CVE-2022-22806 betreffen die TLS[13]-Verbindung zwischen der Schneider Electric Cloud und den UPS-Geräten. Diese Verbindung wird von Geräten, die die SmartConnect-Funktion unterstützen, beim Start oder nach vorübergehender Unterbrechung der Verbindung automatisch aufgebaut. Angreifer können die Schwachstellen ausnutzen, um unauthentifizierte Netzwerkpakete an die Geräte zu senden. Die dritte TLStorm-Schwachstelle CVE-2022-0715 beruht auf einem Designfehler im Programmcode, durch den Firmware-Updates nicht auf sichere Art kryptografisch signiert werden. IT-Angreifer könnten die Schwachstelle ausnutzen, um eine eigens erstellte, bösartige Firmware über das Internet, eine LAN-Verbindung oder über einen USB-Stick auf den Geräten zu installieren. Dadurch hätten Angreifer die Möglichkeit sich dauerhaft auf den UPS-Geräten einzunisten und von diesen ausgehend weitere Cyberangriffe auf das Netzwerk durchzuführen, auch um Daten zu stehlen /THP22w01/. Die drei TLStorm-Schwachstellen werden nachfolgend im Einzelnen beschrieben: /ITA22w01, NVD22i01, SCE22i01/

[13] TLS steht für Transport Layer Security. Dabei handelt es sich um ein weit verbreitetes Sicherheitsprotokoll zur Vereinfachung der Datensicherheit bei Kommunikationen über das Internet. /THP22w02/

- **CVE-2022-22805:** Die Schwachstelle betrifft das Kopieren von Speicherpuffern ohne Überprüfung der Größe der Eingabe (klassischer Pufferüberlauf). Wird ein falsch verarbeitetes TLS-Paket wieder zusammengesetzt, dann kann ein Angreifer aus der Ferne schadhaften Programmcode ausführen. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.0.

- **CVE-2022-22806:** Es besteht eine Sicherheitslücke, bei der die Authentifizierung durch Capture-Replay[14] umgangen werden kann. Angreifern ist es auf diese Weise möglich über den Aufbau einer fehlerhaften Verbindung unauthentizierten Zugriff auf das UPS-Gerät zu erhalten. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.0.

- **CVE-2022-0715:** Die Schwachstelle besteht aufgrund einer unsachgemäßen Authentifizierung. Ist ein Angreifer in den Besitz eines Schlüssels gelangt, so kann er diesen unter Ausnutzung der Schwachstelle dazu verwenden eine schadhafte Firmware auf dem UPS-Gerät zu installieren und dessen Verhalten beliebig zu ändern. Bedrohungsgrad: hoch für verbundene Geräte und mittel für nicht verbundene Geräte. CVSS:3.1-Score: 8.9 für verbundene Geräte und 6.9 für nicht verbundene Geräte.

Um den Versuch der Ausnutzung der Schwachstellen zu erkennen, ist das Verhalten der UPS-Geräte zu überwachen. Schneider Electric hat in Zusammenarbeit mit Armis seine Kunden über die Schwachstellen informiert und stellt entsprechende Patches bereit, um die Sicherheitslücken zu schließen. Beide Unternehmen geben an, dass es derzeit keine Hinweise darauf gibt, dass die TLStorm-Schwachstellen bei einem Cyberangriff ausgenutzt wurden. Schneider Electric hat ein entsprechendes Advisory veröffentlicht /SCE22i01/. Darin empfiehlt das Unternehmen seinen Kunden die Firmwareupdates für die von den TLStorm-Schwachstellen betroffenen UPS-Geräte schnellstmöglich zu installieren, um die Schwachstellen zu schließen. Systeme und per Fernzugriff erreichbare Geräte müssen durch Firewalls geschützt werden. Der physische Zugriff auf Geräte ist auf das autorisierte Bedienpersonal zu beschränken, z. B. durch die Einrichtung von Zugriffskontrollen. Kritische Systeme und Geräte dürfen nur über das Intranetz der Anlage erreichbar sein. Zusätzlich rät die CISA vom Hersteller vergebene Standard-Benutzernamen und -Passwörter in sichere Benutzernamen und Passwörter umzuändern. Falls

[14] Ein Capture-Replay-Werkzeug ermöglicht es manuelle Interaktionen aufzuzeichnen, um diese Interaktionen danach automatisiert und wiederholt durchführen zu können. /TIN23w01/

möglich ist eine Multifaktorauthentifizierung einzurichten und der Zugriff auf die UPS-Geräte ist zeitlich zu beschränken. /CIS22i05, ITA22w01, SCE22i01, THP22w01/

Kerntechnischer Bezug

UPS-Geräte werden auch in kerntechnischen Anlagen verwendet, weshalb diese durch Schwachstellen in den Geräten potenziell gefährdet sind. Zudem kommen Geräte von Schneider Electric in deutschen kerntechnischen Anlagen zum Einsatz. Der GRS ist allerdings nicht bekannt, ob sich darunter auch die von den TLStorm-Schwachstellen betroffenen UPS-Geräte von APC befinden. Ist dies der Fall, dann sollten die beiden TLStorm-Schwachstellen CVE-2022-22805 und CVE-2022-22806 keine Auswirkung haben, da die in der Leittechnik deutscher, kerntechnischer Anlagen eingesetzten UPS-Geräte ausschließlich mit dem internen Netzwerk der Anlage und nicht mit dem Internet verbunden sind. Eine Ausnutzung der dritten TLStorm-Schwachstelle CVE-2022-0715 benötigt jedoch keine Internetverbindung. Sie kann durch einen Innentäter unter Verwendung einer LAN-Verbindung oder eines USB-Sticks erfolgen.

A.6.11 Schwerwiegende Sicherheitslücken in einem Software Development Kit (SDK)

Übersicht

Im August 2023 wurden Informationen zu mehreren kritischen Schwachstellen in der integrierten Entwicklungsumgebung Codesys für speicherprogrammierbare Steuerungen bekannt. Am 10. August 2023 veröffentlichte Microsoft Informationen zu insgesamt 15 kritischen Schwachstellen, wobei die Entwickler von Codesys bereits im September 2022 von Microsoft informiert wurden /MIC23w01/. Durch die Ausnutzung der Schwachstellen sind potenzielle Angreifer in der Lage, Denial-of-Service-Zustände herbeizuführen oder Programmcode über Remote-Verbindungen auszuführen. Am 24. August 2023 veröffentlichte zudem die CISA eine Warnmeldung bezüglich einer weiteren kritischen Schwachstelle, die es potenziellen Angreifern ermöglicht, durch einen Man-in-the-Middle-Angriff beliebigen Code auszuführen /CIS23r01/. Die Kritikalität der Schwachstellen ergibt sich unter anderem aus der weiten Verbreitung der weltweit eingesetzten, plattform-unabhängigen Entwicklungsumgebung, die von hunderten Geräteherstellern wie beispielsweise ABB und Schneider Electric in unterschiedlichen Industriebereichen (unter anderem Fertigung, Energie-Automation und

Prozessautomatisierung) als Programmierschnittstelle im OT-Bereich für Automatisierungskomponenten implementiert ist.

Beschreibung

Das Unternehmen CODESYS Group ist der Hersteller der hardwareunabhängigen Automatisierungssoftware CODESYS, welche die europäische Industrienorm IEC 61131-3 umsetzt und zur Projektierung sowie zur Entwicklung von Steuerungsanwendungen eingesetzt wird /COD23w01/. 15 Schwachstellen mit dem Bedrohungsgrad „hoch“ in einem Software Development Kit (SDK) des Herstellers mit der Bezeichnung CODESYS V3 SDK 15 ermöglichen Cyberangriffe auf kritische Infrastrukturen /GOL23w01/. Das SDK wird in Industrieanlagen eingesetzt, darunter Anlagen zur Energieerzeugung, Automatisierung von Herstellungsprozessen, Energieautomatisierung und Prozessautomatisierung /ARS23w01/. Mit dem SDK werden Programmable Logic Controllers (PLCs), auch speicherprogrammierbare Steuerungen (SPS) genannt, erstellt, die vor allem in Europa in kritischen Infrastrukturen Anwendung finden. Auch kritische Infrastrukturen in Deutschland sind betroffen. Die Unternehmen ABB, Schneider Electric und WAGO nutzen das SDK für die Entwicklung von PLCs in Industrieanlagen, darunter der Modicon TM251 von Schneider Electric und der PFC200 von WAGO /ARS23w01/. Sicherheitsforscher von Microsoft haben die Schwachstellen im September 2022 entdeckt. /HEI23w04/

Angreifer können die Schwachstellen ausnutzen, um DoS-Angriffe und schadhaften Programmcode auszuführen. Dies ermöglicht es ihnen im Extremfall Kraftwerke zum Stillstand zu bringen, eine dauerhafte Backdoor einzurichten und Informationen zu stehlen. Von den Schwachstellen sind mehrere Komponenten der Software CODESYS wie CmpApp betroffen. Über die Bibliothek CmpApp können Informationen über Projekte, Anwendungen, Adressen und Größen von Datentypen ermittelt sowie Variablen gespeichert und ausgelesen werden. Zudem ermöglicht sie das Starten, Stoppen und Zurücksetzen einer Anwendung aus einer anderen Anwendung heraus. Werden Tags mit Anweisungen an den PLC übergeben, dann wird deren Datengröße nicht überprüft, wodurch Speicherfehler ausgelöst werden können. Um die Schwachstellen ausnutzen zu können, muss der Angreifer über eine Authentifizierung und weitgehende Kenntnisse des proprietären Protokolls von CODESYS V3 verfügen. Nach den Sicherheitsforschern von Microsoft stellt die Authentifizierung aber kein großes Hindernis dar, da Angreifer über eine ältere, bereits 2019 entdeckte und geschlossene, Schwachstelle CVE-2019-9013 /COD21i01/ Zugriff auf Zugangsdaten erhalten können. Am 24. August 2023

veröffentlichte zudem die CISA eine Warnmeldung bezüglich einer weiteren kritischen Schwachstelle (CVE-2023-3663), die es potenziellen Angreifern ermöglicht, durch einen Man-in-the-Middle-Angriff beliebigen Code auszuführen /CIS23r01, COD23w02, HEI23w04, MIC23i01/.

Nachstehend wird die Schwachstelle CVE-2019-9013 näher beschrieben. Von ihr betroffen sind alle CODESYS V3-Produkte mit älteren Softwareversionen als der Version V3.5.16.0 /COD21i01, NVD19i01/:

- **CVE-2019-9013:** Ohne die Verwendung der TLS-basierten verschlüsselten CODESYS-Onlinekommunikation sind die Benutzerdaten beim Datentransport nicht ausreichend geschützt und können von einem Angreifer abgerufen werden. Um die Schwachstelle ausnutzen zu können, benötigt ein Angreifer Zugriff auf den Online-Kommunikationsverkehr oder lokalen Zugriff auf den PLC, er muss jedoch nicht über weitreichende Fähigkeiten verfügen. Bedrohungsgrad: hoch. CVSS:3.0-Score: 8.8.

Die zuletzt entdeckten 15 Schwachstellen werden im Folgenden beschrieben. Sie können von einem Angreifer ohne weitreichende Fähigkeiten aus der Ferne ausgenutzt werden. Von den Schwachstellen sind alle CODESYS V3-Produkte mit älteren Softwareversionen als der Version V3.5.19.0 betroffen /COD23i01, NVD23i03/:

- **CVE-2022-47379:** Schreiben außerhalb der Speichergrenzen: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen dazu führen, dass die CmpApp-Komponente vom Angreifer gesendete Daten in den Speicher schreibt, was zu einem Denial-of-Service-Zustand, Speicherüberschreibung oder Remotecodeausführung führen kann. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.8.

- **CVE-2022-47380 und CVE-2022-47381:** Stack-basierter Pufferüberlauf: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen dazu führen, dass die CmpApp-Komponente vom Angreifer gesendete Daten in den Stack schreibt, was zu einem Denial-of-Service-Zustand, Speicherüberschreibung oder Remotecodeausführung führen kann. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.8.

- **CVE-2022-47382 bis CVE-2022-47384 und CVE-2022-47386 bis CVE-2022-47390:** Stack-basierter Pufferüberlauf: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen dazu führen, dass die CmpTraceMgr-Komponente vom Angreifer gesendete Daten in den Stack schreibt,

was zu einem Denial-of-Service-Zustand, Speicherüberschreibung oder Remotecodeausführung führen kann. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.8.

- **CVE-2022-47385:** Stack-basierter Pufferüberlauf: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen dazu führen, dass die CmpAppForce-Komponente vom Angreifer gesendete Daten in den Stack schreibt, was zu einem Denial-of-Service-Zustand, Speicherüberschreibung oder Remotecodeausführung führen kann. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.8.

- **CVE-2022-47391:** Ein unbefugter Angreifer kann aus der Ferne eine fehlerhafte Eingabevalidierung ausnutzen, um ungültige Adressen auszulesen, was zu einem Denial-of-Service-Zustand führt. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.5.

- **CVE-2022-47392:** Unsachgemäße Überprüfung der Konsistenz innerhalb der Eingabe: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen mit inkonsistentem Inhalt dazu führen, dass die CmpApp-,CmpAppBP- und CmpAppForce-Komponenten intern von einer ungültigen Adresse lesen, was möglicherweise zu einem Denial-of-Service-Zustand führt. Bedrohungsgrad: mittel. CVSS:3.1-Score: 6.5.

- **CVE-2022-47393:** Nicht vertrauenswürdige Pointer-Dereferenzierung: Nach erfolgreicher Authentifizierung können auf eine bestimmte Art gestaltete Kommunikationsanfragen dazu führen, dass die CmpFiletransfer-Komponente von der Anfrage für den internen Lesezugriff bereitgestellte Adressen dereferenziert, was zu einem Denial-of-Service-Zustand führen kann. Bedrohungsgrad: mittel. CVSS:3.1-Score: 6.5.

Die von der CISA entdeckte, zusätzliche Schwachstelle wird nachstehend beschrieben /CIS23r01, NVD23i07/:

- **CVE-2023-3663:** Dies Schwachstelle betrifft die CODESYS-Versionen 3.5.11.0 bis 3.5.19.19 und ermöglicht es durch eine fehlende Integritätsprüfung nicht authentifizierten Angreifern den Inhalt von Nachrichten des Codesys Notification Servers zu manipulieren. Dadurch ergeben sich potenziellen Angreifern Möglichkeiten für einen Man-in-the-Middle-Angriff und die Ausführung beliebigen Codes. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.8.

Sicherheitsforscher von Microsoft haben die 15 Schwachstellen bei der Untersuchung der Sicherheit des proprietären CODESYS V3-Protokolls offengelegt.

Dazu verwendeten sie die PLCs Modicon TM251 von Schneider Electric und PFC200 von WAGO. Hintergrund der Analysen war das Ziel die Sicherheitsstandards und forensischen Werkzeuge für ICS-Geräte zu verbessern. Im September 2022 hat Microsoft den Hersteller des SDKs über die entdeckten Schwachstellen informiert. Seit März 2023 ist ein Sicherheitspatch in Form der gegen die Schwachstellen abgesicherten Version V3.5.19.0 des SDK verfügbar, welches von der Webseite des Herstellers heruntergeladen werden kann. Darüber hinaus hat das Unternehmen CODESYS Group ein entsprechendes Advisory /COD23i01/ mit Informationen zu den Schwachstellen veröffentlicht. Schneider Electric hat ebenfalls ein Advisory /SCH23i01/ zu den Schwachstellen verfasst. Die Sicherheitsforscher von Microsoft haben ihre Informationen zu den Schwachstellen auf eine Github-Webseite geladen. Sie stellen frei verfügbare Software-Werkzeuge zur Verfügung, mit denen PLCs auf das Vorhandensein der Schwachstellen hin untersucht werden können. Um auch die zusätzliche Schwachstelle CVE-2023-3663 zu umgehen, empfehlen Microsoft und die CISA als mitigative Maßnahme jeweils ein Update betroffener Komponenten auf neuere Softwareversionen (mindestens Version 3.5.19.20). /CIS23r01, HEI23w04, MIC23i01, MIC23w01/

Kerntechnischer Bezug

Die mit dem, von den Schwachstellen betroffenen, SDK erstellten PLCs werden vor allem in Europa in kritischen Infrastrukturen eingesetzt, unter denen sich auch der Energiesektor befindet. Die entsprechenden PLCs werden zudem in Deutschland verwendet. In den Quellen wird explizit angegeben, dass Angreifer unter Ausnutzung der Schwachstellen Kraftwerke außer Betrieb nehmen können. Damit sind von den Schwachstellen potenziell auch kerntechnische Anlagen betroffen. Der GRS liegen zurzeit allerdings keine Informationen vor, ob die von den Schwachstellen betroffenen PLCs tatsächlich in kerntechnischen Anlagen Anwendung finden. Darüber hinaus ist der GRS nicht bekannt, ob bereits Cyberangriffe unter Ausnutzung der Schwachstellen erfolgt sind.

A.6.12 Sicherheitslücken in Open Automation Software (OAS) gefährden kritische Infrastrukturen

Übersicht

Die Open Automation Software (OAS) des gleichnamigen Herstellers OAS wird von vielen industriellen Steuerungssystemen (ICS) verwendet. Über acht Schwachstellen in der Software können sich Angreifer Zugriff auf Netzwerke verschaffen und beliebigen Code ausführen.

Beschreibung

Der Forscher Jared Rittle des IT-Sicherheitsunternehmens Ciso Talos hat acht Schwachstellen in der Version 16.00.0112 der Open Automation Software (OAS) des gleichnamigen Herstellers OAS entdeckt, von denen zwei kritisch sind. Die Schwachstelle CVE-2022-26082 ist besonders schwerwiegend, da sie einem Angreifer die Ausführung von beliebigem Programmcode auf dem kompromittierten Gerät ermöglicht. Da die Softwareplattform OAS häufig in industriellen Steuersystemen ICS Anwendung findet, werden diese durch die Schwachstellen gefährdet. Die Software ist eine universelle Lösung zur Vereinfachung der Datenkonnektivität, welche den Datentransfer und die Datenumwandlung zwischen Geräten und Anwendungen, sowohl bezogen auf Software als auch auf Hardware betrifft. Sie wird in den Bereichen Maschinelles Lernen, Data Mining, Berichterstellung und Datenvisualisierung eingesetzt und häufig in ICS verwendet, um industrielle und IoT-Geräte, SCADA-Systeme (darunter OPC Modbus SCADA-Systeme), SPS, Datenbanken, Netzwerkpunkte und APIS in einem ganzheitlichen Netzwerksystem miteinander zu verbinden. Da diese Prozesse sehr empfindlich sind, stellen die Schwachstellen eine erhebliche Gefährdung für ICS dar. Unternehmen und Organisationen, die OAS verwenden, sind zum Beispiel Intel, Volvo, Dart Oil and Gas, Mack Trucks, die U.S. Navy, JBT AeroTech und Michelin. /CIT22i01, SEC22w16, THR22w03/

Nachstehend werden die acht Schwachstellen aufgelistet und im Einzelnen beschrieben /NVD22i02, SEC22w16, THR22w03/:

- **CVE-2022-26082:** Die Schwachstelle besteht beim Schreiben von Dateien in der SecureTransferFiles-Funktion der OAS Engine. Über eine speziell gestaltete Reihe von Netzwerkanforderungen, kann ein Angreifer beliebigen Programmcode auf dem Zielgerät ausführen. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8.

- **CVE-2022-26833:** Bei dieser Schwachstelle handelt es sich um einen Authentifizierungsfehler in der REST-API der OAS-Software. Sie ermöglicht es einem Angreifer eine Reihe von HTTP-Anfrage zu senden, um die API der Software ohne Authentifizierung nutzen zu können. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8.
- **CVE-2022-26026:** Es handelt sich um eine DoS-Schwachstelle in der OAS Engine SecureConfigValues-Funktionalität. Ein Angreifer kann eine speziell gestaltete Netzwerkanfrage erstellen, welche zum Verlust der Kommunikation führen kann. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.5.
- **CVE-2022-26067 und CVE-2022-27169:** Über die beiden Schwachstellen kann ein Angreifer, durch Senden einer bestimmten Netzwerkanfrage, eine Verzeichnisliste an jedem, abhängig vom Benutzer, zulässigen Ort abrufen. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.5.
- **CVE-2022-26077:** Diese Sicherheitslücke ermöglicht die Offenlegung von Informationen. Sie kann auf die gleiche Weise ausgenutzt werden und bietet die gleichen Möglichkeiten wie die Schwachstellen CVE-2022-26067 und CVE-2022-27169. Über die Schwachstelle kann ein Angreifer aber zusätzlich eine Liste mit Benutzernamen und Passwörtern abrufen. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.5.
- **CVE-2022-26043 und CVE-2022-26303:** Durch beide Schwachstellen kann ein Angreifer aus der Ferne Konfigurationsänderungen vornehmen. Er kann z. B. eine neue Sicherheitsgruppe und/oder einen neuen Benutzer anlegen. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.5.

Zusammen mit Cisco Talos arbeitete der Hersteller OAS an der Schließung der Schwachstellen. Benutzer sollten die OAS-Software so schnell wie möglich auf die Version 16.00.0113 aktualisieren, da die Schwachstellen in dieser behoben wurden. Das Update steht seit dem 22. Mai 2022 zum Download bereit. Um die Auswirkungen einer Ausnutzung der Schwachstellen zu vermindern, sollten Nutzer eine geeignete Netzwerksegmentierung umsetzen. Auf diese Weise wird der Zugriff für einen potenziellen Angreifer entsprechend eingeschränkt. /SEC22w16, THR22w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.7 2023

A.7.1 Jaguar Tooth

Übersicht

Jaguar Tooth ist eine Malware, die auf Cisco IOS Router abzielt. Sie etabliert eine Backdoor auf dem kompromittierten System, sammelt Informationen und exfiltriert diese über das Trivial File Transfer Protocol (TFTP). Verteilt und ausgeführt wird die Malware über eine SNMP-Schwachstelle. Die APT-Gruppierung, welche die Malware einsetzt, ist unter dem Namen APT28 bekannt.

Beschreibung

Am 18.04.2023 hat das UK National Cyber Security Center (NCSC) zusammen mit dem US Federal Bureau of Investigation (FBI), der US National Security Agency (NSA) und der US Cybersecurity and Infrastructure Agency (CISA) ein gemeinsames Advisory veröffentlicht /NCS23i01/. Darin wird beschrieben, dass die vom russischen Staat gesponserte APT-Gruppierung mit Namen APT28 die seit dem 29.06.2017 bekannte SNMP-Schwachstelle CVE-2017-6742 in der Cisco IOS- und der Cisco IOS XE-Software erfolgreich ausnutzt. Begonnen hat die Kampagne bereits im Jahr 2021. SNMP steht für Simple Network Management Protocol. Es handelt sich um ein Netzwerkprotokoll, das Administratoren die Überwachung und Konfiguration von Netzwerkgeräten aus der Ferne ermöglicht. Von IT-Angreifern kann SNMP allerdings missbraucht werden, um sensible Netzwerkinformationen abzugreifen und Netzwerke über verwundbare Geräte zu infiltrieren. APT28 verwendet die Schwachstelle um schwache SNMP-Community-Strings, darunter der öffentliche SNMP-Community-String, über eine IP-Adresse an Netzwerkrouter des Herstellers Cisco zu senden. SNMP-Community-Strings sind wie Anmeldeinformationen, welche es jedem, der den konfigurierten String kennt ermöglichen, SNMP-Daten von einem Gerät abzurufen. Mit schwachen SNMP-Community-Strings sind Standard- oder leicht zu erratende SNMP-Community-Strings gemeint. Auf diese Weise können die Angreifer Netzwerke ausspionieren und Router-Schnittstellen auflisten. Sie konfigurieren die kompromittierten Router derart, dass sie SNMP v2-Anfragen akzeptieren. Dabei ist zu beachten, dass SNMP v2 keine Datenverschlüsselung unterstützt. In der Folge werden alle Daten und SNMP-Community-Strings unverschlüsselt gesendet. Die Angreifer nutzen die SNMP-Community-Strings, um die

Schadsoftware Jaguar Tooth auf öffentlich zugänglichen Cisco-Routern zu verteilen, die ihnen einen unauthentifizierten Zugriff ermöglichen. Mithilfe der Schadsoftware können sie Geräteinformationen sammeln und mittels des Datentransferprotokolls Trivial File Transfer Protocol (TFTP)[15] exfiltrieren. Diese Informationen dienen den Angreifern zu Spionagezwecken oder für die Planung zukünftiger Cyberangriffe /CIS23i02/. Die Ziele der Kampagne von APT28 sind auf der ganzen Welt verteilt, erstrecken sich aber hauptsächlich auf Europa, Regierungsinstitutionen in den USA und auf etwa 250 ukrainische Ziele. /BLC23w01, CIS23w01, NCS23i01/

Die APT-Gruppierung APT28 gehört zu Russlands militärischem Geheimdienst und ist Teil des Hauptnachrichtendienstes des russischen Generalstabes (GRU), 85. Haupt-Sonderdienstleistungszentrum (GTsSS), militärische Einheit 26165 /BAN21w01, REC21w02/. Zu ihren Haupt-Angriffszielen gehören politische und militärische Einrichtungen in Europa, speziell in osteuropäischen Staaten wie Georgien. Seit16 ist APT28 auch an US-amerikanischen Einrichtungen und an Unternehmen im Energiesektor interessiert. APT28 ist auch unter den Namen Fancy Bear, Strontium, Pawn Storm, the Sednit Gang und Sofacy bekannt /NCS23i01/. /FIR14r01, ITE20w01, TAG16w01/

Im Folgenden wird die von APT28 ausgenutzte Schwachstelle CVE-2017-6742 beschrieben /NIS17i01/:

- **CVE-2017-6742:** Die Schwachstelle betrifft das Simple Network Management Protocol (SNMP)-Subsystem von Cisco IOS 12.0 bis 12.4 und 15.0 bis 15.6 sowie IOS XE 2.2 bis 3.17. Sie ermöglicht es einem authentifizierten Angreifer aus der Ferne manipulierte SNMP-Pakete an ein von der Schwachstelle betroffenes System zu senden. Die Schwachstelle ist auf einen Pufferüberlauf im SNMP-Subsystem der Software zurückzuführen und betrifft alle Versionen von SNMP. Um die Schwachstelle über SNMP Version 2c oder früher ausnutzen zu können, muss der Angreifer den SNMP-Readonly-Community-String für das betroffene System kennen. Für eine Ausnutzung der Schwachstelle über SNMP Version 3 muss der Angreifer über Benutzeranmeldeinformationen für das betroffene System verfügen. Bedrohungsgrad: hoch. CVSS:3.0-Score: 8.8

[15] Beim Trivial File Transfer Protocol (TFTP) handelt es sich um ein paketorientiertes Protokoll zur Übertragung von Dateien zwischen Computern welches verwendet wird, wenn keine Verschlüsselung, Benutzerauthentifizierung und Verzeichniseinsicht benötigt werden. Daher wird es hauptsächlich in lokalen Netzwerken eingesetzt. /COW23w01/

Jaguar Tooth ist eine Schadsoftware, die auf Cisco IOS-Router mit der Firmware C5350-ISM, Version 12.3(6) abzielt. Haben Angreifer Zugriff auf einen Router erhalten, so wird dessen Speicher dazu gebracht, die Schadsoftware zu installieren. Dadurch wird eine Backdoor auf dem kompromittierten Gerät eingerichtet, indem zwei Authentifizierungsfunktionen gepatcht werden, um so ohne Passwortüberprüfung Zugriff auf lokale Konten für Telnet und physische Sitzungen zu erhalten. Darüber hinaus patcht Jaguar Tooth das Cisco IOS-Image im Speicher des Routers, um die Benutzer-Authentifizierung zu umgehen. Auf diese Weise ermöglicht die Schadsoftware den Angreifern ohne jegliche Passwortüberprüfung den Zugriff auf lokale Accounts. Zusätzlich startet Jaguar Tooth einen neuen Prozess mit Namen Service Policy Lock. Dieser arbeitet eine hart codierte Liste ab, in der sich Cisco IOS- und Tcl-Befehle befinden, welche automatisch ausgeführt werden und Geräteinformationen des Netzwerks abfragen.

Die Netzwerkinformationen werden gesammelt und unter Verwendung des Datentransferprotokolls TFTP exfiltriert. Die Informationen umfassen Konfigurationsdaten, die Firmwareversion, die Verzeichnisliste des Speichers, Router-Tabellen, Interfaces und verbundene Router. /BLC23w01, NCS23r01/

Um die Ausnutzung der Schwachstelle CVE-2017-6742 zu verhindern, sollten Nutzer ihre Cisco-Router auf die letzte Firmwareversion aktualisieren. Der Hersteller rät seinen Kunden auf öffentlich zugänglichen Routern von SNMP zu NETCONF[16] oder RESTCONF[17] zu wechseln, da diese eine höhere Sicherheit und eine robustere Funktionalität bieten. Wird SNMP dennoch benötigt, sollten Administratoren Listen vertrauenswürdiger und nicht erlaubter Administratoren und IP-Adressen erstellen, um den Netzwerkzugriff auf das SNMP-Interface auf öffentlich zugänglichen Routern zu beschränken. Zusätzlich sollte der schwache Community-String zu einem starken, zufälligen String abgeändert werden. Darüber hinaus empfiehlt die CISA, die Protokolle SNMP v2 oder Telnet auf Cisco-Routern zu deaktivieren, da sie den Diebstahl von Anmeldedaten aus unverschlüsseltem Datenverkehr ermöglichen. Besteht der Verdacht, dass ein Router kompromittiert wurde, ist die Integrität des Cisco IOS-Images zu verifizieren. /BLC23w01, CIS23w01/

---

[16] NETCONF steht für Network Configuration Protocol. Es handelt sich um ein Netzwerkprotokoll, das sichere Mechanismen zur Installation, Manipulation und zum Löschen von Konfigurationsdaten auf Netzwerkgeräten wie Firewalls und Switches bereitstellt. /TEC23w01/

[17] RESTCONF ist ein HTTP-basiertes Netzwerkprotokoll, das die im NETCONF definierten Datenspeicherkonzepte verwendet, um eine Schnittstelle für den Datenzugriff bereitzustellen. /FIR23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.7.2 Sicherheitslücken in Moxa MXsecurity Series betreffen kritische Infrastrukturen

Überschrift

Mit der Software MXsecurity Series können Administratoren IT-Sicherheitsvorfälle aufdecken. Im März diesen Jahres wurden Schwachstellen in der Netzwerküberwachungslösung MXsecurity Series des Unternehmens Moxa Inc., welche auch in kritischen Infrastrukturen eingesetzt wird, entdeckt. Weitere Schwachstellen wurden Anfang September bekannt. Über die Schwachstellen können sich Angreifer aus der Ferne Zugriff auf IT-Systeme verschaffen und dort Schadcode ausführen.

Beschreibung

Die Netzwerküberwachungssoftware MXsecurity Series des taiwanesischen Herstellers von Industriesteueranlagen Moxa Inc. wird weltweit in kritischen Infrastrukturen und speziell für ICS eingesetzt /BSI23i01, VUL23w01/. Mit ihr können Administratoren Netzwerke überwachen und IT-Sicherheitsvorfälle erkennen. Über zwei nun in der Software bekannt gewordene, als kritisch eingestufte Schwachstellen CVE-2023-33235 und CVE-2023-33236, können sich Angreifer aus der Ferne Zugriff auf IT-Netzwerke von ICS verschaffen (CVE-2023-33236) und schadhaften Programmcode ausführen (CVE-2023-33235) /BSI23i01, VUL23w01/. Im schlimmsten Fall können Angreifer auf diese Weise Instanzen vollständig übernehmen. Die beiden Schwachstellen wurden unabhängig voneinander von zwei Sicherheitsforschern entdeckt /VUL23w01/. Der Hersteller hat am 08.03.2023 ein entsprechendes Sicherheits-Advisory veröffentlicht /BSI23i01/. Darin wird angegeben, dass in der abgesicherten Version 1.0.1 von MXsecurity die Schwachstellen behoben wurden. Die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) und die Zero Day Initiative (ZDI) haben ebenfalls Advisories veröffentlicht /VUL23w01/. Der Prozess zur Offenlegung der Schwachstellen wurde von ZDI koordiniert /SEC23w01/. Die beiden Schwachstellen CVE-2023-33235 und CVE-2023-33236 betreffen die Softwareversion v1.0 und ältere Versionen von MXsecurity Series /CIS23i01/:

- **CVE-2023-33235:** Hat sich ein Angreifer Autorisierungsrechte für das SSH-Client-Programm[18] erschlichen, kann er aus der Shell[19] ausbrechen und eigenen Programmcode ausführen. Bedrohungsgrad: hoch. CVSS:3.1-Score: 7.2. /BSI23i01, HEI23w01, NVD23i01/

- **CVE-2023-33236:** Da Zugriffsdaten hart codiert wurden, kann ein Angreifer die Authentifizierung umgehen, beliebige JWT-Tokens[20] erzeugen und sich über webbasierte APIs[21] Zugriff auf Systeme verschaffen. Gemäß der CISA sollen dadurch Cyberangriffe aus der Ferne mit verhältnismäßig geringem Aufwand ermöglicht werden. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8. /BSI2023i01, CIS23i01, HEI23w01, NVD23i02/

Am 01.09.2023 wurden fünf weitere Schwachstellen in der Software MXsecurity Series bekannt, die somit auch die zuvor aktualisierte Version 1.0.1 und frühere Softwareversionen betreffen. In dem zugehörigen Advisory gibt der Hersteller Moxa Inc. an, dass alle bisher entdeckten Schwachstellen in der Version 1.1.0 beseitigt wurden. Netzwerk-Administratoren sollten daher zügig das Update auf diese Version der Software installieren. Die fünf zusätzlichen Schwachstellen werden nachstehend beschrieben:

- **CVE-2023-39979:** Ein Angreifer kann aus der Ferne den Authentifizierungsprozess umgehen und unautorisierten Zugriff auf die Softwareanwendung erlangen. Bedrohungsgrad: hoch. CVSS:3.1-Score: 9.8. /CYB23i01, MOX23i0/

- **CVE-2023-39980:** Über diese Schwachstelle kann ein Angreifer aus der Ferne speziell präparierte Anfragen an die Anwendung senden und beliebige SQL-Befehle in der Anwendungsdatenbank ausführen. Der Angreifer kann Daten in der Datenbank lesen, löschen und ändern und die vollständige Kontrolle über die betroffene

---

[18] Secure Shell (SSH) ist ein Netzwerkprotokoll, das eine sichere Verbindung eines Rechners mit einem anderen Rechner oder Server ermöglicht. Ein SSH-Client ist eine Software, die verwendet wird, um diese Art der Verbindung herzustellen. /CHI23w01/

[19] Eine Shell stellt eine Benutzeroberfläche bereit und dient als Mensch-Maschinen-Schnittstelle zwischen Nutzer und Programm. /BIT20w01/

[20] JWT steht für JSON Web Token. Es handelt sich um ein genormtes Access-Token, durch das Kommunikationspartner JSON-Objekte untereinander sicher austauschen können. JSON ist wiederum die Abkürzung für Java Script Object Notation und bezeichnet ein bestimmtes Datenformat. /OPC23w01, SEC22w13/

[21] Eine API (Application Programming Interface) ist ein Satz von Befehlen, Funktionen, Protokollen und Objekten, die von Programmierern verwendet werden, um Software zu erstellen oder um Interaktionen mit einem externen System durchzuführen. /TAL23w01/

Anwendung erlangen. Die Sicherheitslücke besteht, da vom Benutzer bereitgestellte Daten unzureichend bereinigt werden. Bedrohungsgrad: mittel. CVSS:3.1-Score: 7.1. /CYB23i01, MOX23i0/

- **CVE-2023-39981:** Ein Angreifer kann aus der Ferne den Authentifizierungsprozess umgehen und Zugriff auf Geräteinformationen erhalten. Die Sicherheitslücke besteht aufgrund eines Fehlers bei der Verarbeitung von Authentifizierungsanfragen. Bedrohungsgrad: mittel. CVSS:3.1-Score: 7.5. /CYB23i01, MOX23i0/
- **CVE-2023-39982:** Die Schwachstelle ermöglicht einem Angreifer aus der Ferne aufgrund hart codierter Anmeldeinformationen im Anwendungscode einen Man-in-the-Middle-Angriff (MitM) durchzuführen und den SSH-Datenverkehr zu entschlüsseln. Bedrohungsgrad: mittel. CVSS:3.1-Score: 7.5. /CYB23i01, MOX23i0/
- **CVE-2023-39983:** Ein Angreifer kann sich aus der Ferne unbefugten Zugriff auf eingeschränkte Funktionen verschaffen und ein Gerät über die nsm-web-Anwendung registrieren bzw. hinzufügen. Bedrohungsgrad: mittel. CVSS:3.1-Score: 5.3. /CYB23i01, MOX23i0/

Um Cyberangriffe aus dem Internet unter Ausnutzung der Schwachstellen zu verhindern, dürfen kritische Instanzen nicht öffentlich erreichbar sein. Aufgrund der Möglichkeit eines Innentäters sind Netzwerke durch Zugriffsbeschränkungen vor potenziellen Angriffen von innen zu schützen. /BSI23i01, BSI23i02, HEI23w01, MOX23i02/

Die CISA empfiehlt die folgenden, zusätzlichen Maßnahmen, um das Risiko einer erfolgreichen Ausnutzung der Schwachstellen durch Angreifer zu verhindern /CIS23i01/:

- Zur Ermittlung, welche der nachfolgend aufgelisteten Abwehrmaßnahmen in Frage kommen, sind zunächst eine Auswirkungsanalyse und eine Risikobewertung durchzuführen.
- Minimierung des Zugriffs auf alle Kontrollsysteme und -geräte. Darüber hinaus muss sichergestellt werden, dass die Systeme und Geräte nicht über das Internet verfügbar sind.
- Kontrollsystemnetzwerke und Geräte mit Fernzugriff müssen durch Firewalls geschützt und vom Unternehmensnetzwerk getrennt werden.
- Ist ein Fernzugriff auf Systeme und / oder Geräte erforderlich, dann muss dieser abgesichert werden.

Derzeit verfügt die GRS über keine Informationen, dass die Schwachstellen bei Cyberangriffen auf kritische Infrastrukturen ausgenutzt worden sind.

Kerntechnischer Bezug

Ob die Software MXsecurity Series auch in deutschen kerntechnischen Anlagen verwendet wird, ist der GRS derzeit nicht bekannt.

Der Missbrauch von Netzwerküberwachungslösungen als Angriffsweg im Rahmen eines Cyberangriffs ist aus Angreifersicht durchaus erstrebenswert. Zum einen kann bei einem durch den Angreifer kontrollierten Netzwerküberwachungssystem häufig die Wahrscheinlichkeit für eine Entdeckung des Angriffs deutlich reduziert werden. Zum anderen besitzen Netzwerküberwachungssysteme typischerweise weitgehende Rechte, die sich der Angreifer zunutze machen kann.

A.7.3 Netscaler/Citrix

Übersicht

Im Juli 2023 wurden drei Schwachstellen in den Produkten Netscaler ADC und Netscaler Gateway des Herstellers Citrix aufgedeckt. Die schwerwiegendste der drei Schwachstellen wurde zu diesem Zeitpunkt bereits aktiv von IT-Angreifern ausgenutzt. Betroffen ist auch eine Organisation aus dem Bereich der kritischen Infrastrukturen in den USA.

Beschreibung

Am 18.07.2023 berichtete das Unternehmen Citrix über drei kritische Schwachstellen CVE-2023-3466, CVE-2023-3467 und CVE-2023-3519 in seinen Produkten Netscaler Application Delivery Controller (ADC) und Netscaler Gateway (ehemals Citrix ADC und Citrix Gateway) /MAN23w01/. Besonders schwerwiegend ist die Schwachstelle CVE-2023-3519, welche es einem nicht authentifizierten Angreifer ermöglicht aus der Ferne beliebigen Programmcode auszuführen. Sie wird von Angreifern bereits aktiv ausgenutzt, welche Verbindungen zur APT-Gruppierung FIN8 besitzen sollen. Dies ist jedoch zum aktuellen Zeitpunkt noch nicht abschließend geklärt. Sicherheitsforscher von Sophos X-Ops geben an, dass die Angreifer Schadsoftware über die Dateien *wuauclt.exe* oder *wmiprvse.exe* laden. FIN8 ist bereits seit 2016 bekannt und verfolgt finanzielle Motive. Die APT-Gruppierung zielt auf Point-of-Sale-Systeme ab, um Zahlungsdaten

zu stehlen und soll mit der Ransomware White Rabbit in Verbindung stehen, die als Ransomware-as-a-Service entwickelt wurde. Im Juni 2023 richteten die Angreifer unter Ausnutzung der Schwachstelle CVE-2023-3519 eine Webshell auf einem Netscaler ADC-Gerät außerhalb der Produktionsumgebung einer Organisation aus dem Bereich der kritischen Infrastrukturen in den USA ein /CIS23i03/.

Mit der Webshell konnten die Angreifer das Dateiverzeichnis ausspionieren sowie Daten daraus extrahieren und abgreifen. Anschließend versuchten sie sich lateral im Netzwerk zu bewegen und einen Domänencontroller zu infizieren, was durch die Netzwerksegmentierung verhindert wurde. Nach Entdeckung wurde der Vorfall durch die Organisation an die US Cybersecurity and Infrastructure Security Agency (CISA) und Citrix gemeldet. Daraufhin veröffentlichte Citrix am 18.07.2023 ein Patch, um die Sicherheitslücke zu schließen und die CISA am 20.07.2023 ein entsprechendes Advisory /CIS23i03/. Gelingt es IT-Angreifern jedoch durch Ausnutzung der Schwachstelle CVE-2023-3519 eine Backdoor auf dem System einzurichten, bevor die Installation des Patch erfolgte, so besteht nach wie vor weiterhin Zugriff auf das entsprechende System. Insgesamt sind 2.000 Citrix Netscaler Server mit Webshells kompromittiert worden, was auf ein automatisiertes Vorgehen schließen lässt. Auf mehr als 1200 Servern wurde eine Backdoor installiert, bevor die Installation des Patch durch Administratoren erfolgte. Die Angriffsziele befinden sich im Wesentlichen in Deutschland und Europa, aber auch in Französisch-Guyana, Japan, China, Indien, Brasilien und Südafrika. /BSI23i04, HEI23w11/

Die drei von Citrix veröffentlichten Schwachstellen werden nachfolgend beschrieben /BSI23i04, CIS23i03, CIT23i01, HEI23w11, NVD23i04, SEC23w06/:

- **CVE-2023-3519:** Unauthenticated Remote Code Execution-Lücke in einem über das Internet erreichbaren Dienst: Die Schwachstelle ermöglicht es einem Angreifer aus der Ferne und ohne Authentifizierung beliebigen Programmcode auszuführen. Eine erfolgreiche Ausnutzung der Schwachstelle erfordert, dass das Gerät als Gateway (VPN Virtual Server, ICA Proxy, CVPN, RDP Proxy) oder als virtueller AAA-Server (Authentication, Authorization und Auditing) konfiguriert ist. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8.
- **CVE-2023-3466:** Reflected Cross-Site Scripting (XSS): Eine Ausnutzung der Schwachstelle erfordert, dass das Opfer auf einen vom Angreifer kontrollierten Link im Browser zugreift, während es sich in einem Netzwerk mit Konnektivität zum NSIP befindet. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.3.

- **CVE-2023-3467:** Rechteausweitung zum Root-Administrator (nsroot): Die Schwachstelle ermöglicht einem authentifizierten Angreifer den Zugriff auf NSIP oder SNIP mit Zugriff auf die Verwaltungsschnittstelle. Bedrohungsgrad: hoch. CVSS:3.1-Score: 8.0.

Von den IT-Sicherheitsunternehmen Mandiant und FOXiT wurden Scanner zur Erkennung einer Kompromittierung unter Ausnutzung der Schwachstelle CVE-2023-3519 entwickelt und auf GitHub veröffentlicht /BSI23i04/. Dort befindet sich auch eine Liste mit Indicators of Compromise (IoCs), die von Sophos erstellt wurde /BLC23w04/. Auf *deyda.net* ist eine Anleitung erschienen, mit der sich die Citrix Systeme auf eine mögliche Kompromittierung hin untersuchen lassen. Cyberangriffe können dabei über veränderte Datei-Zeitstempel erkannt werden. Diese Zeitstempel ändern sich nur bei Netscaler-Updates. Sind die Zeitpunkte der letzten Updates bekannt und weichen die Zeitstempel einiger Installationsdateien davon ab, dann deutet dies auf Aktivitäten von IT-Angreifern hin. Hinweise auf einen Angriff lassen sich auch in den http Fehlerprotokoll-Dateien und in den Shell-Protokolldateien finden. Darüber hinaus gibt deyda.net über weitere Indizien einer Kompromittierung Auskunft. /HEI23w11/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.7.4 Schwachstelle in der APSystems Altenergy Power Control Software

Übersicht

Eine Schwachstelle in der Altenergy Power Control Software des Herstellers APSystems ermöglicht die Ausführung von beliebigem Programmcode im Betriebssystem. Die Software wird zum Auslesen von Wechselrichtern innerhalb kritischer Infrastrukturen im Bereich des Energiesektors eingesetzt.

Beschreibung

Am 01.08.2023 hat die US Cybersecurity and Infrastructure Security Agency (CISA) eine Warnung bezüglich einer kritischen Schwachstelle CVE-2023-28343 in der Altenergy Power Control Software des US-amerikanischen Herstellers APSystems veröffentlicht. Von der Schwachstelle betroffen ist die Version C1.2.5 der Software. Die Software wird

zum Auslesen von Wechselrichtern verwendet und ist nach eigenen Angaben von AP-Systems weltweit im Einsatz. Sie findet innerhalb kritischer Infrastrukturen im Bereich des Energiesektors Anwendung. Die Schwachstelle ist besonders schwerwiegend, da sie die Ausführung von beliebigem Programmcode im Betriebssystem ermöglicht. Ein Proof of Concept (PoC), um die Software auf das Vorhandensein der Schwachstelle hin zu untersuchen, ist verfügbar. Derzeit ist aber nicht bekannt, ob der Hersteller ein Patch zum Schließen der Schwachstelle erstellt hat. Die CISA gibt an, dass der Hersteller AP-Systems bislang auf Kontaktversuche ihrerseits nicht reagiert habe. /BSI23i05, CIS23i04/

Die Schwachstelle wird nachfolgend beschrieben /BSI23i05, NVD23i05/:

- **CVE-2023-28343:** Eine ungenügende Eingabevalidierung von Zeitzonenparametern ermöglicht es einem Angreifer aus der Ferne beliebigen Programmcode im Betriebssystem auszuführen. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8.

Anwender der Software sollten weitere Informationen über den Kundensupport von AP-Systems einholen. Zusätzlich müssen die Standardvorkehrungen zum Schutz von Industriesteuerprodukten getroffen werden wie Minimierung der Netzwerkexposition und Isolierung der Netze. Derzeit liegen der GRS keine Informationen über eine Ausnutzung dieser Schwachstelle bei Cyberangriffen vor. /BSI23i05, CIS23i04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.7.5 Kritische Schwachstellen in Siemens SIMATIC S7-1200 und S7-1500CPU-Systemen

Übersicht

Am 12.10.2022 veröffentlichte das BSI eine Cyber-Sicherheitswarnung zu einer kritischen Schwachstelle in Siemens SIMATIC S7-1200 und S7-1500 CPU-Produkten /BSI22r19/. Am 13.10.2022 veröffentlichte die CISA zudem eine entsprechende Warnmeldung (ICS-Advisory ICSA-22-286-04) /CIS22r04/. Die Warnmeldungen basieren auf einem am 11.10.2022 veröffentlichten Siemens Security Advisory (SSA-568427: Weak Key Protection Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families

/SSA22r01/) und handeln von einer Schwachstelle bzgl. der Verwendung eines veralteten kryptographischen Schlüssels in den entsprechenden Produkten. Bei erfolgreicher Ausnutzung dieser Schwachstelle könnten Angreifer an vertrauliche Konfigurationsdaten gelangen. Das BSI und die CISA weisen in ihren Warnmeldungen insbesondere auf die vergleichsweise einfache geringe Angriffskomplexität bei der Ausnutzung und das hohe Schadenspotential der Schwachstelle hin, der ein CVSS-Score von 9.3 (kritische Schwachstelle) zugewiesen wurde. Das BSI geht aufgrund der hohen Verbreitung der Systeme in verschiedenen Branchen von einer hohen Relevanz aus. /BSI22r19, CIS22r04/

Beschreibung

Bei der Schwachstelle handelt es sich um einen globalen, fest kodierten privaten kryptografischen Schlüssel auf Basis eines veralteten kryptografischen Standards für Funktionen von Siemens Produkten. Dieser Schlüssel wird zum Schutz von vertraulichen Konfigurationsdaten und älteren Kommunikationsverbindungen eingesetzt. Potenzielle Angreifer, die Zugriff auf ein Gerät der Produktfamilie haben, können den nicht länger als sicher zu betrachtenden Schlüssel extrahieren unterschiedliche Arten von Cyberangriffen ausführen. Beispielsweise können vertrauliche Konfigurationsdaten wie kryptografische Schlüssel oder Passwörter extrahiert werden oder Man-in-the-Middle-Angriffe durchgeführt werden, bei denen Angreifer den Datenaustausch zwischen SPS und Human-Machine-Interfaces/Engineering-Stations lesen, modifizieren oder blockieren können. Siemens hat ein Update veröffentlicht, das die Schwachstelle beseitigt und empfiehlt seinen Kunden dringend die entsprechende Aktualisierung der von der Schwachstelle betroffenen Systeme. /BSI22r19, CIS22r04/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen, da speicherprogrammierbare Steuerungen der genannten Produktfamilien auch in diesen eingesetzt werden.

A.7.6 Kritische Schwachstelle in BeyondTrust PRA und RS

Übersicht

Eine kritische Schwachstelle betrifft die Produkte PRA und RS des Herstellers BeyondTrust. Eine Verwendung der beiden Produkte im Bereich der kritischen Infrastrukturen kann derzeit nicht ausgeschlossen werden.

Beschreibung

Eine kritische Schwachstelle mit Bezeichnung CVE-2023-4310 betrifft die Produkte Privileged Remote Access (PRA) und Remote Support (RS) des amerikanischen Herstellers BeyondTrust, die den Fernzugriff auf IT-Systeme ermöglichen. Es handelt sich um eine Command-Injection-Schwachstelle, welche vom Sicherheitsforscher Brian Krebs am 31.07.2023 während eines Tests entdeckt wurde. Unter Ausnutzung der Schwachstelle kann ein entfernter, nicht authentifizierter Angreifer speziell gestaltete HTTP-Anfragen senden, was ihm das Ausführen von Betriebssystembefehlen im Kontext des Webseitennutzers ermöglicht. Die Schwachstelle besitzt einen CVSS:3.1-Score von 9.8 /NVD23i08/ und betrifft die Versionen 23.2.1 und 23.2.2. In Deutschland sind bislang 250 potenziell verwundbare Server bekannt, von denen einige möglicherweise auch in kritischen Infrastrukturen eingesetzt werden. Ein Hotfix mit Bezeichnung TRY-21041 kann über das Menü zur Updatesuche ausgeführt oder über das Kundenportal nach erfolgter Anmeldung heruntergeladen werden. Im Kundenportal befindet sich auch die zur Schwachstelle gehörende Meldung und das Advisory von BeyondTrust. Die Schwachstelle soll in der Version 23.2.3 behoben werden, während nach Angaben des Unternehmens die Cloud-Instanzen der beiden Produkte bereits gepatscht und Kunden per E-Mail darüber informiert und aufgefordert wurden, das Patch so schnell wie möglich zu installieren. BeyondTrust gibt zudem an, dass man jeden Kunden, bei dessen Produkten ein Upgrade nicht bestätigt werden konnte, telefonisch kontaktiert habe. /BET23i01, BSI23i11, NVD23i08/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B IT-Sicherheitsvorfälle und Cyberangriffe

In den folgenden Abschnitten werden ausgewählte IT-Sicherheitsvorfälle und Cyberangriffe kurz beschrieben, bei denen im Rahmen des Screenings der IT-Bedrohungslage eine mögliche Relevanz für industrielle Steuerungssysteme und kritische Infrastrukturen ein-schließlich kerntechnischer Anlagen ausgemacht wurde. Dies schließt auch die Angriffswerkzeuge und Schadsoftwarekomponenten ein, die bei diesen Cyberangriffen zum Einsatz kamen. Angriffswerkzeuge, die bislang noch keinem Cyberangriff zugeordnet werden konnten, wurden bereits in Abschnitt A beschrieben.

Wie schon einleitend beschrieben, werden diese Ersteinschätzungen der GRS zu diesen IT-Sicherheitsvorfällen und Cyberangriffen immer wieder an die vorliegenden Informationen angepasst, um weitere Aspekte ergänzt und bei Bedarf vollständig überarbeitet. Sie sind daher Bestandteil eines lebenden Dokuments und nicht als abgeschlossen zu verstehen.

Neben den IT-Sicherheitsvorfällen und Cyberangriffen, für die bereits eine Ersteinschätzung vorgenommen wurde, sind hier auch solche Vorfälle und Angriffe gelistet, deren Auswertung im aktuell laufenden Vorhaben nicht durchgeführt werden konnte, aber im Rahmen des geplanten Anschlussvorhabens erfolgen wird. Dabei handelt es sich so-wohl um kürzlich bekannt gewordene IT-Sicherheitsvorfälle und Cyberangriffe, als auch um ältere Vorfälle und Angriffe, die für die IT-Bedrohungslage relevant sind und deren Aufarbeitung nach und nach erfolgt. Der Zeitpunkt, zu dem ein IT-Sicherheitsvorfall oder Cyberangriff bekannt wird, hat keinen Einfluss auf dessen Bedeutung für die IT-Bedrohungslage, daher ist es für ein möglichst vollständiges Verständnis der IT-Bedrohungslage ausschlaggebend, alle bislang bekannt gewordenen, relevanten IT-Sicherheitsvorfälle und Cyberangriffe möglichst umfassend zu berücksichtigen. Daher sind im hier wiedergegebenen lebenden Dokument nicht nur IT-Sicherheitsvorfälle und Cyberangriffe beschrieben, die im Berichtszeitraum bekannt geworden sind, sondern es wurden sukzessive auch herausragende Vorfälle und Angriffe aus früheren Jahren aufgearbeitet, soweit es im Rahmen des Vorhabens möglich war.

Viele Cyberangriffe laufen unbemerkt oder auch ungehindert über mehrere Jahre, daher ist die Zuordnung zu einem einzelnen Jahr oftmals nicht eindeutig. Konkrete IT-Sicherheitsvorfälle werden hier typischerweise dem Jahr zugeordnet, in dem sie

bekannt wurden. Länger andauernde Angriffswellen werden dem Jahr zugeordnet, in dem ihr (teilweise auch vorläufiger) Höhepunkt ausgemacht werden kann

B.1 2007

B.1.1 Stuxnet 0.5

Übersicht

Bei Stuxnet 0.5 handelt es sich um die derzeit älteste bekannte Version der Stuxnet-Schadsoftwarefamilie. Sie wurde bereits seit 2005 entwickelt und ab 2007 eingesetzt.

Beschreibung

Mit dem Namen Stuxnet wird nicht nur eine einzige Schadsoftwarekomponente bezeichnet, vielmehr werden unter Stuxnet eine ganze Familie von Schadsoftwarekomponenten zusammengefasst. Als erste entdeckt wurde eine im März 2010 kompilierte Version der Schadsoftware, die heute als Stuxnet Variante B bekannt ist und sich weltweit am meisten verbreitete. Im Zuge der massiven Recherchen und Untersuchungen, die nach Bekanntwerden von Variante B angestrengt wurden, entdeckte man auch die nicht ganz so stark verbreitete Variante A aus dem Jahr 2009 und die Variante C aus dem Jahr 2010. Alle drei Varianten haben gemein, dass sie eine Funktionalität zur Manipulation von Motoren besitzen, die speziell im Bereich von Zentrifugen zur Urananreicherung eingesetzt werden.

Eine deutlich früher erstellte Version der Schadsoftware, Stuxnet 0.5, wurde erst 2013 entdeckt. Sie ist im Gegensatz zu den späteren, bereits 2010 entdeckten Varianten auf eine Manipulation von Ventilen zur Regelung des Uranhexafluiddurchflusses im Anreicherungsprozess ausgerichtet und wurde derzeitigen Erkenntnissen zufolge von einem im Geheimdienstauftrag agierenden Innentäter in die Anlage Natanz eingebracht.

Stuxnet 0.5 besitzt deutlich weniger Flexibilität hinsichtlich möglicher Verbreitungswege als spätere Varianten. So verbreitet sich diese Schadsoftware nur über infizierte Step 7 Projekte.

Es ist derzeit nicht bekannt, wie erfolgreich der Angriff mit Stuxnet 0.5 auf die Urananreicherung in Natanz war. Die relativ hohe Austauschrate bei den Zentrifugen im relevanten Zeitraum deutet zumindest auf einen teilweisen Erfolg hin. Auch gibt es Berichte über den in großer Zahl vorgenommenen Austausch von Technikern. Die Tatsache, dass die späteren Stuxnet-Varianten eine andere Angriffsstrategie verfolgen, deutet allerdings darauf hin, dass man sich von dieser anderen Strategie noch höhere Ausfallraten versprach.

Kerntechnischer Bezug

Die Schadsoftware Stuxnet wurde offensichtlich gezielt entwickelt, um das iranische Atomprogramm zu sabotieren. Tatsächlich kam es zu Beschädigungen an einem erheblichen Teil der in der iranischen Urananreicherungsanlage Natanz eingesetzten Zentrifugen. Zusätzlich zu den physischen Schäden, die durch die von Stuxnet hervorgerufenen Manipulationen langfristig an den Zentrifugen entstanden sind, ist davon auszugehen, dass die Manipulationen auch einen Einfluss auf die Qualität des angereicherten Urans hatten.

B.2 2008

B.2.1 BlackEnergy 1 – Cyberangriffe auf georgische Einrichtungen

Übersicht

Bei BlackEnergy 1 handelt es sich um ein HTTP-basiertes Angriffswerkzeug zur Durchführung von DDoS-Angriffen. BlackEnergy 1 wurde mehrfach weiterentwickelt. In den Jahren 2010 bzw. 2015 wurden die Versionen BlackEnergy 2 bzw. BlackEnergy 3 (siehe Abschnitte B.5.2 bzw. B.7.1) erstmalig bekannt und in den Folgejahren jeweils breit eingesetzt, wobei von jeder Version zahlreiche Varianten in Umlauf sind.

Beschreibung

Die Schadsoftware BlackEnergy 1 besteht aus einem Dropper, einem Treiber bzw. Rootkit und der MainDLL. Diese Komponenten werden im Folgenden erklärt. /ITB16r01/

Der Dropper ist ein Hilfsprogramm. Er lädt den in ihm enthaltenen Rootkit-Treiber und zählt alle auf dem befallenen Gerät bereits installierten Treiber auf. Danach wählt er zufällig einen deaktivierten Treiber aus und ersetzt diesen durch den infizierten Treiber. Der entsprechende Dateipfad wird so konfiguriert, dass er bei einem Bootvorgang automatisch gestartet wird. Auf diese Weise erreichen die Angreifer eine persistente Verbindung. Der Rootkit-Treiber bildet somit eine Backdoor. Nur diese Komponente verbleibt dauerhaft auf dem infizierten System. Der Dropper startet das System neu und verweist danach auf sich selbst, wodurch er eine Signatur erzeugt. Er aktiviert unter Windows den Testmodus im Boot-Menü. Somit können Treiber verwendet werden, die nicht von Microsoft digital signiert wurden, was die Anwendung des infizierten Treibers ermöglicht /MIS20w01/. Danach blendet der Dropper die Hinweise aus, dass das System im Testmodus gestartet wurde und umgeht die Benutzerkontensteuerung (User Account Control UAC) von Windows. Der Dropper nutzt die Microsoft-Schwachstelle MS08-025 aus, die es dem Angreifer erlaubt seine Zugriffsrechte auf das System zu erhöhen, auch wenn der Benutzer des infizierten Geräts über keine Rechte verfügt, neue Software zu installieren. Auf diese Weise ist der Dropper in der Lage die Installation des Rootkit-Treibers abzuschließen. /FSE14r01, ITB16r01, SEC10w01/

Der Rootkit-Treiber verwendet API-Hooking[22], um Objekte auf Festplatten, in der Registry und in Speichern zu verbergen. Dadurch wird die Detektion des Treibers erschwert. Schließlich lädt der Treiber die in ihm eingebettete MainDLL der Schadsoftware und führt diese aus. /SEC10w01/

Die MainDLL kann Dateien vom C&C-Server der Angreifer laden und ausführen. Dazu zählen auch Updates der Schadsoftware /SEC10w01/. Ab Version 1.8, welche 2008 entwickelt wurde, verfügt BlackEnergy 1 über drei zusätzliche Plugins zur Durchführung von DDoS-Angriffen. Diese unterscheiden sich in der Art und Weise der Durchführung des Angriffs und werden als *DDoS-Plugin, syn-Plugin und http-Plugin* bezeichnet: /ITB16r01, SEC10w01/

- **DDoS-Plugin**: Dieses Plugin greift das Zielgerät mit zufälligen TCP-, UDP-, ICMP- und HTTP-Nachrichten an. Die Abkürzungen stehen für verschiedene Netzwerkprotokolle. /SEC10w01/

[22] API-Hooking beschreibt Techniken, mit denen das Verhalten und der Fluss von API-Anfragen modifiziert und manipuliert werden kann /INF14w01/. APIs (Application Programming Interfaces) wiederum sind Software-to-Software-Schnittstellen /HUB22w01/.

- **syn-Plugin**: Das Plugin lädt einen Kernel-Treiber, der das Zielgerät mit TCP SYN-Paketen bombardiert. SYN steht für Synchronization. Durch Verwendung des Kernels können die SYN-Pakete sehr schnell und ohne Einfluss auf die TCP-Statustabelle des Systems verschickt werden, welche nur eine begrenzte Anzahl an Einträgen aufnehmen kann. /SEC10w01/
- **http-Plugin**: Das Plugin nutzt die OLE-Automatisierung des Internet Explorers, um das Zielgerät mit HTTP-Anfragen zu bombardieren. Obwohl dieser Angriff langsamer als der HTTP-Angriff des DDoS-Plugins abläuft, macht es die Verwendung des Internet Explorers schwieriger zwischen einem Angriff und normalem Browsen zu unterscheiden. /SEC10w01/

Entscheidend ist, dass durch die Möglichkeit des Herunterladens von Plugins ein modularer Aufbau der Schadsoftware realisiert wird, da diese jederzeit durch zusätzliche Plugins erweiterbar ist.

Die Schadsoftware BlackEnergy 1 wurde zum ersten Mal von Arbor Networks in der Mitte des Jahres 2007 entdeckt. Dabei wurden 27 mit BlackEnergy 1 infizierte Botnetze untersucht, von denen jedes aus etwa 100 Bots bestand. Die meisten Botnetze befanden sich in Russland und Malaysia, wobei sich die meisten Ziele für über die Botnetze durchgeführte DDoS-Angriffe in Russland befanden. BlackEnergy 1 wurde im Rahmen zahlreicher Cyberangriffe eingesetzt, unter anderem wohl auch bei mehreren Angriffswellen 2008 auf georgische Einrichtungen im Vorfeld der militärischen Auseinandersetzungen zwischen Russland und Georgien. Betroffen waren unter anderem Webseiten zahlreicher Regierungseinrichtungen, Nachrichtenagenturen und Finanzunternehmen. /THS16r01, FSE14r01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.3 2010

B.3.1 Stuxnet – Cyberangriff auf Natanz

Übersicht

Bei Stuxnet handelt es sich um die erste bekannt gewordene, speziell auf die Manipulation von SPS (Speicherprogrammierbaren Steuerungen) ausgerichtete Schadsoftware. Stuxnet ist eine hochentwickelte, komplexe Schadsoftware, die nach einer erfolgten Erstinfektion in der Lage ist, auch autonom zu agieren und für die Durchführung der gezielten Manipulationen von Steuerungen nicht auf eine Interaktion mit den Angreifern angewiesen ist.

Beschreibung

Bei Stuxnet handelt es sich um eine Schadsoftware, die gezielt mehrere Sicherheitslücken im Microsoft Betriebssystem Windows ausnutzt, um sich zu verbreiten. Eine dieser Schwachstellen nutzt Stuxnet, um sich beispielsweise über Netzwerke oder mobile Datenträger wie USB-Sticks auf ein IT-System einzuschleusen, auch über Air-Gaps hin-weg. Hierfür benötigt Stuxnet keine Aktion des Nutzers und keine aktivierte Autostart-Funktion, sondern es reicht aus, ein Verzeichnis zum Betrachten zu öffnen, das eine infizierte LNK-Datei enthält. Der Schadcode wird bereits bei Anzeige des manipulierten Icons im Explorer ausgeführt. Die hierbei ausgenutzte Schwachstelle, die als LNK-Schwachstelle bekannt ist, wurde von Microsoft zeitnah gepatcht, allerdings sind die entsprechenden Patches nach wie vor nicht flächendeckend eingesetzt. Microsoft listete beispielsweise im Security Intelligence Report für 2015 die LNK-Schwachstelle, als die am häufigsten von Angreifern ausgenutzte Einzelschwachstelle des Jahres 2015 /MIC15r01/. Zusätzlich dazu ist trotz Patchen der Schwachstelle eine Infektion mit Stuxnet durch Doppelklick auf eine infizierte Datei möglich. Neben der Verbreitung über Wechselmedien ist Stuxnet aber auch in der Lage, sich über zahlreiche andere Wege wie beispielsweise über das Intranet, gemeinsam genutzte Drucker, die Microsoft SQL Datenbank von WinCC sowie Step-7 Projekte zu verbreiten, teilweise unter Ausnutzung weiterer Schwachstellen im Microsoft Windows Betriebssystem. /GRS12f01/

Bei der Infektion eines Systems mit Stuxnet wird jeweils eine Schadsoftwarekomponente zum Ausspähen von Informationen und ein sogenanntes Rootkit zum Verschleiern der Infektion installiert.

Auf infizierten Systemen sucht Stuxnet gezielt nach Prozesssteuerungssystemen, die SIMATIC WinCC oder SIMATIC PSC7 von Siemens einsetzen. Als erste Schadsoftware ist Stuxnet speziell darauf ausgerichtet, diese Software zu manipulieren und darüber speicherprogrammierbare Steuerungen zu infizieren und zu manipulieren. Die bekannten Versionen von Stuxnet (Variante A und Variante B) zielen auf die Manipulation von Frequenzumrichtern für besonders hohe Frequenzen ab, wie sie beispielsweise für Zentrifugen bei der Urananreicherung eingesetzt werden. /GRS12f01/

Kerntechnischer Bezug

Die Schadsoftware Stuxnet wurde offensichtlich gezielt entwickelt, um das iranische Atomprogramm zu sabotieren. Tatsächlich kam es zu Beschädigungen an einem erheblichen Teil der in der iranischen Urananreicherungsanlage Natanz eingesetzten Zentrifugen. Zusätzlich zu den physischen Schäden, die durch die von Stuxnet hervorgerufenen Manipulationen langfristig an den Zentrifugen entstanden sind, ist davon auszugehen, dass die Manipulationen auch einen Einfluss auf die Qualität des angereicherten Urans hatten.

B.4 2011

B.4.1 Chinese Gas Pipeline Intrusion Campaign

Übersicht

Zwischen den Jahren 2011 und 2013 wurden vom chinesischen Staat unterstützte Spear-Phishing-Angriffe auf US-amerikanische Gaspipeline-Unternehmen durchgeführt. Diese Angriffe hatten das Potential physische Schäden an den Pipelines durchzuführen und ihren Betrieb zu stören.

Beschreibung

Zwischen Dezember 2011 und 2013 wurden im Zuge einer vom chinesischen Staat unterstützten Spear-Phishing-Kampagne US-amerikanische Öl- und Gaspipeline-Unternehmen angegriffen. Von den 23 betroffenen Gaspipeline-Unternehmen wurden 13 kompromittiert, bei acht Unternehmen ist der Grad der Intrusion unbekannt und bei drei

Unternehmen konnte ein Eindringen in das Netzwerk gerade noch verhindert werden. /CIF21i01, EEN21w01/

Die Spear-Phishing-E-Mails waren an die Angestellten der Unternehmen gerichtet und waren mit großem Aufwand so gestaltet, dass sie die Angestellten dazu verleiteten die schadhaften Dateien im E-Mail-Anhang zu öffnen /CSM12w01/. Neben der Spear-Phishing-Kampagne versuchten die Angreifer wohl auch sich durch Social Engineering Zugriff zu den Firmennetzwerken zu verschaffen. In einem Unternehmen erhielten An-gestellte und Manager, die in der Netzwerk-Engineering-Abteilung arbeiteten, dubiose Anrufe, in denen sie über die aktuellen Sicherheitsmaßnahmen zum Schutz des Firmennetzwerks befragt wurden. Dabei gaben sich die Angreifer als Angestellte einer Computersicherheitsfirma aus, die Umfragen durchführen würde. Diese Anrufe erfolgten unmittelbar nachdem die Angriffe erkannt, die Angreifer erfolgreich aus dem Netzwerk ausgesperrt wurden und das System neu gestartet worden war. Während der Cyberangriffe wurden die Dokumente-Repositories von den Angreifern nach SCAD*-Dateien, Personallisten, Benutzernamen und Passwörtern, Dial-up-Zugriffsinformationen sowie Systemhandbüchern durchsucht. Sie kompromittierten eine Vielzahl autorisierter Fernzugriffskanäle. Dazu zählen auch Systeme für den Datentransfer mit und den Zugriff auf ICS-Netzwerke. Darüber hinaus gelang es ihnen auf die SCADA-Netzwerke von Gaspipeline-Unternehmen zuzugreifen. Nach Ansicht des CISA und des FBI könnten die gestohlenen Daten und Informationen für die Vorbereitung eines Cyberangriffs des chinesischen Staates auf die Pipeline-Infrastruktur der USA genutzt werden, mit dem Ziel die Pipelines physisch zu beschädigen oder ihren Betrieb zu stören und so die US-amerikanische Pipeline-Infrastruktur zu gefährden. /CIF21i01, EEN21w01/

Um eine Infizierung von Netzwerken zu vermeiden, empfehlen das CISA und das FBI Zugriffsbeschränkungen und eine Multi-Faktor-Authentifizierung einzurichten. Darüber hinaus sollte der Datenverkehr gefiltert und kontrolliert werden. Eine Segmentierung zwischen IT-Netzen und ICS- bzw. OT-Netzen (OT – Operational Technology) erschwert die Ausbreitung schadhafter Einwirkungen vom Firmennetzwerk auf die Steuerungssysteme. /CIF21i01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.5 2012

B.5.1 Shamoon – Cyberangriff auf Saudi Aramco

Übersicht

Die Schadsoftware Shamoon (auch W32.DistTrack) wurde im Jahr 2012 bei einem Cyberangriff auf Saudi Aramco, das weltweit größte Unternehmen zur Erdölförderung, eingesetzt /BBC12w01/. Shamoon ist in der Lage, die auf den Rechnern enthaltenen Dateien zu überschreiben und die Rechner selbst in einem nicht-bootfähigen Zustand zu hinter-lassen. Auf diese Weise kann für ein angegriffenes Unternehmen erheblicher Schaden entstehen.

Beschreibung

Shamoon besteht im Wesentlichen aus drei Schadsoftwarekomponenten /SYM12r01/:

- Einer Dropper-Komponente, die für die Installation der weiteren Komponenten verantwortlich ist,
- einer Wiper-Komponente, welche auf dem infizierten Rechner zuerst Dateien und schließlich auch den Master Boot Record überschreibt, wonach der Rechner nicht mehr gebootet werden kann, sowie
- einer Reporter-Komponente, welche Informationen über die Infektion einschließlich einer Liste der gelöschten Dateien an die Angreifer schickt.

Der beim Angriff auf Saudi Aramco eingesetzte Code von Shamoon enthielt zusätzlich einen Timer, der zu der zeitgleichen Ausführung der Wiper-Komponente auf allen infizierten Rechnern führte.

Der Angriff auf Saudi Aramco begann vermutlich Mitte 2012 mit einer gezielten Spear-Phishing-Attacke, welche zur Infektion eines ersten Rechners führte und den Angreifern Zugriff auf das Anlagennetzwerk verschaffte. Von einem Command-and-Control Server aus nutzten die Angreifer diesen Rechner zur weiteren Verbreitung im Anlagennetz. Dies schließt auch die Infektion von Rechnern mit ein, die selbst nicht mit dem Internet verbunden waren. /SEC12w01/

Am 12. August 2012, zeitgleich um 11:08 Uhr begann Shamoon mit dem Überschreiben von Dateien auf 30 000 Rechnern. Insgesamt waren von dem Angriff etwa drei Viertel der Informationsinfrastruktur von Saudi Aramco betroffen. /BBC12w01, NYT12w01/

Kaspersky und andere IT-Sicherheitsunternehmen haben Shamoon untersucht und auch mögliche Parallelen zu den Cyberangriffen in Zusammenhang mit Flame (siehe Abschnitt B.5.1) untersucht, bezeichnen Shamoon aber letztlich als Copycat und schreiben ihn „begabten Amateuren“ zu. /DAR12w01, SEC12w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.5.2 BlackEnergy 2 – Globaler Cyberangriff

Übersicht

Bei BlackEnergy 2 handelt es sich um eine Weiterentwicklung des als BlackEnergy 1 (siehe Abschnitt B.2.1) bekannt gewordenen HTTP-basierten Angriffswerkzeugs zur Durchführung von DDoS-Angriffen. Wie schon von BlackEnergy 1 sind auch von BlackEnergy 2 zahlreiche Varianten in Umlauf. Die IT-Sicherheitsfirma Kaspersky Labs zählte 2010 bereits mehr als 4000 Varianten der beiden Schadsoftware-Versionen /SEC10w02/.

Beschreibung

BlackEnergy 2 wurde 2010 entwickelt und besteht wie BlackEnergy 1 (siehe Abschnitt B.2.1) aus dem Dropper, dem Rootkit-Treiber, der MainDLL und wurde zusätzlich um eine Vielzahl herunterladbarer Plugins erweitert, darunter Plugins zur Versendung von Spam-Nachrichten und für Betrügereien beim Online-Banking. Dadurch erhielt die Schadsoftware einen modularen Aufbau. Durch den modularen Aufbau ist die Schad-software sehr vielseitig einsetzbar. /ITB16r01/

Der Programmcode wurde dabei von BlackEnergy 1 übernommen. Die Unterschiede zu BlackEnergy 1 bestehen darin, dass BlackEnergy 2 moderne Methoden zum Entpacken des Rootkit-Treibers und der Infiltrierung von Benutzer-Prozessen verwendet. /SEC10w01/

Der Dropper von BlackEnergy 2 lädt zunächst einen Rootkit Decrypter, in dem der eigentliche Rootkit-Treiber enthalten ist. Letzterer wird wiederum vom Rootkit Decrypter entpackt. Abgesehen von dieser zusätzlichen Einbettung, weist BlackEnergy 2 dieselbe verschachtelte Struktur wie BlackEnergy 1 auf. Auch der Entpackungsvorgang der Schadsoftware ist bis auf diesen zusätzlichen Schritt identisch.

Von Antivirenprogrammen wird BlackEnergy 2 häufig als Rustock.E fehlidentifiziert, da der Rootkit-Treiber von BlackEnergy 2 einige ähnliche Techniken verwendet wie das Rootkit der Schadsoftware Rustock.E. Letztere gehört jedoch zu einer anderen Schadsoftware-Familie. Auch die verschachtelte Struktur ist beiden Schadsoftware-Varianten gemein. /SEC10w01/

Nachfolgend werden die zusätzlichen Plugins beschrieben, die BlackEnergy 2 bereit-stellt:

- **Spam-Plugin**: Hierbei handelt es sich um eine wieder verwendete Version des Spambots Grum, ein infiziertes Computernetzwerk, das von C&C-Servern dazu gebracht wird Spam-Mails zu verschicken. Dieser Spambot ist mit der Plugin-Architektur von BlackEnergy 2 kompatibel. /SEC10w01, SPI12w01/
- **Ibank-Plugin**: Über dieses Plugin können die Zugangsdaten für das Online-Banking eines Benutzers gestohlen werden. Es besteht aus zwei Komponenten, dem Haupt- und dem in diesem eingebetteten Unter-Modul. Das Haupt-Modul schleust das Unter-Modul in die Internet Explorer-, Firefox-, Flock- Opera- und Java-Browseranwendungen ein. In jeder dieser Anwendungen führt das Unter-Modul eine Programmschleife aus und überprüft die jeweilige Anwendung auf einen auf Java basierenden Dialog. Von diesem speichert es die Tastatureingaben oder Eingaben aus der Zwischenablage durch den Benutzer, um dessen Zugangsdaten für das Online-Banking zu erhalten. Darüber hinaus speichert das Unter-Modul angeforderte Internetadressen zur Identifikation des Geldinstituts. Die gespeicherten Informationen werden schließlich an das Haupt-Modul gesendet. Dieses leitet sie an den C&C-Server der Angreifer weiter. Das Plugin ist auf ein spezielles, auf öffentlicher Verschlüsselung basierendes, Online-Banking-System zugeschnitten, das von vielen russischen und ukrainischen Banken verwendet wird. /SEC10w01/
- **Kill-Plugin**: Dieses Plugin wird in Verbindung mit dem zuvor beschriebenen Ibank-Plugin eingesetzt. Es zerstört das Dateisystem des infizierten Computers, indem es auf jeder unter Windows aufgelisteten Festplatte die ersten 4096 Cluster mit

zufälligen Daten überschreibt und die Bootfähigkeit des Systems zerstört. Danach fährt das Plugin das System herunter. Das Plugin wird vermutlich nach dem Diebstahl der Daten für das Online-Banking eingesetzt. Dadurch wird verhindert, dass der Benutzer sich in sein Portal für das Online-Banking einloggen kann. Auf diese Weise erkennt er nicht, dass von den Angreifern Geld von seinem Konto abgehoben wird, was ihn dazu veranlassen könnte sein Geldinstitut über die illegale Transaktion zu informieren. /SEC10w01/

Die APT-Gruppierung Sandworm übernahm im Jahr 2013 die BlackEnergy 2 Schad-software und erweiterte diese um eine Vielzahl eigener, zusätzlicher Plugins. Diese ermöglichen die Erzeugung zusätzlicher Backdoors, die Auskundschaftung des Netzwerkes, das Überschreiben, Löschen, Herunterladen und Ausführen von Dateien, die Aufzeichnung von Tastatureingaben, den Diebstahl von Passwörtern, den Fernzugriff auf den Desktop, die Erstellung von Screenshots, den Diebstahl von Zertifikaten und das Löschen der Festplatte /ITB16r01/, /SEC14w01/

Darüber hinaus hat die ATP-Gruppierung Sandworm Plugins für Linux-Umgebungen geschrieben. Somit wird die Kompatibilität von BlackEnergy 2 von Windows-Betriebssystemen auf Linux-Systeme erweitert. /SEC14w01/

BlackEnergy 2 wurde ab 2010 bei zahlreichen Cyberangriffen eingesetzt, insbesondere Ende 2013 und 2014. Das IT-Sicherheitsunternehmen Kaspersky berichtete für diese Angriffswelle von einer Vielzahl von weltweit verteilten Angriffszielen, unter anderem in Russland, der Ukraine, Polen, Litauen, Weißrussland, Aserbaidschan, Kasachstan, Iran, Israel, der Türkei, Kuwait, Taiwan, Vietnam, Indien, Kroatien, Deutschland, Belgien und Schweden. Als Angriffsziele werden beispielsweise Kraftwerksbetreiber und deren Subunternehmer sowie Hersteller und Zulieferer von Kraftwerkskomponenten und industriellen Steuerungssystemen, aber auch Regierungseinrichtungen, Forschungseinrichtungen, Messstationen, Rettungsdienste und Banken genannt. /SEC14w01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.5.3 Spear-Phishing-Angriff durch ehemaligen U.S. NRC Mitarbeiter

Übersicht

2013 deckte das FBI die Hintergründe eines Spear-Phishing-Angriffs auf Mitarbeiter des U.S. Department of Energy auf. Ein vormaliger Mitarbeiter der U.S. NRC versuchte damit IT-Systeme zu kompromittieren, die sensible Informationen über nukleare Waffen enthalten, um diese Informationen zum Kauf anzubieten. /DOJ16r01/

Beschreibung

Ein ehemaliger Mitarbeiter des Department of Energy (DOE) und der Nuclear Regulatory Commission (NRC) der USA wurde 2010 von der NRC entlassen und griff im Jahr 2015 von den Philippinen aus seine früheren Kollegen beim DOE über eine Spear-Phishing-Kampagne an. Das Ziel des Angriffs war die Infizierung der staatlichen Netzwerke, der Diebstahl von geheimen Daten zu Nuklearwaffen und der Verkauf dieser Daten an ausländische Regierungen. /FED16w01/

Im Jahr 2013 bot er zunächst einer ausländischen Botschaft in Manila 5000 E-Mail-Accounts von DOE-Mitarbeitern, welche nach seinen Aussagen streng geheim waren, zum Verkauf an und verlangte dafür 18800 Dollar. Er sagte den Angestellten der Botschaft, dass falls diese nicht zustimmen würden, er China, dem Iran oder Venezuela das gleiche Angebot machen würde. Man stimmte dem Kauf zu, wobei es sich bei den Angestellten um verdeckt ermittelnde FBI-Agenten handelte. Über eine Zeitspanne von mehr als einem Jahr kauften ihm die Agenten tausende von E-Mail-Accounts ab, welche veröffentlicht werden sollten. Während eines Treffens im Juni 2014 händigte er den Agenten eine Liste von 30000 E-Mails aus und bot ihnen an, einen Spear-Phishing-Angriff gegen das DOE durchzuführen, um noch mehr geheime Informationen zu stehlen. Bei diesem Angriff im Januar 2015 schrieb er eine E-Mail an 80 DOE-Mitarbeiter über eine angeblich bevorstehende Konferenz und bettete darin einen Link ein, den er von einem der FBI-Agenten erhalten hatte und von dem er glaubte, dass er schadhaft sei. Ein Teil der von diesem potenziellen Spear-Phishing-Angriff betroffenen DOE-Angestellten arbeitete in nuklearen Laboren. /FCW16w01, FED16w01/

Als der ehemalige NRC-Mitarbeiter die ihm für den Angriff versprochenen 80000 Dollar abholen wollte, wurde er festgenommen und an die USA ausgeliefert. Er wurde im April 2016 zu einer Haftstrafe von 18 Monaten verurteilt /INF16w01/. Aufgrund der Arbeit

der FBI-Agenten kam es zu keinem Schaden und die sensiblen Informationen blieben geheim. /FED16w01/

Kerntechnischer Bezug

Bei diesem Angriff sollten Unbefugten sensible Informationen über nukleare Waffen zugänglich gemacht und diese an ausländische Regierungen verkauft werden. Durch die Arbeit der verdeckt ermittelten FBI-Agenten konnte dies allerdings verhindert werden.

B.6 2014

B.6.1 Cyberangriff auf südkoreanisches Kernkraftwerk

Übersicht

Im Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines Cyberangriffs in Form eines Informationsdiebstahls wurde. Nach Mutmaßungen der Staatsanwaltschaft in Seoul ist die nordkoreanische Gruppierung Kimsuky für den Angriff verantwortlich, da die eingesetzten Techniken und Angriffsmuster mit denen von Kimsuky übereinstimmen. Weitere Informationen befinden sich in Abschnitt 3.12.8.

Kerntechnischer Bezug

Beim Angriffsziel handelt es sich um einen Kraftwerksbetreiber, der unter anderem auch die südkoreanischen Kernkraftwerke Kori, Shin-Kori, Wolsong, Ulchin und Yeonggwang betreibt.

B.6.2 Cyberangriff auf ein deutsches Stahlwerk

Übersicht

Im Jahr 2014 erfolgte ein Cyberangriff auf ein deutsches Stahlwerk. Dabei kam es zu massiven physischen Schäden an der Anlage. Welche APT-Gruppierung den Angriff durch-geführt hat, ist bislang nicht bekannt. Auch ist derzeit nicht eindeutig bekannt, welche Schadsoftware bei diesem Angriff zum Einsatz kam. /SAN14r01/

Beschreibung

Die Angreifer verschafften sich über eine Spear-Phishing-Kampagne und ausgefeiltes Social Engineering Zugriff auf das Büronetz des Stahlwerks und über dieses wiederum Zugriff auf das OT-Netzwerk des Stahlwerks und die industriellen Steuerungssysteme /BSI14r01/. Die Angreifer verfügten offenbar über fortgeschrittene technische Kenntnisse bezüglich typischer IT-Sicherheitsmaßnahmen und von ICS-Systemen, da es ihnen gelang einen Ausfall mehrerer Systemkomponenten herbeizuführen /BSI14r01/. Da diese in der Folge nicht mehr gesteuert bzw. geregelt werden konnten, kam es zu massiven physischen Schäden, z. B. am Hochofen, der nicht mehr abgeschaltet werden konnte und sich in einem undefinierten Zustand befand /BSI14r01/. Bei den bekannten betroffenen Systemen handelt es sich um Komponenten der industriellen Steuerungen der Anlage aus den Bereichen Lastkontrolle, Lastverteilung, Massen- und Energieausgleich, kinetische Prozessmodelle und Heißluftsystem sowie um den Hochofen selbst. Als mögliche weitere betroffene Systeme werden zentrale Steuerungen, welche über eine speicherprogrammierbare Steuerung (SPS – programmable logic controller, PLC) angesteuert werden, Alarmsysteme, Komponenten der Sicherheitsleittechnik (SIS) und Mensch-Maschinen-Schnittstellen (Human Machine Interface, HMI). /SAN14r01/

Kerntechnischer Bezug

Da es sich um einen sehr gezielten Cyberangriff handelt und das Angriffsziel ein Stahlwerk war, besteht kein direkter Bezug zu kerntechnischen Anlagen.

B.6.3 Havex und Karagany – Erste Angriffswelle durch APT Dragonfly

Übersicht

Bei den Cyberangriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Abschnitt 2.10.5) handelt es sich um hochentwickelte, mehrstufige Angriffe. Die APT-Gruppierung setzt dabei ein breites Spektrum an Angriffswerkzeugen und Schadsoftwarekomponenten ein. Auch verfolgt Dragonfly eine effektive Strategie bei der Kompromittierung von Zielnetzwerken über die Lieferkette.

Beschreibung

Bislang werden Dragonfly zwei Angriffswellen zugeordnet, wobei die erste ihren Höhe-punkt 2013 erreichte und nach ihrer Entdeckung 2014 abflaute. Unabhängig von den eingesetzten Angriffswerkzeugen und Schadsoftwarekomponenten nutzte Dragonfly während der ersten Angriffswelle drei verschiedene Angriffsvektoren /CIS14r01/: Spear Phishing über E-Mail mit kompromittierten pdf-Anhängen, Watering-Hole-Angriffe mit verschiedenen Exploit Kits zur Umleitung von Zugriffen auf legitime Webseiten und die Kompromittierung der Update-Seiten von Herstellern industrieller Steuerungssysteme. /SYM14r01/

Als wesentliche Angriffswerkzeuge und Schadsoftwarekomponenten kamen im Rahmen der ersten Angriffswelle vor allem Havex und Karagany zum Einsatz, wobei es sich bei ersterer um eine maßgeschneiderte, bislang nur von Dragonfly eingesetzte Schadsoftwarekomponente handelt /SYM14r01/. Sowohl Havex als auch Karagany dienen da-zu, auf infizierten Systemen eine Backdoor für Remote-Zugriffe zu etablieren und einen Kanal für die Einschleusung weiterer Schadsoftware sowie das Extrahieren von gesammelten Informationen bereitzustellen.

Havex enthält neben der Komponente zur Etablierung der Backdoor noch eine persistente Komponente, die mit einem Command-and-Control-Server interagiert, um beliebige weitere Schadsoftwarekomponenten nachzuladen und auszuführen sowie ausgespähte Informationen weiterzugeben. Nach erfolgreicher Infektion sammelt Havex auf den kompromittierten Systemen systematisch Informationen, vornehmlich auch solche Informationen, die mit industriellen Steuerungssystemen in Zusammenhang stehen. Die Informationen werden anschließend verschlüsselt and den Command-and-Control-Server gesendet. Zu den Schadsoftwarekomponenten, die Havex typischerweise herunterlädt zählen unter anderem auch Komponenten zur Verschleierung des Angriffs. /SYM14r01/

Es ist derzeit nicht genau bekannt, wie viele Unternehmen von der ersten Angriffswelle betroffen waren, Schätzungen zufolge waren es über 2000 /DRA17r02/. Zu den angegriffenen Unternehmen zählten auch Hersteller industrieller Steuerungssysteme, wie beispielsweise die belgische Firma Ewon /SAN16r01/, welche auf Produkte zur Fernwartung spezialisiert ist /EWO20w01/, die schweizerische Firma MESA Imaging /SAN16r01/, welche optische Instrumente einschließlich Überwachungsgeräten herstellt

und die deutsche Firma MB Connect Line GmbH, welche ebenfalls Fernwartungslösungen anbietet /MBC20w01/.

Kerntechnischer Bezug

Es ist derzeit nicht bekannt, ob auch kerntechnische Anlagen und Einrichtungen von der ersten Angriffswelle betroffen waren. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r11/.

B.6.4 Epic Turla – Globaler Cyberangriff

Übersicht

Bei Epic Turla handelte es sich um eine Angriffswelle zur Cyber-Spionage, die erstmals im März 2014 publik geworden ist, aber vermutlich bereits seit mindestens 2012 lief. Bei der Angriffswelle wurden mehrere hundert Rechner in über 45 Ländern infiziert. Die Angriffe wurden durch die russische APT-Gruppierung Turla (siehe Abschnitt 2.10.13) durchgeführt. Bei den Angriffen handelte es sich um hochentwickelte Angriffe mit dem Ziel der Spionage. Ziele der Angriffe waren Regierungsinstitutionen (Innenministerien, Wirtschaft- und Handelsministerien, Außenministerien, Geheimdienste), Botschaften, militärische Einrichtungen, Bildungseinrichtungen, Forschungsunternehmen und Pharmaunternehmen. Die Opfer befanden sich meist in Europa und im Nahen und Mittleren Osten, aber vereinzelt auch in anderen Regionen, darunter USA und Russland. /ITS21w01/, /SEC14w03/, /KAS21w03/

Laut /BFV16l01/ wird davon ausgegangen, dass es sich um staatlich gelenkte Angriffe gehandelt hat. Darauf deutet die Verwendung hochwertiger Schadprogramme sowie der lange Zeitraum der Angriffsoperationen und der damit verbundene hohe Aufwand an Ressourcen sowie die IT- und Analysekompetenz der Angreifer.

Beschreibung

Bei Epic Turla wurden verschiedene Angriffsvektoren genutzt: Spear Phishing E-Mails mit Adobe-pdf-Exploits, Social-Engineering-Methoden, um das Opfer dazu zu bringen, Malware mit SCR-Dateierweiterung auszuführen, Watering-Hole-Attacken unter

Verwendung von Java-, Flash- oder Internet Explorer-Exploits und auf Social-Engineering fußende Watering-Hole-Attacken, die das Opfer dazu bringen sollten, als Flash Player getarnte Malware auszuführen. Bei den Angriffen wurden mindestens zwei Zero-Day-Exploits ausgenutzt: eine Privilegieneskalations-Sicherheitslücke bei Windows XP und Windows 2003 (CVE-2013-5065) und eine Sicherheitslücke im Adobe Reader, die das Ausführen von beliebigem Code ermöglicht (CVE-2013-3346). /ITS21w01/, /SEC14w03/, /KAS21w03/

Bei der Angriffswelle handelt es sich um eine mehrstufige Infektion. Epic Turla ist dabei die erste Phase der Cyber-Spionage-Kampagne.

In Abhängigkeit von der erkannten IP-Adresse des Opfers stellen die Angreifer Java- oder Browser-Exploits, signierte, aber falsche Adobe Flash Player-Software oder eine gefälschte Version von Microsoft Security Essentials bereits. Außerdem wurden mehr als 100 infizierte Webseiten für Watering-Hole-Attacken entdeckt. Das Öffnen einer mit Malware präparierten Datei (z. B. einer pdf Datei) ruft die Infektion des betreffenden Rechners hervor. Die Schadsoftware ist in der Lage, dem Angreifer die Kontrolle über das System zu verschaffen, Daten zu stehlen und den Netzwerkdatenverkehr mitzuschneiden. Außerdem wird auf den infizierten Systemen eine Backdoor zur Einschleusung weiterer Schadsoftware sowie das Extrahieren von gesammelten Informationen etabliert. Im nächsten Schritt wird dann zielgerichtet Schadsoftware auf den angegriffenen Rechner geladen. Dazu stellt Epic Turla über eine Backdoor eine Verbindung zum Command-and-Control-Server her, um ein Paket mit Systeminformationen des Opfers an die Angreifer zu senden. Dadurch erhält der Angreifer Informationen zum Opfer, auf deren Basis eine Batch-Datei entwickelt wird, die eine Reihe ausführbarer Befehle enthält. Außerdem werden diverse Tools zur Seitwärtsbewegung des Angreifers hochgeladen. Der Kommunikation zwischen Opfersystem und Command-and-Control-Server sind mindestens zwei Ebenen von Proxy-Servern zwischengeschaltet, um den Angreifern die Wahrung der Anonymität zu ermöglichen. Zur Verschleierung des physikalischen Standorts der Angreifer wird zudem satellitengestützte Kommunikation genutzt, die auf dem Kapern von DVB-S-Verbindungen und dem Fälschen von Datenpaketen basiert und damit hochgradig anonym ist. /ITS21w01/, /SEC14w03/, /KAS21w03/, /BFV16l01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Laut /BFV16l01/ zeigte sich anhand der Zielauswahl ein Interesse der Angreifer an Wirtschaft

und Forschung in den Bereichen Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung. Aus diesem Grund ist ein kerntechnischer Bezug nicht auszuschließen.

B.7 2015

B.7.1 BlackEnergy 3 – Cyberangriff auf das ukrainische Stromnetz

Übersicht

Am 23.12.2015 kam es zu einem ungeplanten Ausfall im Stromnetz der Ukraine und zu einem mehrstündigen Stromausfall für ca. 225.000 Kunden. Der Ausfall ereignete sich aufgrund eines Cyberangriffs, bei welchem Systeme von insgesamt drei Energieversorgungsunternehmen erfolgreich angegriffen wurden. Drei weitere Unternehmen wurden ebenfalls angegriffen, ihr Betrieb konnte aber fortwährend weiterlaufen. /CIS16i01/

Beschreibung

Von BlackEnergy sind zurzeit drei Versionen bekannt, BlackEnergy 1, 2 und 3. Erste Versionen von BlackEnergy 1 wurden bereits 2007 aufgefunden. Bei dieser Version der Schadsoftware handelt es sich um ein HTTP-basiertes Botnet zur Durchführung von DDoS-Angriffen. Diese ursprüngliche Version der Schadsoftware wurde durch eine Vielzahl von herunterladbaren Plugins erweitert, darunter Plugins zur Versendung von Spam-Nachrichten und für Betrügereien beim Online-Banking. Dadurch erhielt die Schadsoftware einen modularen Aufbau. Diese Version wurde 2010 erstmalig aufgefunden und ist unter BlackEnergy 2 bekannt.

In der Schadsoftware-Version BlackEnergy 3, die ab 2014 aufgefunden wurde, ist die Anzahl der Plugins wieder stark reduziert worden, weshalb diese Version der Schadsoftware auch als BlackEnergy Lite bezeichnet wird. Deren Plugins und ihre Funktionen beschränken sich im Wesentlichen auf die Auskundschaftung von Netzwerken. Darüber hinaus verfügt BlackEnergy 3 über die Schadsoftwarekomponente KillDisk. Eine spätere, abgewandelte Version bietet zusätzlich die Möglichkeit industrielle Steuerungssysteme zu manipulieren. /ICF16w01/, /ITB16r01/, /SEC10w01/, /SEC14w01/ Beim Cyberangriff auf das ukrainische Stromnetz 2015 wird davon ausgegangen, dass die Angreifer vorher Angriffsschritte zur umfassenden Aufklärung durchführten und dann

mittels Remote-Zugängen auf Büro-IT und Leittechniksysteme zugriffen. Die Systeme wurden mittels der Schadsoftwarekomponente KillDisk angegriffen und für den Betrieb notwendige Daten wurden gelöscht. Auch wurde die Steuerung der unterbrechungsfreien Stromversorgung für die Server angegriffen.

Die vom Cyberangriff betroffenen Betreiber gaben bekannt, dass die Systeme von der Schadsoftware BlackEnergy 3 betroffen waren, aber in welchem Umfang diese Schad-software genutzt wurde, ist bislang nicht klar. Es ist aber sehr wahrscheinlich, dass BlackEnergy 3 bei den Angriffen auf das Stromnetz der Ukraine zumindest eine unter-stützende Rolle spielte, indem die Schadsoftware den Angreifern den Zugriff auf die Computer-Arbeitsplätze und die Netzwerke der Anlagen ermöglichte /CIS16i01/, /ITB16r01/.

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.7.2 GreyEnergy – Cyberangriff auf Stromnetze in Osteuropa

Übersicht

Die Schadsoftware GreyEnergy wurde bei Cyberangriffen gegen kritische Infrastrukturen in Zentral- und Osteuropa eingesetzt, wobei die Angriffs-Ziele hauptsächlich in der Ukraine lagen. Die Schadsoftware weist große Ähnlichkeiten zu BlackEnergy (siehe Abschnitt B.2.1) auf. Gegen Ende des Jahres 2015 erfolgte ein Cyberangriff mit GreyEnergy auf ein Energieversorgungsunternehmen in Polen. Aber auch danach wurde GreyEnergy bei ähnlichen Angriffen eingesetzt, zuletzt wurden Cyberangriffe mit dieser Schadsoftware Mitte des Jahres 2018 bekannt. /ESE18r01/

Beschreibung

Die APT-Gruppierung, die GreyEnergy entwickelt hat, wird von ESET ebenfalls als GreyEnergy bezeichnet und hat nach Einschätzung dieser IT-Analysten vermutlich mit der APT-Gruppierung TeleBots zusammengearbeitet. Das Interesse der APT-Gruppierung GreyEnergy ist auf Industrienetzwerke und kritische Infrastrukturen gerichtet. /ESE18r01/

Der Angriff über die Schadsoftware GreyEnergy kann auf zwei möglichen Angriffswegen erfolgen. Wenn Unternehmen Webdienste zur Verfügung stellen, die über einen Server mit dem internen Netzwerk des Unternehmens verbunden sind, versuchen die Angreifer sich über diesen Weg Zugang zum Firmennetzwerk zu verschaffen.

Der zweite Angriffsweg verwendet Spear-Phishing-E-Mails mit angehängten Word-Dokumenten, die infizierte Makros enthalten /FSE19r02/. Die Schadsoftware GreyEnergy ist modular auf-gebaut. Im Gegensatz zur Schadsoftware Crashoverride (siehe Abschnitt B.8.1) besitzt GreyEnergy kein Modul, das ICS-Systeme direkt beeinflussen kann. Die Module dienen hauptsächlich dazu, das Netzwerk auszukundschaften und Zugangsrechte zu erhalten /BLE18w01/. Stattdessen besitzt die Schadsoftware eine Disk-Wiping-Komponente, um Arbeitsprozesse im betroffenen Unternehmen zu unterbrechen und um die Spuren des Angriffs zu verwischen. Angriffsziele sind ICS-Steuerungsrechner mit SCADA-Software und -Servern /ESE18w01/. Die Infiltrierung der Netzwerke dient vermutlich der Spionage und der Erkundung als Vorbereitung für spätere Angriffe /ZDN18w02/. Eine Version von GreyEnergy wurde mit einem gültigen digitalen Zertifikat gekennzeichnet, das zuvor vermutlich von einer taiwanesischen Firma gestohlen wurde, die ICS-Geräte herstellt. /ESE18r01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.8 2016

B.8.1 Crashoverride/Industroyer – Cyberangriff auf die Stromversorgung in Kiew

Übersicht

Bei der Schadsoftware Crashoverride, die auch als Industroyer bezeichnet wird, handelt es sich um die erste Schadsoftware, die gezielt für Angriffe auf elektrische Stromnetze entwickelt wurde. Mit dieser Schadsoftware können die ICS von Umspannwerken und anderen elektrischen Einrichtungen direkt manipuliert werden. Sowohl Dragos als auch ESET gehen davon aus, dass die Schadsoftware beim Angriff auf das ukrainische Stromnetz am 17.12.2016 zum Einsatz kam, bei dem ein Umspannwerk in Kiew von

einem massiven Cyberangriff betroffen war. Dieser führte zu einem Stromausfall, der über eine Stunde andauerte. /DRA20r01/, /ESE17r01/

Beschreibung

Die Schadsoftware Crashoverride bietet die Möglichkeit, Schalter und Trennschalter in Umspannwerken direkt zu kontrollieren. Beim Angriff auf das Umspannwerk in Kiew wurden die Handlungsoptionen, die Crashoverride den Angreifern bereitstellt, nicht voll ausgeschöpft. Daher geht Dragos davon aus, dass es sich bei diesem Angriff lediglich um einen Test der Schadsoftware gehandelt hat. /DRA20r01/

Crashoverride ist modular aufgebaut und kann daher durch zusätzliche Module erweitert werden. Somit sind nach Einschätzung der Analysten weitere Angriffsmöglichkeiten denkbar. Die wichtigsten Komponenten der Schadsoftware sind eine Komponente zur Etablierung einer Backdoor, ein Launcher, verschiedene Payloads, ein Werkzeug zur Durchführung von DoS-Angriffen und eine Data-Wiper-Komponente, mit der die Angreifer versuchen, ihre Spuren zu verwischen. /DRA20r01/, /ESE17r01/

Der Cyberangriff auf das Umspannwerk in Kiew wird der APT-Gruppierung ELECTRUM (siehe Abschnitt 2.10.6) zugeschrieben, welche nach Einschätzung der Analysten in direkter Verbindung mit der APT-Gruppierung Sandworm (siehe Abschnitt 2.10.11) steht. /DRA20r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wird der Sachverhalt von der GRS auch im Rahmen einer Stellungnahme detailliert ausgewertet.

B.8.2 Mirai – Cyberangriff auf IoT-Systeme

Überblick

Bei Mirai handelt es sich um eine auf IoT spezialisierte Schadsoftware, die gezielt nach smarten Geräten wie beispielsweise Routern, Kameras oder Fernsehgeräten, die über das Internet erreichbar sind, sucht und diese infiziert.

Infizierte Geräte melden sich bei einem Command-and-Control-Server an und werden so Teil eines Botnetzes. Damit können sie von den Angreifern, die das Botnetz kontrollieren, manipuliert und benutzt werden, beispielsweise zur Durchführung von DDoS-Angriffen.

Beschreibung

Infektionen mit der Schadsoftware Mirai können ohne Nutzerinteraktion auftreten, d. h. ohne, dass der Nutzer die Schadsoftware herunterlädt oder ausführt. Laut BSI sind prinzipiell alle IoT-Geräte gefährdet, „die keinen Passwortschutz haben oder ein schwaches Passwort (z. B. Werks-/Standardpasswörter) verwenden“ /BSI20w04/. Vorrangiges Ziel von Mirai sind dabei Linux-basierte Systeme. Infektionen mit Mirai verlaufen typischer-weise unbemerkt. Die Infektion ist nicht persistent, sondern existiert vollständig im flüchtigen Speicher der infizierten Systeme. Daher reicht ein Neustart aus, um die Schad-software zu entfernen. Dieses Vorgehen schützt verwundbare Systeme aber nicht vor einer Reinfektion. /BSI20w04/

Von Mirai existieren mehrere Varianten. Neben der Suche nach und Infizierung von Geräten mit Standardkennungen und -passwörtern gibt es weitere Angriffsvektoren. Bei einer dieser Möglichkeiten werden Router über die für das Kommunikationsprotokoll TR-069 reservierten Ports 7547 und 5555 infiziert. In einer Cyber-Sicherheitswarnung /BSI16i01/ beschreibt das BSI eine Mirai-Version, welche das Kommunikationsprotokoll TR-064 verwendet, das eigentlich für lokale Wartungsarbeiten und die Konfiguration der Router verwendet wird. Die entsprechende Schnittstelle sollte nicht über das Internet erreichbar und durch eine Authentifizierung gesichert sein. Dies ist aber nicht bei allen Gerätetypen gegeben, was einen Zugriff über den Port 7547 ermöglicht. Daher enthalten neuere Versionen des Mirai-Botnetzes Module, die nach offenen TR-069 Ports suchen. /BSI16i01/

Eine weitere Version nutzt eine Debug-Schnittstelle, die bei manchen Android Geräten fälschlicherweise offen ist. Bei den betroffenen Geräten ist die Schnittstelle über den Port 5555 erreichbar und es können ohne Authentifizierung Befehle auf den Geräten ausgeführt und Programme installiert werden. Eigentlich sollte die Schnittstelle deaktiviert sein (und eine Aktivierung sollte nur über eine USB-Verbindung möglich sein). Allerdings ist dies bei nicht allen Geräten der Fall. Betroffen sind dabei verschiedenste Geräte wie Smartphones, digitale Videorekorder oder Fernseher. Bei diesem Angriff scheint das Ziel nicht eine Etablierung eines Botnetzes, etwa zur Vermietung für weitere

Angriffe zu sein, sondern die Geräte zum Generieren von Kryptowährungen zu nutzen. Die Verbindung zu den vorigen Angriffen besteht darin, dass anscheinend eine modifizierte Version des Mirai Codes genutzt wird. /DOU18w01/

Neben den Varianten, die Linux-Systeme als Ziel haben, existiert seit 2017 auch eine Version, die Windows Systeme, insbesondere über ungesicherte SQL-Server, angreift. Ziel dieser Angriffe scheint aber nicht die Infektion der Server, sondern der Zugriff auf die Datenbanken zu sein. Des Weiteren findet auch eine Verbreitung von Mirai durch Windows-Hosts, über bereits bestehende Botnetze, statt. Hierbei werden wie gehabt Linux-Systeme angegriffen, im Unterschied zu früheren Versionen von Mirai kann der Angriff aber auch von einem Windows-Host gestartet werden. /SEC17w01/

Darüber hinaus gibt es noch weitere Varianten, die jeweils verschiedene Angriffspfade benutzen. Gemeinsam ist den Angriffen jeweils das Ausnutzen von Schwachstellen von Geräten, die aus dem Internet öffentlich zugänglich sind.

Durch die Heterogenität der Angriffe und deren Ziele ist es schwer direkte Folgen anzugeben. Die verschiedenen zuvor aufgeführten Angriffe gleichen sich zwar bis zu einem gewissen Grad in der Art des Angriffs und teilen oft auch Teile des Codes (der öffentlich verfügbar ist), jedoch scheint es, als würden die Angriffe mit unterschiedlichen Zielen und wahrscheinlich auch durch unterschiedliche Akteure durchgeführt.

Im Falle der Etablierung eines Botnetzes dient das Netz als Infrastruktur für weitere An-griffe, insbesondere DDoS-Attacken. Der tatsächliche entstandene Schaden hängt nicht nur von den direkten Folgen, sondern vornehmlich auch von den folgenden Angriffen durch das Botnetz ab. Angriffe wurden dabei unter anderem auf die Webseiten von GitHub, Twitter, Netflix, Airbnb, aber auch die deutsche Telekom durchgeführt. /REG16w01/

Mit Hilfe des Mirai-Botnetzes wurden mehrere erfolgreiche DDoS-Angriffe durchgeführt, die alle bis dahin verzeichneten DDoS-Angriffe hinsichtlich ihrer Bandbreite übertrafen. Hierzu zählt neben dem viel beachtete DDoS-Angriff auf den Blog des IT-Sicherheitsspezialisten Brian Krebs im September 2016 (620 Gbps) vor allem der DDoS-Angriff auf das US-Unternehmen Dyn, das zum Zeitpunkt des Angriffs weite Teile der Domain Name System (DNS) Infrastruktur kontrollierte. Letzterer Angriff führte im Oktober 2016 zu einem Zusammenbruch des Internets in weiten Teilen Europas und der USA. /SSL20w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9 2017

B.9.1 Ccleaner Hack – Cyberangriff über schadsoftwarebehaftete Ccleaner Version

Übersicht

Der als Ccleaner Hack bekanntgewordene Cyberangriff war ein spezialisierter Supply-Chain-Angriff, welcher am 13. September 2017 der Öffentlichkeit vorgestellt wurde. Ccleaner ist ein kostenlostes Programm zur Optimierung von Betriebssystemen, welches bis zum 18. Juli 2017 vom IT-Unternehmen Piriform entwickelt wurde und nach dem Kauf Piriforms durch das IT-Sicherheitsunternehmen Avast weiter von Avast entwickelt und angeboten wurde. Ccleaner wurde bis zum bekanntgewordenen Cyberangriff über 2 Milliarden Mal von Nutzern heruntergeladen und ist weltweit verbreitet.

Beschreibung

Die forensischen Untersuchungen haben ergeben, dass ab dem 11. März 2017 IT-Angreifer Zugriff auf die IT-Umgebung des Entwicklers hatten. Die hierfür notwendigen Zugriffsdaten sind womöglich bei einem früheren Cyberangriff entwendet worden. Mit der umfassenden Schadsoftware Shadowpad, welche aus einer Backdoor sowie Manipulationswerkzeugen, die sich dieser Backdoor ermächtigen besteht, griffen die IT-Angreifer auch auf den sogenannten Build-Server des Ccleaner zu. Der Build Server wird in der Softwareentwicklung zur Versionskompilierung verwendet, sodass die IT-Angreifer eigene Ccleaner Versionen entwickeln und auf dem Build-Server unbemerkt platzieren konnten. Schließlich wurde ab dem 2. August 2017 von den Angreifern eine eigene manipulierte Version von Ccleaner auf den Servern von Avast zur Verfügung gestellt, welche bis zum3. September 2017, dem Tag der Entdeckung, über 2 Millionen Mal heruntergeladen wurde. /WIR18r01/

Die manipulierten Versionen von Ccleaner waren für Nutzer und Antivirensoftware nicht direkt erkennbar, da die Programmierer für die Schadsoftware die Zertifikate von

Ccleaner anwendeten und ihre Schadsoftware so in den Programmcode einpflegten, dass keine Abweichungen zu nicht manipulierten Versionen auffielen. Die Schadsoftware wurde mehrstufig aufgebaut, wobei die ersten zwei Stufen der Systemidentifikation dienten und in den manipulierten Versionen von Ccleaner integriert waren. Darauf aufbauend wurde dann die dritte Stufe, die Schadsoftwarekomponente Shadowpad, heruntergeladen und ggf. durch die Angreifer aktiviert. Mit Shadowpad werden z. B. sämtliche Eingaben in gängige Programme ausgelesen, um Passwörter in Erfahrung zu bringen. Shadowpad bietet aber auch die Möglichkeit, weitere Schadmodule herunterzuladen und zu nutzen. Die Command-and-Control-Server der Angreifer wurden am 16. September 2017 von der US-amerikanischen Bundespolizei stillgelegt und es wurde in Erfahrung gebracht, dass auf insgesamt 40 PCs Aktivierungsbefehle für höhere Stufen der Schadsoftware eingegangen waren. Die betroffenen IT-Systeme gehörten zu elf verschiedenen Unternehmen wie Google, Cisco, Intel, Samsung oder Gauselmann. /INS18r01/

Bei Ccleaner Hack handelt sich damit um einen sehr spezifischen Supply-Chain-Angriff, der eine weit verbreitete legitime Software nutzte, um gezielt ausgewählte IT-Systeme mit potenter Schadsoftware unerkannt anzugreifen. Ähnliche Vorgehensweisen wurden in weiteren Cyberangriffen unterschiedlichen Ausmaßes angewendet.

So beim Shadowhammer genannten Cyberangriff 2018 (siehe Abschnitt B.10.1), bei welchem die Angreifer die Kontrolle über die Updateroutinen der Steuerungssoftware des PC-Herstellers ASUSteK Computer Inc. (ASUS) erlangten und über 600 Systeme, identifiziert mittels der MAC-Adresse, mit mehrstufiger Schadsoftware angriffen. /KAS19r01/ Einen ähnlich aufgebauten Cyberangriff, jedoch mit deutlich größerem Ausmaß und Wirkung, stellt der SolarWinds Angriff im Jahr 2020 dar (siehe Abschnitt B.12.4). Bei diesem wurden ebenfalls die Updates einer legitimen Software mit Schadsoftware versehen, jedoch gehören über 18.000 Unternehmen, Behörden, Geheimdienste und weitere kritische Stellen zu den Kunden, welche das mit Schadsoftware versehende Update erhalten haben.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.2 Triton/TriSIS – Cyberangriff auf Petro Rabigh

Überblick

Im Juni und August des Jahres 2017 kam es in einer petrochemischen Anlage in Saudi-Arabien in Folge der Manipulation von Steuerungen von Sicherheits- und Schutzsystemen der Anlage mit der Schadsoftware Triton/TriSIS zu mehreren Schutzabschaltungen von sicherheitsrelevanten verfahrenstechnischen Prozessen /FIR17w01/, /GUT19w01/.

Beschreibung

Bei der breit angelegten forensischen Analyse zu diesem IT-Sicherheitsvorfällen wurde die inzwischen als Triton/TriSIS bekannte Schadsoftware im Image einer dem Safety Instrumented System (SIS) zugeordneten Engineering Workstation gefunden. Zusätzlich wurde unbekannte Software im Speicher aller betroffenen Controller des SIS aufgefunden /GUT19w01/. Ausgehend von der Kompromittierung des SIS und daraus resultierenden potenziellen Auswirkungen auf die Ausführung von Sicherheits-, Sicherungs- und Schutzfunktionen, wurden die rechnerbasierten und programmierbaren Systeme der betroffenen Anlage flächendeckend auf das Vorhandensein weiterer Schadsoftware untersucht /GUT19w01/. Hierbei wurde festgestellt, dass neben dem SIS auch das industrielle Steuerungssystem zur Steuerung des verfahrenstechnischen Prozesses, das in der betroffenen Anlage im Gegensatz zum SIS nicht von Schneider Electric, sondern von einem anderen Hersteller stammte /SCH18w02/, kompromittiert war /MID18w01/, /CON18w01/.

Insgesamt wurde im Rahmen der Untersuchungen zum IT-Sicherheitsvorfall im August des Jahres 2017 festgestellt, dass die Angreifer bereits im Jahr 2014 Zugriff auf das Anlagennetzwerk erlangt und sich fortan schrittweise langsam und unentdeckt im Anlagennetzwerk ausgebreitet hatten. /MIT19w01/

Aus den der GRS vorliegenden Informationen geht hervor, dass es sich bei Triton/TriSIS um eine hochentwickelte Schadsoftware handelt, die ähnlich wie Stuxnet, Havex, BlackEnergy und Industroyer/Crashoverride auf industrielle Steuerungssysteme (Industrial Control Systems, ICS) von kritischen Infrastrukturen ausgerichtet ist. Im Unterschied zu den genannten Vertretern von ICS-angepasster Schadsoftware, die vor allem auf die Manipulation industrieller Steuerungssysteme zur Prozesssteuerung ausgerichtet sind,

zielt Triton/TriSIS jedoch als bisher einzige bekannt gewordene Schadsoftware auf die Manipulation derjenigen industriellen Steuerungssysteme, die Sicherheits-, Sicherungs- oder Schutzfunktionen ausführen und entsprechende Schutzaktionen auslösen (SIS, Safety Instrumented System). Mit Hilfe von Triton/TriSIS sind daher nicht nur Beschädigungen von Komponenten oder die Abschaltung industrieller Prozesse denkbar, sondern prinzipiell auch die Manipulation von SIS bei gleichzeitiger Herbeiführung von unsicheren Anlagenzuständen. Die Schadsoftware Triton/TriSIS deckt hierbei nicht den gesamten Cyberangriff ab, sondern stellt einen wesentlichen Baustein innerhalb eines komplexen, mehrstufigen Cyberangriffs dar.

Hierbei beschränken sich die Möglichkeiten von Triton/TriSIS nicht auf die Verhinderung des Eingriffs von Systemen, die Sicherheits-, Sicherungs- oder Schutzfunktionen aus-führen, oder die Herbeiführung einer Fehlauslösung solcher Funktionen. Die Schadsoftware Triton/TriSIS ist vielmehr auf die Einrichtung einer Backdoor innerhalb von Controllern eines SIS ausgerichtet, welche den Angreifern erlaubt, die uneingeschränkte und unbemerkte Kontrolle über das SIS zu erlangen und heimlich beliebige Manipulationen an Sicherheits-, Sicherungs- oder Schutzfunktionen mit sehr ernsten potenziellen Auswirkungen durchzuführen. /MID18w01/, /FIR19w01/, /DRA19r01/

Zwischenzeitlich wurden ein weiterer IT-Sicherheitsvorfall im Zusammenhang mit Triton/TriSIS (siehe Abschnitt B.11.3) und weitere Aktivitäten der Angreifer bekannt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r01/. Zudem wurde die Weiterleitungsnachricht 2021/01 verfasst /GRS21i01/.

B.9.3 Karagany.B und Heriplor – Zweite Angriffswelle durch APT Dragonfly

Übersicht

Bei den Cyberangriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Abschnitt 2.10.5) handelt es sich um hochentwickelte, mehrstufige Angriffe /BSI20i01/. Die APT-Gruppierung setzt dabei ein breites Spektrum an Angriffswerkzeugen und Schadsoftwarekomponenten ein. Auch verfolgt Dragonfly eine effektive Strategie bei der Kompromittierung von Zielnetzwerken über die Lieferkette einzelner Systeme.

Beschreibung

Bislang werden Dragonfly zwei Angriffswellen zugeordnet. Die zweite Angriffswelle wird ab 2015 ausgemacht und erreichte 2017 einen vorläufigen Höhepunkt, dauert aber nach wie vor an /SYM14r01/, /BSI20i01/ (für Informationen zur ersten Angriffswelle siehe Abschnitt B.6.3, für Informationen zur APT-Gruppierung Dragonfly siehe Abschnitt 2.10.5). Auch bei diesen Angriffen handelt es sich um mehrstufige, komplexe Angriffe, die anschließend an erste Aufklärungsschritte zunächst Spear Phishing und Watering-Hole-Techniken nutzen. Darauf aufbauend setzen die Angreifer eine Vielzahl an Methoden ein, um Remote Zugriff auf die Zielnetzwerke zu erlangen und sich dort weiter auszubreiten. Berichtet wird hierzu beispielsweise von Man-in-the-Middle Angriffen, Passwort Cracking Methoden, Credential Harvesting und Brute-Force-Angriffen auf Fernwartungsprotokolle. Zur Einschleusung von Schadcode nutzen die Angreifer beispielsweise kompromittierte LNK-Dateien. Auch wird vom unautorisierten Einsatz von Red Team Tools[23] zur weiteren Ausbreitung im Zielnetzwerk, der Manipulation von Firewalls zur Etablierung von dauerhaften Remote-Zugriffen und unautorisierten Änderungen der Konfiguration der Netzwerkkomponenten zur Umleitung des Datenverkehrs über von den Angreifern kontrollierte Systeme berichtet. /BFV18r01/

[23] Bei Red Teams handelt es sich um IT-Sicherheitsspezialisten, die zur Überprüfung von IT-Systemen Sicherheits- und Penetrationstests ausführen und dabei die Perspektive echter Angreifer einnehmen.

Nach Erlangung und Verfestigung des entsprechenden Zugriffs setzen die Angreifer beispielsweise Schadsoftwarekomponenten zur Etablierung von Backdoors ein, auch mehrere parallel. Konkret genannt werden verschiedene Schadsoftwarekomponenten wie Godoor, Dorshel, Karagany.B und Heriplor /SYM17r01/. Wie bei Havex (siehe Abschnitt B.6.3) handelt es sich bei Heriplor um eine maßgeschneiderte Schadsoftware, die anderen Angreifergruppierungen bislang nicht zugänglich ist. Analysten gehen davon aus, dass Heriplor auf Basis des Codes von Havex entwickelt wurde /SYM17r01/, /SEC19w02/. Bei Karagany.B handelt es sich um eine Weiterentwicklung der bei der ersten Angriffswelle eingesetzten Schadsoftwarekomponente Karagany. Neben diesen Schadsoftwarekomponenten verwendeten die Angreifer für die einzelnen Angriffsschritte noch weitere, maßgeschneiderte Angriffswerkzeuge sowie frei oder kommerziell verfüg-bare Werkzeuge /CIS18r01/. Darüber hinaus bedient sich die APT-Gruppierung sogenannter Living-off-the-Land-Techniken, bei denen legitime im Anlagennetzwerk vorhandene Systeme für maliziöse Handlungen eingesetzt werden /BSI20i02/.

Häufig greifen die Angreifer die anvisierten Ziele nicht direkt an, sondern kompromittieren zunächst geeignete Zwischenziele in der Lieferkette.

Bei den anvisierten Zielen liegt der Fokus der Angreifer nach bisherigen Erkenntnissen auf dem systematischen Ausforschen der Zielnetzwerke. Hierbei werden gezielt Informationen über Nutzer, Hosts und die Netzwerkumgebung gesammelt und aufgelistet. Auch werden Nutzeraktivitäten erfasst, einschließlich aktueller Bildschirminhalte. Die Angreifer erfassen insbesondere auch Informationen zu den industriellen Steuerungssystemen wie Konfiguration und Zugriffsinformationen sowie Informationen zu deren Bedienung einschließlich der Erfassung von Screenshots während des Betriebs. /CIS18r01/

Im Rahmen der zweiten Angriffswelle werden vornehmlich Unternehmen im Energiesektor einschließlich der kerntechnischen Industrie sowie der Öl- und Gasindustrie angegriffen. Die Angriffe konzentrieren sich auf Unternehmen in Europa und den USA, betroffen sind aber auch einige asiatische Länder /CYC18w01/. Das BSI berichtet, dass es im Rahmen der zweiten Angriffswelle durch Dragonfly auch zur Kompromittierung von Unternehmen in Deutschland gekommen ist /BSI20i01/.

Kerntechnischer Bezug

Im Rahmen der zweiten Angriffswelle kam es auch zu mindestens einem Angriff auf eine kerntechnische Anlage. Betroffen war das US-amerikanische Kernkraftwerk Woolf Creek. In einer ersten Reaktion gab die Anlage an, die möglichen Auswirkungen des Angriffs sei auf administrative und geschäftliche Teile des Anlagennetzwerks beschränkt, die Untersuchungen seien aber noch nicht abgeschlossen /NYT17w01/. Aus Sicht der GRS besteht eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r11/.

B.9.4 WannaCry – Globaler Cyberangriff

Übersicht

Ab dem 12. Mai 2017 infizierte die Ransomware mit dem Namen WannaCry, WCry, WannaDecryptor Computer weltweit. WannaCry ist eine Schadsoftware, die von Erpressern eingesetzt wird, um Computerdateien zu verschlüsseln und für die Entschlüsselung Lösegeld (engl. ransom) in Form von Bitcoins zu fordern /CIS17i02/.

Beschreibung

WannaCry greift Rechner mit dem Windows Betriebssystem an, wobei die Malware eine Schwachstelle im Windows Server Protokoll nutzt. Dabei waren in der überwiegenden Mehrheit (98 %) Computer mit dem Betriebssystem Windows 7 betroffen, die das wenige Wochen zuvor zur Verfügung gestellte Patch der Schwachstelle noch nicht eingespielt hatten /HEI17w01/. Zum damaligen Zeitpunkt war Windows 7 das am meisten genutzte Betriebssystem noch vor Windows 10. Etwa 0,1 % der Infektionen betrafen das veraltete Betriebssystem Windows XP. Laut Microsoft wurden keine Windows 10 Rechner von WannaCry infiziert /MIC17r01/.

Zunächst wurde angenommen, dass die initiale Infektion eines Computernetzwerkes über E−Mails mit maliziösem Anhang oder Link erfolgt, wie es für Ransomware typisch ist. Es zeigte sich jedoch, dass die initiale Infektion eines Computers über einen Angriff auf den Server aus dem Internet erfolgt, indem eine Schwachstelle im Windows Server Protokoll SMBv1 (Server Message Block) (CVE-2017-0144 /NVD18w01/) ausgenutzt

wurde. Der Server Message Block ist ein Netzwerkprotokoll von Microsoft für Zugriffe auf Dateien und Serverdienste in Rechnernetzen /BSI17i01/.

Sobald ein Rechner mit der Schadsoftware befallen ist, kann sich WannaCry weiter über lokale Netzwerke ausbreiten, da WannaCry laut Microsoft entsprechende Wurmeigenschaften besitzt. Aufgrund dieser Eigenschaft konnte sich WannaCry sehr schnell verbreiten und durch eine initiale Infektion eines Rechners im Netzwerk das gesamte Netz-werk kompromittieren /MIC17r01, BSI17i01/.

Der erste Schritt bei einer Infektion mit WannaCry erfolgt über eine eigenständig aus-führbare Programm Datei (sog. Dropper), welche das Exploit EternalBlue verwendet. EternalBlue nutzt die oben genannte Sicherheitslücke des Protokolls SMBv1, um sich Zugang zum Computersystem zu verschaffen (nähere Informationen s. u.) /CIS17r01/, /MAL17w01/. Dieser Dropper enthält einen sog. Killswitch, der von den Entwicklern als eine Art Notausschalter programmiert wurde, um die Schadsoftware zu stoppen. Dabei schickt der Dropper eine Anfrage an eine Internetseite (www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). Kann eine Verbindung zu dieser Seite hergestellt werden, wird der Dropper nicht weiter ausgeführt und die Infektion des Computers wird gestoppt /CIS17r01/, /HEI17w03/, /MAL17w01/. Erfolgt keine Verbindung, wird der Computer mit der Schadsoftware infiziert, indem ein Service (mssecsvc2.0) gestartet wird, der alle IP−Adressen des lokalen Netzwerkes des infizierten Computers scannt und versucht, sich mit dem TCP Port 445 (SMB) jeder IP−Adresse zu verbinden. Gelingt es der Malware, unter der Ausnutzung der SMBv1 Schwachstelle auf einen Rechner zu gelangen, wird eine ausführbare Datei auf dem System installiert. Die ausführende Datei tasksche.exe sucht Dateien auf der Festplatte, den Netzlaufwerken und den Wechselspeichergeräten, die dann mit einem kryptographischen Verfahren verschlüsselt werden. Dabei können etwa 120 unterschiedliche Dateiformate verschlüsselt werden, darunter Text-, Audio-, Video- und Bilddateien. Zudem werden durch zwei weitere ausführbare Dateien taskdl.exe und taskse.exe alle temporären Dateien (mit denen eine Wiederherstellung der Dateien möglich wäre) gelöscht und eine Bildschirmanzeige mit der Lösegelderpressung angezeigt /CIS17r01/. Die von WannaCry ausgenutzte Sicherheitslücke SMBv1 wurde vom US-amerikanischen Auslandsgeheimdienst (NSA) entdeckt und mit dem Zero-Day-Exploit EternalBlue SMBv1 über drei Jahre lang verwendet ohne Microsoft über die Schwachstelle zu informieren. Erst als dieses Wissen von der Angreifergruppierung Shadow Brockers gestohlen wurde, informierte die NSA Microsoft über die Sicherheitslücke /NYT17w02, HEI17w04/.

Daraufhin wurde am 14. März 2017 ein Patch für Windows Vista, Windows 7, Windows 8.1, Windows 10 sowie Windows Server 2008 zur Verfügung gestellt. Später folgten auch Patches für Windows XP, Windows 8 und Windows Server 2003.

Betroffen von den Cyberangriffen mit der Ransomware WannaCry waren laut Medienberichten Computer unterschiedlicher Organisationen in über 150 Ländern, u. a. Deutschland, Frankreich, Großbritannien, Japan, Russland, Spanien, Taiwan und USA. Darunter sind das Innenministerium in Russland mit 1000 infizierten Rechnern, der National Health Service in Großbritannien (NHS), wodurch in vielen Krankenhäuser die Behandlung von Patienten erheblich beeinträchtigt wurde /BSI17i01/, /HEI17w05/, /MAL17w01/. Die Autohersteller Nissan (in Großbritannien) und Renault (in Frankreich), der Flugzeughersteller Boeing, die Netzbetreiber Telefónica (in Spanien) und Telecom (in Portugal), das Logistikunternehmen FedEx (USA) und sowie die Deutsche Bahn, deren Anzeigetafeln und Fahrscheinautomaten betroffen waren. /HEI17w05/, /HEI17w06/, /SEA17w01/

Laut Forbes /FOR17w01/ waren auch zahlreiche medizinische Einrichtungen in den USA betroffen. Dabei waren nicht nur Bürorechner infiziert, sondern auch medizinische Geräte, auf denen das Microsoft Betriebssystem lief und die sich im Netzwerk befanden. Als Beispiel wurde ein Überwachungssystem zur Injektion von Kontrastmittel bei Magnetresonanztomographie von Bayer genannt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.5 Bad Rabbit – Globaler Cyberangriff

Übersicht

Im Oktober 2017 wurde bekannt, dass osteuropäische Unternehmen und Behörden vor allem in der Ukraine und Russland Opfer einer Angriffswelle mit der Ransomware Bad-Rabbit wurden. Betroffen waren unter anderem eine russische Nachrichtenagentur, die U-Bahn in Kiew und der Flughafen in Odessa. Es folgten außerdem weitere Cyberangriffe auf Ziele in mehreren europäischen Staaten (darunter Deutschland), Japan, den USA und weiteren Staaten.

Die Ransomware gelangte vermutlich über Watering-Hole-Angriffe, bei denen von Zielpersonen besuchte Webseiten mit Schadsoftware infiziert waren, auf die Systeme der Opfer. Dabei wurden die Opfer über ein manipuliertes Skript zur angeblichen Installation bzw. zum Update des Adobe Flash-Players aufgefordert, woraufhin die Schadsoftware auf das System des Opfers gelangte und mit der Verschlüsselung der Daten begann. /AIR17w01/, /TRE17w01/

Beschreibung

Nachdem die Schadsoftware BadRabbit auf das Zielsystem gelangt ist, nutzt sie das frei verfügbare Angriffswerkzeug Mimikatz, um die lokalen Anmeldeinformationen der Benutzer oder Administratoren zu extrahieren. Dabei handelt es sich um ein für Cyberangriffe oftmals verwendetes Programm, welches verwendet werden kann, um bei Windows-Systemen unter Ausnutzung einer Schwachstelle an zwischengespeicherte Anmeldeinformationen zu gelangen. Mimikatz wurde u. a. beispielsweise beim NotPeyta-Angriff im Jahr 2017 eingesetzt. BadRabbit nutzt anschließend das frei verfügbare Programm DiskCryptor, um die Daten des infizierten Systems zu verschlüsseln. Die Verschlüsselung umfasst die meisten gängigen Dateitypen wie beispielsweise Microsoft Office Dateien, PDF-Dateien und Bilddateien. Außerdem wird der Master Boot Record (MBR) verschlüsselt, der das Startprogramm für BIOS-basierte Computer enthält. Nachdem die Daten verschlüsselt wurden, startet BadRabbit das System neu und das Opfer bekommt eine Lösegeldforderung angezeigt, indem eine Zahlung in Bitcoins verlangt wird, um die Daten entschlüsseln zu können. Die Schadsoftware ist in der Lage, sich über das Netz-werk im System des Opfers zu verbreiten und so weitere Computer zu infizieren. Dabei wird unter anderem eine modifizierte Version des Exploits Eternal-Romance genutzt. /AIR17w01/, /TRE17w02/

Die Behörde für nationale Cybersecurity des Vereinigten Königreichs, das National Cyber Security Centre (NCSC), vermutet, dass die APT-Gruppierung Sandworm (siehe Abschnitt 2.10.11) für die Cyberangriffe mit der Ransomware BadRabbit verantwortlich ist /NCS18i02/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.6 NotPetya – Cyberangriffe auf ukrainische Behörden, Infrastruktur und weltweite Unternehmen

Übersicht

Am 27. Juni 2017 waren weltweit Unternehmen und Organisationen von einem massiven Ausfall ihrer Informationsinfrastruktur betroffen, nachdem unbekannte Angreifer bereits im Frühjahr 2017 Zugriff auf die Server des Unternehmens Linkos Group erlangt und unbemerkt die Kontrolle über die Updateserver für das Programm M.E.Doc des Unternehmens übernommen hatten. M.E.Doc ist eine in der Ukraine weit verbreitete Software zur Unterstützung der Erstellung von Steuerabrechnungen und -erklärungen, welche von vielen in der Ukraine tätigen ausländischen Unternehmen und Konzerntöchtern verwendet wird. Der NotPetya-Angriff erfolgte somit über die Lieferkette. Hauptsächlich galt der Angriff Firmen und Regierungsbehörden in der Ukraine, darunter die Post, das Metrosystem in Kiew, ukrainische Banken und das ukrainische Stromnetzunternehmen Kievenergo. Das Kernkraftwerk Tschernobyl war ebenfalls betroffen, bei dem infolge des Cyberangriffs die Strahlungsüberwachung manuell durchgeführt werden musste. Besonders betroffen von dem Cyberangriff war außerdem das dänische Logistikunternehmen Maersk. /CNN17w01/, /NYT17w03/, /GUA17w01/

Beschreibung

Die Angreifer luden auf die betroffenen Systeme per Softwareupdate die Schadsoftware NotPetya hoch und aktivierten diese zeitgleich am 27. Juni 2017. Diese Schadsoftware, auch unter dem Namen Wiper geführt, wird teilweise der Schadsoftware Petya, einem klassischen Verschlüsselungstrojaner, zugeordnet, unterscheidet sich aber in wesentlichen Punkten fundamental von diesem.

Beispielsweise ist das Ziel beim NotPetya-Angriff keine Lösegeldzahlung der Opfer, sondern die Verschlüsselung der Daten der Opfer ohne Möglichkeiten der Entschlüsselung, sodass die betroffenen Daten verloren und die Systeme unzugänglich sind. Die Schadsoftware NotPetya breitete sich in den betroffenen IT-Netzwerken aus, vernichtete sämtliche gespeicherte Daten der betroffenen Systeme und versuchte, weitere IT-Systeme zu infizieren. IT-Analysten rechnen den Angriff dem russischen Militär zu, mit dem Ziel, Schadsoftware auf den Computern der ukrainischen Regierung und Unter-nehmen zu installieren. Durch die Aktivitäten internationaler Unternehmen in der Ukraine, konnte sich die Schadsoftware dann verbreiten.

Innerhalb weniger Tage entstand weltweit ein wirtschaftlicher Schaden von mehreren Milliarden Dollar. Die Schadsoftware verwendet das aus dem Arsenal der National Security Agency (NSA) der USA gestohlene Angriffswerkzeug EternalBlue, welches eine Microsoft Windows Schwachstelle ausnutzt. /CNN17w01/, /NYT17w03/, /BUS17w01/, /CNE18w01/

Ein umfassendes Beispiel der Schadwirkung von NotPetya ist die Zerstörung des Firmennetzwerkes bei dem Logistikunternehmen Maersk. Eine Niederlassung von Maersk in der Ukraine nutzte die Software M.E.Doc für ihre Abrechnungen. Von dort ausgehend verbreitete sich NotPetya im gesamten Netzwerk des Unternehmens, das aus über 80.000 IT-Systemen besteht. Jedes IT-System wurde infiziert und dessen gespeicherte Dateien unwiderruflich zerstört. Die weitere Ausbreitung der Schadsoftware umfasste u. a. das französische Baustoffunternehmen Saint-Gobain, die britische Werbeagentur WPPGY, die russischen Unternehmen Rosneft (Öl und Gas), Gazprom (Gasunternehmen) und die Bank Home Credit, das Stahl- und Bergbauunternehmen Evraz, das Gesundheitsunternehmen Heritage Valley Health Systems in Pennsylvania, die globale Transportfirma FedEx, das Pharmaunternehmen Merck, das Unternehmen Mondelez (MDLZ) (dem weltweit Unternehmen zur Herstellung von Süßwaren wie Oreos und Cadbory angehören) und die Anwaltskanzlei DLA Piper. /CNN17w01/, /NYT17w03/

Kerntechnischer Bezug

Mit dem Ausfall der Strahlungsüberwachung im Kernkraftwerk Tschernobyl, welche daraufhin manuell durchgeführt werden musste, hat der Cyberangriff einen direkten Bezug zu kerntechnischen Anlagen. /PRV17r01/

B.10 2018

B.10.1 Shadowhammer – Cyberangriff über schadsoftwarebehaftete ASUS Steuerungssoftware

Übersicht

Bei dem als Operation Shadowhammer genannten Cyberangriff handelt es sich um einen typverwandten oder womöglich Nachfolgeangriff zum beschriebenen Ccleaner Cyberangriff (siehe Abschnitt B.9.1).

Im März 2019 veröffentlichte Kaspersky Labs zu einem bis dahin unbekannten Supply-Chain-Angriff einen umfassenden Bericht, welcher das unter dem Markennamen ASUS auftretende Unternehmen ASUSTeK Computer Inc. betraf.

Beschreibung

Im Verlauf des Jahres 2018 sicherten sich die IT-Angreifer Zugriff auf die Webseite von ASUS, auf welcher dieser eine Steuerungssoftware für seine Kunden zum Herunterladen anbietet. Die IT-Angreifer platzierten beginnend im Juni 2018 unbemerkt eine mit Schadcode versehende Version auf der Webseite. Diese manipulierte Version wurde mit legitimen Zertifikaten ausgestattet und so an Kunden des Unternehmens verteilt. Nach bisherigen Erkenntnissen lief der Cyberangriff vom Juni 2018 bis November 2018 und wurde dann am 29. Januar 2019 entdeckt. /SEN19r01/

Ähnlich zum Ccleaner Cyberangriff diente die initiale Schadsoftwarekomponente aus-schließlich der Identifizierung der betroffenen IT-Systeme. Die IT-Angreifer nutzen eine Liste von insgesamt 600 eindeutig zu identifizierenden MAC Adressen unbekannter Herkunft zur Erkennung von IT-Systemen, bei welchen die zweite Schadsoftwarekomponente zum Einsatz kommen sollte. Diese zweite Schadsoftwarekomponente ähnelte der beim Ccleaner Hack eingesetzten Shadowpad Schadsoftware. Zu den Opfern gehören neben ASUS selbst insbesondere IT-Unternehmen aus der Republik China und den USA. /SEN19r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.2 Cyberangriff auf den französischen Baukonzern Ingérop

Übersicht

Im November 2018 wurde bekannt, dass Daten des französischen Baudienstleisters Ingérop, der für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo arbeitet, zunächst teilweise im Internet aufzufinden waren und anschließend ein aus 11.000 Dateien bestehendes Archiv im Darknet angeboten wurde.

Darunter befinden sich nach aktuellem Kenntnisstand auch Daten über französische kerntechnische Anlagen. Nach bisherigen Erkenntnissen wurde Ingérop im ersten Halbjahr 2018 Opfer eines Phishing-Angriffs, bei welchem ein oder mehrere Mitarbeiter des Konzerns mittels fingierter Emails zur Installation einer bisher nicht bekannten Schad-software verleitet wurden.

Kerntechnischer Bezug

Der französische Baudienstleister Ingérop, der Opfer des Phishing-Angriffs wurde, arbeitet für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo.

B.10.3 Emotet – Globale Cyberangriffe auf Behörden und Infrastruktur

Übersicht

Bei Emotet handelt es sich um eine erstmalig 2014 beschriebene Schadsoftware des Typs Ransomware mit hohem Schadpotenzial. Emotet zielt hierbei jedoch nicht auf Privatanwender, sondern wurde von seinen Entwicklern immer weiter spezialisiert, um große Firmennetzwerke gezielt angreifen zu können. Aufgrund der rasant gestiegenen Schadwirkung und Fähigkeiten der Emotet-Schadsoftware veröffentlichte das BSI im Jahr 2018 eine Warnmeldung bezüglich Emotet /BSI20r04/. Betroffen waren Krankenhäuser, Stadtverwaltungen, das Medienunternehmen Heise Gruppe, das Berliner Kammergericht, der BwFuhrparkservice und damit der Fahrdienst des Deutschen Bundestages und viele weitere Unternehmen, Institutionen und Verwaltungen in Deutschland und anderen Nationen. /SOP19r01/, /TON20r01/

Beschreibung

Die Gefährlichkeit der Emotet-Schadsoftware nahm im Jahr 2018 insbesondere durch neuere Emotet-Versionen zu, welche in der Lage waren, Emails betroffener IT-Systeme auszulesen und unter Hilfe der ausgelesenen Emails täuschend echte Emails mit kompromittiertem Anhang zu versenden oder gar auf bestehende Emails zu antworten. Empfänger solcher Emails wurden häufig durch die legitimen Titel, Absender, Inhalte und Bezeichnung des Anhangs dazu geführt die zur Installation von Emotet notwendigen Schritte (Herunterladen der Word-Datei im Anhang, Erlaubnis von Word-Makros) durch-zuführen.

Wird Emotet auf einem IT-System ausgeführt, beginnt Emotet umfassende Auswertungen von Eingaben, Auslesung von Emails sowie die eigene Weiterverbreitung über angeschlossene Netzwerke und Emailversendungen. Emotets Kernfunktion ist hierbei die Verschlüsselung sämtlicher angeschlossener Massenspeicher aller betroffener IT-Systeme. Hierdurch kommt es zum Teil zu vollständigen Ausfällen der Netzwerkinfrastruktur oder gar aller vernetzter IT-Systeme der betroffenen Opfer. Einen Schlüssel zur Entschlüsselung erhielten die Opfer nur nach Zahlung einer hohen Geldsumme an die IT-Angreifer. Emotet wurde konstant weiterentwickelt und wurde mit hoher Schadwirkung bis Ende 2020 eingesetzt. /SOP19r01/

Anfang 2021 gelang den deutschen Sicherheitsbehörden BSI und BKA die vollständige Übernahme der Command-and-Control-Server von Emotet. Hierdurch war es den Behörden möglich, die Tätigkeiten von Emotet zunächst zu unterbinden. So wurde über die Command-and-Control-Server ein spezielles Update an alle aktiven Emotet-Versionen versendet, welches zum einen die Emotet-Schadsoftware „quarantänisiert“ und damit inaktiviert, zum anderen aber auch für Antivirensoftware einfach erkennbar macht. Weiterhin wurde die Kommunikation zu einem direkt von den Strafverfolgungsbehörden kontrollierten Server umgeleitet und die Besitzer mit Emotet infizierter Systeme wurden aktiv kontaktiert. Nach Übernahme der Command-and-Control Server von Emotet wurde da-von auszugegangen, dass die Aktivitäten von Emotet stark zurückgehen werden und immer mehr Systeme von der Schadsoftware bereinigt werden. /BSI21r01/, /BIT22w02/

Tatsächlich wurden zwischen Januar 2021 und November 2021 keine Emotet Aktivitäten mehr entdeckt. Seit dem vierten Quartal 2021 sind wieder große Angriffswellen unter Nutzung oder Beteiligung der Schadsoftware Emotet und der ihr zugehörigen Emotet-Gruppe entdeckt worden. Hierbei wurden Emotet Funktionen zum einen in die Malware Trickbot übernommen und zum anderen kommt es seit November 2021 zu wiederholten schwerwiegenden Angriffsserien durch Emotet, wobei wieder Emails mit manipulierten Anhängen oder Weblinks zur Verbreitung von Emotet eingesetzt werden. Basierte die Übertragung früher zumeist auf der Nutzung von Macro-Funktionen von MS Office Produkten, hat sich der Angriffsvektor vermehrt zur Ausführung von gefälschten Apps verschoben, z. B. PDF-Lesern sowie Java-Archiven und für Webseitenfunktionen wichtige Javascripts. Die aktuellen weltweiten Infektionswellen mit Emotet zeigen, dass aktuell durch Emotet insbesondere der Abfluss verwertbarer Informationen wie E-Mail-Passwörter, Kontakte und andere Zugangsdaten als Kernfunktion durchgeführt wird und damit von den betroffenen IT-Systemen neuer glaubwürdiger E-Mail Spam

verschickt wird. Einige Emotet-Versionen besitzen die Möglichkeit zum Nachladen von weiteren Schadsoftwares. Gemäß einer Auswertung des IT-Systemherstellers und Dienstleisters HP Inc. ist im ersten Quartal 2022 zu einer 27-fachen Steigerung der Anzahl an Emotet Identifikationen gegenüber dem letzten Quartal 2021 gekommen, womit Emotet zur häufigsten identifizierten Schadsoftware durch HP wurde. /HPW22w01/, /BIT22w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.4 Operation Sharpshooter – Globale Cyberangriffe auf Behörden und Infrastruktur

Übersicht

Operation Sharpshooter wird eine große, international wirkende Angriffsserie professioneller Art genannt, welche von McAfee Global Threat Intelligence 2018 der Öffentlichkeit vorgestellt wurde und im Rahmen eines großen Berichts näher beleuchtet wurde /MCA18r01/. Die Kampagne zielte auf Unternehmen und Behörden im Bereich der kritischen Infrastruktur sowie im Verteidigungsbereich ab. Dabei nutzten die Angreifer beim Cloudspeicheranbieter Dropbox hinterlegte Worddokumente mit Schadcode, welcher mittels Word Macros ausgeführt wurde. Über die Macros wurden dann Alibi-Worddokumente erzeugt, welche zum Herunterladen der eigentlichen Schadsoftware mit dem Namen Rising Sun verwendet wurden. Rising Sun wird zum einen zum Ausspähen von Netzwerken, Computernamen, Nutzernamen, IP-Adressen, Systeminformationen und anderen Informationen verwendet und zusätzlich ist die Schadsoftware in der Lage die gesammelten Daten an einen Command-and-Control-Server zu übertragen und damit zu entwenden. /MCA18r01/

Die beim Angriff hinterlassenen Spuren deuten darauf hin, dass die ATP Lazarus in dieser Angriffsserie involviert ist. Dies ist jedoch keine sichere Erkenntnis, sondern basiert auf Indizien, die auch für die Verwischung der Spuren von IT-Angreifern absichtlich platziert sein könnten. /MCA18r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.5 Shamoon v3 – Cyberangriff auf Saipem

Übersicht

Ende des Jahres 2018 wurde eine weitere Variante der Shamoon Schadsoftwarefamilie, Shamoon v3, entdeckt.

Beschreibung

Ziel des Angriffs mit Shamoon v3 war das italienische Öl- und Gasunternehmen Saipem. Angaben von ZDNet zufolge waren etwa 10 % der gesamten Rechnerinfrastruktur von Saipem betroffen, Infektionen wurden sowohl im Mittleren Osten als auch in Italien, In-dien und Spanien vermeldet. Im Gegensatz zu den ersten beiden Angriffen mit Shamoon 2012 und 2016 wurden die Daten auf den betroffenen Rechnern diesmal nicht mit Bilddaten, sondern mit zufälligen, nicht zusammenhängenden Daten überschrieben. /ZDN18w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11 2019

B.11.1 IT-Sicherheitsvorfall durch Cryptomining in KKW Südukraine

Übersicht

Wie die ukrainische Nachrichtenplattform InternetUA im August 2019 berichtete, wurde am 10. Juli 2019 vom ukrainischen Geheimdienst SBU der Verwaltungstrakt des Kern-kraftwerks Südukraine durchsucht. Dabei wurden mehrere IT-Systeme beschlagnahmt, welche für die Generierung (sogenanntes Mining) von digitalen Währungen wie Bitcoins verwendet wurden.

Beschreibung

Digitale Währungen (auch Kryptowährungen genannt) wie Bitcoin oder Dogecoin basieren bei ihrer Generierung auf hochkomplexen Gleichungen, welche mittels stromintensiver Grafikkarten gelöst werden. Die Stromkosten sind daher eine der einflussreichsten Grenzkosten des Minings, wodurch es bereits zu wiederholten Strom- und Rechenzeitdiebstählen in wissenschaftlichen und technischen Einrichtungen kam. /ZDN19r02/

Mitarbeiter des Kernkraftwerks brachten eigene IT-Systeme, sogenannte Miningracks mit mehreren stromintensiven Grafikkarten in den Verwaltungstrakt ein, schlossen diese Systeme an das interne Netzwerk des Verwaltungstrakts und dieses interne Netzwerk wiederum an das Internet an. Es bestand zu keiner Zeit eine Verbindung zwischen dem Netzwerk des Verwaltungstraktes und dem leittechnischen Netzwerk des Kraftwerkes. Nach Berichten wurde weiteres Equipment für die Generierung von digitalen Währungen in den auf dem Kraftwerksgelände befindlichen militärischen Kasernen gefunden. Die militärischen Kasernen werden von der ukrainischen Nationalgarde genutzt, da die Nationalgarde mit dem Schutz des Kraftwerks beauftragt ist. Es ist nicht bekannt, ob Mitglieder der Nationalgarde direkt an dem IT-Ereignis beteiligt waren. /ZDN19r02/

Kerntechnischer Bezug

Der IT-Sicherheitsvorfall ereignete sich in einem Verwaltungstrakt des KKW Südukraine.

B.11.2 Cyberangriff auf KKW Kudankulam

Übersicht

Im September 2019 wurde die Öffentlichkeit durch einen Tweet eines früheren Sicherheitsforschers der indischen nationalen technisch Forschungsorganisation (NTRO) auf einen aktiven Cyberangriff auf das indische Kernkraftwerk Kudankulam (2 russische DWR-Reaktoren) informiert /PUS19w01/.

Beschreibung

Die indischen Behörden leugneten einen solchen Cyberangriff zuerst, jedoch wurden Stück für Stück Informationen bekannt, welche aufzeigten, dass das Kernkraftwerk auf dem Niveau eines Domain Level Controllers (also zentralen Authentifizierungsservers) An-fang September 2019 kompromittiert worden war und damit die Angreifer einen weiten Zugriff zumindest auf das administrative Netzwerk des Kernkraftwerks erhalten hatten. /PKM20r01/

Der initiale Cyberangriff wurde mit der Verteilung manipulierter Emails durchgeführt. Die IT-Angreifer, welche nach bisherigen Kenntnissen seit mehreren Jahren Informationen zu wichtigen Personen des indischen zivilen nuklearen Programms ausforschten, nutzten ihre Informationen um sich in Emails als Regierungsmitarbeiter auszugeben und per Email Schadcode an Unternehmen und Privatpersonen des indischen zivilen nuklearen Sektors zu verteilen.

Als Schadcode wurde in Folge der Trojaner Dtrack eingesetzt; ein Trojaner für die Aufklärung und das Nachladen weiteren Schadcodes. Dtrack ist zum Auslesen von Tastatureingaben, Browserhistorien, Systeminformationen, Netzwerkinformationen und allen gespeicherten Daten fähig. Die eingesetzte Dtrack- Version basiert auf einem Bankingtrojaner, welcher im Jahr 2016 gegen indische Finanzinstitute angewendet wurde. Die Herkunft des Trojaners und des gesamten Cyberangriffes auf das Kernkraftwerk wird wegen verschiedener Indizien der ATP Lazarus zugeschrieben. /PKM20r01/

Nach bisherigen Informationen erreichten die IT-Angreifer vollumfänglich ihr Ziel. Mit in der Schadsoftware fest eingepflegten, gültigen Zugriffsinformationen konnten sie umfassend auf das administrative Netzwerk zugreifen und Daten aus diesem Netzwerk entwenden. Es wird davon ausgegangen, dass große Datenmengen, die in dem Netzwerk verfügbar waren, entwendet wurden. Es kam zu keinem Angriff oder Zugriff auf die leittechnischen Systeme des Kraftwerks, die Schadsoftware war nicht für solche Zugriffe ausgelegt. /PKM20r01/

Kerntechnischer Bezug

Das Kernkraftwerk Kudankulam war direkt von dem Cyberangriff betroffen und das administrative Netzwerk des Kraftwerks wurde von den Angreifern kompromittiert.

B.11.3 Weiterer IT-Sicherheitsvorfall in Zusammenhang mit Triton/Trisis

Übersicht

Über den in Abschnitt B.5.1 beschriebenen Cyberangriff unter Einsatz der Schadsoftware Triton/TriSIS auf eine petrochemische Anlage in Saudi-Arabien hinaus, wurde im April 2019 ein weiterer IT-Sicherheitsvorfall bekannt, bei dem es denselben Angreifern gelungen war, in eine weitere kritische Infrastruktur in Saudi-Arabien einzudringen /FIR19w01/.

Beschreibung

Details zu diesem weiteren IT-Sicherheitsvorfall in Zusammenhang mit der Schadsoftware Triton/TriSIS werden nach wie vor geheim gehalten. Bestätigt ist jedoch, dass es den Angreifern auch hier gelang, sich Zugriff auf das SIS zu verschaffen. Auf Basis der Untersuchung dieses IT-Sicherheitsvorfalls wurden Erkenntnisse zu den Angriffswerkzeugen veröffentlicht, mit denen die APT-Gruppierung in das Netzwerk der betroffenen Anlage eindrang, sich in diesem Netzwerk bewegte und den Einsatz der Schadsoftware Triton/TriSIS vorbereitete /FIR19w01/. Die entdeckten Angriffswerkzeuge sind im Rahmen eines komplexen und mehrstufigen Cyberangriffs, der sich typischerweise über Monate oder Jahre erstreckt, Angriffsschritten zuzuordnen, die zeitlich deutlich früher erfolgt sind als der Einsatz der Schadsoftware Triton/TriSIS selbst. Bemerkenswert ist, dass dabei eine ganze Reihe von Angriffswerkzeugen, darunter auch neue, von den Angreifern maßgeschneiderte Angriffswerkzeuge gefunden wurden.

Die von der IT-Sicherheitsfirma FireEye durchgeführte Analyse /FIR19w01/ dieses IT-Sicherheitsvorfalls zeigt, dass sich die Angreifer fast ein Jahr im Netzwerk der angegriffenen Anlage bewegten, bevor sie Zugriff auf industrielle Steuerungssysteme zur Ausführung von Sicherheits-, Sicherungs- oder Schutzfunktionen erlangten. Nach dem ersten Eindringen ins IT-Netzwerk der Anlage und einer Verfestigung des Zugriffs auf das Anlagennetzwerk lag der Fokus der Angreifer darauf, Zugriff auf die industriellen Steuerungssysteme zu erlangen. Hierzu setzten sie vor allem Werkzeuge zur Ausforschung des Anlagennetzwerks, für die laterale Ausbreitung im Anlagennetzwerk und für die Etablierung dauerhafter Präsenz im Anlagennetzwerk ein.

Zusätzlich nutzten sie eine Reihe von Techniken, um ihre Aktivitäten zu verbergen und wie legitime Aktionen erscheinen zu lassen.

Mittels dieser Techniken gelang es ihnen, ihre Spuren zu verwischen, die Identifikation der mit Schadcode behafteten Dateien zu verhindern, sowie eine potenzielle forensische Untersuchung ihrer Werkzeuge zu erschweren. Beispielsweise erlangten die Angreifer zwar Zugriff auf das industrielle Steuerungssystem zur Prozesssteuerung, nutzten diesen zunächst aber weder zur Manipulation der entsprechenden Controller noch zu Spionagezwecken. Nachdem sie Zugriff auf die anvisierten Controller des SIS erlangt hatten, lag der Fokus der Angreifer insbesondere darauf, diesen Zugriff dauerhaft zu erhalten und dort die Schadsoftware Triton/TriSIS einzusetzen. /FIR19w01/

Bisher ist jedoch nicht bekannt, ob es in der Folge zu Manipulationen oder Störungen von Sicherheits-, Sicherungs- oder Schutzfunktionen in der betroffenen Anlage gekommen ist.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r01/. Zudem wurde die Weiterleitungsnachricht 2021/01 verfasst.

B.11.4 ZeroCleare – Cyberangriffe auf den Energiesektor im mittleren Osten

Übersicht

Im Jahr 2019 gaben IT-Sicherheitsanalysten von IBM Security die Entdeckung einer neuen Wiper-Schadsoftware bekannt, die in der ersten Jahreshälfte 2019 bei mehreren Angriffen auf den Energiesektor im Mittleren Osten eingesetzt worden war. Die Schad-software wird als ZeroCleare bezeichnet.

Beschreibung

Bei ZeroCleare handelt es sich um einen klassischen Wiper, der versucht, auf den infizierten Systemen so viele Daten wie möglich zu löschen, wie sie auch in früheren An-griffen bereits eingesetzt wurden. ZeroCleare weist dabei Parallelen zur Schadsoftware Shamoon (siehe Abschnitt B.5.1) auf.

So versucht ZeroCleare, genau wie Shamoon, in Windows-basierten Systemen den Master Boot Record (MBR) zu überschreiben und Partitionen zu beschädigen. /IBM20i01/, /ZDN19w01/

Die beschriebenen Angriffe mit ZeroCleare begannen typischerweise mit einem Brute-Force-Angriff, um einen Erstzugriff auf einen Server zu erlangen. Anschließend nutzten die Angreifer eine Schwachstelle in SharePoint aus, um Schadsoftwarekomponenten wie beispielsweise China Chopper und Tunna zu installieren. Nach erfolgreicher lateraler Ausbreitung im Zielnetzwerk setzten die Angreifer im letzten Angriffsschritt die Schadsoftware ZeroCleare ein. Wie schon die bislang aufgefundenen Versionen von Shamoon /SEC12w04/ setzt ZeroCleare das von sich aus nicht schädliche Werkzeug EldoS RawDisk auf maliziöse Weise ein, um mit Dateien, Laufwerken und Partitionen zu interagieren und diese letztlich zu zerstören. EldoS RawDisk erlaubt das direkte Ändern von Daten unter Umgehung von Security Features des Windows-Betriebssystems. /IBM20i01/

Nach eingehender Untersuchung der Schadsoftware äußert IBM die Vermutung, dass die Angriffe von iranischen, staatlich geförderten Angreifern durchgeführt wurden. Die Rede ist hierbei von APT34/OilRig sowie mindestens einer weiteren Gruppierung. /IBM20i01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.5 Cyberangriff mit LockerGoga auf Norsk Hydro

Übersicht

Im März 2019 wurde bekannt, dass der norwegische Konzern Norsk Hydro, einer der größten Aluminiumproduzenten der Welt, am 19.03.2020 Opfer eines großangelegten Cyberangriffs mit der Ransomware LockerGoga wurde. Nachdem ursprünglich Unternehmensnetzwerke in den USA betroffen waren, verbreitete sich die Schadsoftware innerhalb von Stunden und betraf auch andere Niederlassungen des Unternehmens, welches in 40 Ländern agiert /GOO19w01/. Norsk Hydro stoppte daraufhin die Produktion in einigen Anlagen oder stellte in betroffenen Anlagen auf manuellen Betrieb um.

Insgesamt waren alle 35.000 Mitarbeiter des Unternehmens betroffen, wobei Daten auf über 1.000 PCs und Servern verschlüsselt wurden und sowohl die Produktion als auch Büro-Netzwerke betroffen waren. Der Vorfall verursachte finanzielle Schäden in Höhe von etwa 71 Millionen Dollar und hatte Auswirkungen auf den weltweiten Aluminium-markt. /BRI19w01/

Beschreibung

Die Schadsoftware LockerGoga wurde erstmals Anfang 2019 bei einem Cyberangriff auf das französische Unternehmen Altran Technologies, das vor allem in der Technologieberatung tätig ist, beobachtet. Altran Technologies veröffentlichte am 28.01.2019 eine Pressemitteilung in der angegeben wird, dass nach ihren Erkenntnissen keine Daten gestohlen wurden und dass sich die Schadsoftware nicht zu ihren Kunden verbreitet hat /ALT19i01/. Neben den Angriffen auf Altran Technologies und Norsk Hydro wurden auch zwei Cyberangriffe auf die europäischen bzw. US-amerikanischen Chemieunternehmen Hexicon und Momentive im Jahr19 bekannt, bei der die Schadsoftware LockerGoga verwendet wurde /WIE19w01/.

Im Fall von Norsk Hydro verschafften sich die Angreifer bereits Monate vor der Aktivierung der Schadsoftware durch eine mit Schadsoftware behaftete E-Mail an einen Mitarbeiter, die von einem vertrauenswürdigen Kunden des Unternehmens abgesendet wurde, Zugriff auf das Unternehmensnetzwerk. /BRI19w01/ In den folgenden Monaten breiteten die Angreifer sich lateral im Netzwerk aus, wobei u. a. Tools verwendet wurden, die Zugangsdaten erfordern, sodass davon auszugehen ist, dass die Angreifer diese Daten im Verlauf des Cyberangriffs über Spear-Phishing oder Brute-Force-Angriffe bzw. über den ursprünglichen Cyberangriff der schadsoftwarebehafteten E-Mail erlangten. Das auf den Bereich IT-Sicherheit spezialisierte japanische Unternehmen Trend Micro geht da-von aus, dass der Angriff mit der entsprechenden Vorbereitung sehr gezielt und mit der Absicht der Beeinträchtigung der Produktion von Norsk Hydro erfolgte. /TRE19w01/

Nach der Installation modifiziert LockerGoga die Accounts der Benutzer des Systems, indem es die Passwörter ändert. Die Schadsoftware versucht dabei, eingeloggte Benutzer auszuloggen. Daten auf den betroffenen Systemen (Laptops, Server, Desktop-PCs) werden anschließend verschlüsselt und auf dem Desktop eine Textdatei mit der Lösegeldforderung erstellt. Das Opfer wird darin aufgefordert, Kontakt mit den Angreifern aufzunehmen und Lösegeld in Form von Bitcoins zu zahlen.

Die verschlüsselten Daten umfassen dabei u. a. Dokumente wie PDF-Dateien, Tabellen, PowerPoint-Dateien, Datenbanken, Videos, sowie Python-Dateien und Java-Skripte. Je nach Version der Schadsoftware kann die Verschlüsselung spezifischer Dateien oder aller Daten sowie auch die Löschung von Daten von LockerGoga durchgeführt werden. In einigen von Trend Micro untersuchten Fällen war auch der Windows Boot Manager betroffen, sodass die betroffenen Systeme nicht mehr gestartet werden konnten. Bei allen von Trend Micro untersuchten Fällen waren die Systeme so stark beeinträchtigt, dass weder ein Entschlüsselungsprogramm genutzt werden noch eine Lösegeldforderung hätte erfüllt werden können, da die Opfer keinen Zugang zum System hatten. /TRE19w01/

Nach der Verschlüsselung der Daten versucht LockerGoga alle Netzwerkverbindungen des betroffenen Systems zu deaktivieren. Die Schadsoftware besitzt nach derzeitigen Informationen nicht die Fähigkeit, sich selbstständig auszubreiten wie beispielsweise WannaCry (siehe Abschnitt B.9.4) oder NotPetya (siehe Abschnitt B.9.6). Dagegen ist LockerGoga darauf ausgelegt, bis zur Ausführung möglichst unerkannt zu bleiben.

Dazu ist die Schadsoftware beispielsweise mit verschiedenen gültigen Zertifikaten (Alisa Ltd., Kitty's Ltd., and Mikl Limited) ausgestattet, die mittlerweile widerrufen wurden. Außerdem erzeugt die Schadsoftware keinen Netzwerk-Traffic, sodass diese Erkennungsmöglichkeit umgangen wird. Dazu werden weitere Techniken angewandt, um unerkannt zu bleiben. /TRE19w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.6 Cyberangriffe über VPN-Schwachstellen

Übersicht

Auf der BlackHat 2019, einer jährlichen Konferenz zu Informationssicherheit und Cyberangriffen, wurde ein umfassender Vortrag über Cyberangriffe auf VPN-Clients und VPN-zugängliche Netzwerke vorgestellt, welcher nach Einschätzung der Experten auf iranische IT-Angreifer zurückgeht. Die Erkenntnisse des Vortrages wurden Anfang 2020 in einem umfangreichen Bericht weiter dargelegt. /BLH20r01/

Beschreibung

Im Jahr19 sind eine Reihe von schwerwiegenden Schwachstellen in VPN-Clients bekannt geworden (CVE-2019-11510, CVE-2019-13379, CVE-2019-1579 usw.) welche von den im Vortag und zugehörigen Bericht genannten IT-Angreifern teilweise innerhalb von Stunden nach Veröffentlichung genutzt wurden, um Cyberangriffe durchzuführen.

Ziel der Angreifer waren nach bisherigen Erkenntnissen Netzwerke von Unternehmen und Behörden, welche VPN-Software für die datentechnischen Verbindungen ihrer Mitarbeiter benötigen, die außerhalb der Niederlassungen arbeiteten.

Wenn die Angreifer Zugriff auf die VPN-Verbindungen der Unternehmen bzw. Behörden erreichten, nutzten sie eine Reihe weiterer Schadsoftwarekomponenten und IT-Werkzeuge, um sich im betroffenen Netzwerk auszubreiten und immer mehr IT-Systeme zu kompromittieren. Nach bisherigen Erkenntnissen dienten die bisher erkannten Cyberangriffe über VPN-Schwachstellen durch mehrere iranische APT-Gruppierungen ausschließlich der Aufklärung, dem Abfließen von Informationen und der sicheren Installation von Hintertüren für die IT-Angreifer. Langfristig können solche Aufklärungs- und Zugriffsmöglichkeiten jedoch auch direkte Schadwirkung entfalten, z. B. wenn die IT-Angreifer Zugriff auf die Updateverteilsysteme von Softwarefirmen erhalten oder mit Datenlöschsoftware die Netzwerke und gespeicherten Daten unwiderruflich zerstören. /BLH20r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.7 Cyberangriff auf Windkraftanlage in den USA

Übersicht

Am 5. März 2019 wurde der u. a. in Utah (USA) ansässige Betreiber von Windkraft- und Solarenergieanlagen sPower, der über 130 Stromerzeugungsanlagen verteilt über die Vereinigten Staaten betreibt, Opfer eines Cyberangriffs. Das Unternehmen verzeichnete ei-ne Reihe von Verbindungsabbrüchen zwischen dem Hauptkontrollzentrum und entfernten Stromerzeugungsstandorten, die jeweils kurz und intermittierend auftraten.

Die Ausfallzeiten, die als Loss-of-View bezeichnet werden, wurden durch Denial-of-Service-Angriffe (DoS) verursacht und beeinträchtigten die Fähigkeit des Unternehmens, den aktuellen Status der betroffenen Anlagen zu überwachen. Die Stromerzeugung der betroffenen Anlagen war nicht beeinträchtigt. /SEA19w01/

Beschreibung

Die Angreifer nutzten für die DoS-Angriffe eine ungepatchte Sicherheitslücke in der Firewall der betroffenen Anlagen aus, die es unautorisierten Benutzern erlaubte, betroffene Geräte wiederholt neu zu starten. Dies führte zu mehreren kurzen (im Bereich weniger Minuten) Kommunikationsausfällen zwischen Geräten vor Ort in den Anlagen, sowie zwischen den Stromerzeugungsstandorten und dem Hauptkontrollzentrum. Die betroffenen Geräte sind Firewalls der amerikanischen Firma Cisco Systems, die als Sicherheitseinrichtungen gegen Cyberangriffe bzw. unerlaubte Zugriffe von außerhalb dienen. Bei den Standorten und dem Kontrollzentrum handelt es sich um Einrichtungen mit geringem Einfluss auf das Stromnetz. Die durchgeführten Untersuchungen des IT-Sicherheitsvorfalls ergaben, dass der extern initiierte Neustart der Firewalls über einen Zeitraum von 10 Stunden auftrat und in den jeweiligen Einzelfällen für weniger als fünf Minuten vorlag. Cisco Systems stellte nach diesem Vorfall dem Unternehmen einen Firmware-Patch bereit, der anschließend von sPower im System aufgespielt wurde. Die Schwachstelle war bereits vor dem Ereignis bekannt und Cisco Systems hatte den Firmware-Patch bereits veröffentlicht, jedoch hatte der Betreiber sPower diesen nicht installiert. /NER19r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12 2020

B.12.1 Cyberangriff auf US-amerikanischen Pipeline Betreiber

Übersicht

Am 18. Februar 2020 veröffentlichte die Cybersecurity and Infrastructure Security Agency (CISA) der USA einen Bericht zu einem bis dahin unbekannten Cyberangriff auf einen nicht genannten Pipelinebetreiber. Im Rahmen des Cyberangriffes wurde neben dem administrativen Netzwerk auch das die Pipeline steuernde leittechnische Netzwerk beeinflusst, sodass es zur Beeinflussung des Betriebsablaufes kam. /CIS20r05/

Beschreibung

Die IT-Angreifer nutzten Spear-Phishing- und Watering-Hole-Techniken für den initialen Einbruch in die IT-Systeme des Pipelinebetreibers. Zielgenau erstellte Links auf manipulierte Webseiten wurden hierbei genutzt, um an Nutzer in der Zielorganisation, welche die manipulierten Webseiten für legitime Webseiten hielten, Schadsoftware zu verteilen. Die so in das IT-Netzwerk des Pipelinebetreibers eingebrachte Schadsoftware verbreitete sich dann über Netzwerkverbindungen an jedes weitere angebundene IT-System innerhalb des betroffenen Pipelinekontrollzentrums. Da keine spezifische Barriere zwischen dem IT-Netzwerk und dem leittechnischen Netzwerk des Pipelinebetreibers bestand, breitete sich die Schadsoftware auch im leittechnischen Netzwerk aus. Als Schadsoftware kam ein Erpressertrojaner für Windowssysteme zum Einsatz, sodass alle betroffenen Windows-PCs und Server von den IT-Angreifern verschlüsselt wurden und damit nicht mehr nutzbar waren. Im leittechnischen Netzwerk waren hierdurch Mensch-Maschine-Schnittstellen, Server und Datenarchivierungssysteme betroffen, jedoch keine leittechnischen Steuereinheiten mit Einfluss auf die Pipeline. /CIS20r05/

Aufgrund der verschlüsselten IT-Systeme kam es bei dem Betreiber der Pipeline zu Ausfällen von Anzeigen im Pipelinekontrollzentrum, jedoch konnte der Pipelinebetrieb weiterhin gesteuert werden. Aufgrund der Ausfälle wurde die Pipeline für zwei Tage ab-geschaltet, die betroffenen IT-Systeme wurden getauscht und der Betrieb anschließend wieder aufgenommen.

Der Cyberangriff und seine Auswirkungen auf das leittechnische Netzwerk waren insbesondere dadurch möglich, dass der Betreiber der Pipeline kein IT-Sicherheitskonzept

etabliert hatte und Cyberangriffe nicht in potenzielle Notfall- und Sicherungspläne aufnahm. Die fehlende Trennung der administrativen und leittechnischen Netzwerke ist auf fehlendes Verständnis für die Bedeutung der Informationssicherheit und dem vorrangigen Ziel den täglichen Betrieb zu erleichtern zurückgeführt worden. CISA beschreibt umfassende Maßnahmen des Pipelinebetreibers zur Erhöhung der Informationssicherheit nach dem Vorfall. /CIS20r05/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12.2 SNAKE/EKANS – Cyberangriffe auf weltweite Unternehmen

Übersicht

Im Januar 2020 veröffentlichten Forscher mehrerer IT-Sicherheitsunternehmen wie Dragos und SentinelLABS Informationen zu der im Dezember 2019 erstmals entdeckten Schadsoftware Snake (auch als EKANS bezeichnet, Bezeichnung taucht bei den Angriffen als String auf; Snake rückwärts und im weiteren Verlauf als Snake bezeichnet), bei der es sich um Ransomware handelt /DRA20w02, WAL20w01/. Neben der für Ransomware üblichen Verschlüsselung von Daten und der angezeigten Lösegeldforderung ist nach /DRA20w02/ die Besonderheit bei Snake, dass die Schadsoftware verschiedene Prozesse beeinflussen bzw. stoppen kann, die unter anderem im Zusammenhang mit industriellen Steuerungen (ICS) stehen. Im Verlauf des Jahres 2020 wurden Angriffe auf verschiedene Unternehmen mit der Schadsoftware beobachtet.

Beschreibung

Die Schadsoftware Snake ist – wie es häufig bei Ransomware der Fall ist – in der open-source Programmiersprache Golang geschrieben, die durch ihre Unterstützung multipler Plattformen auf den drei großen Betriebssystemen Windows, macOS und Linux Anwendung findet. Nach der Infektion überprüft Snake zunächst, ob das System bereits von der Schadsoftware betroffen ist. Bevor im weiteren Verlauf die Verschlüsselung gestartet wird, erzwingt Snake das Stoppen von Prozessen, die in der Schadsoftware als Liste codiert sind und neben mit industriellen Steuerungssystemen in Zusammenhang stehenden Prozessen hauptsächlich Datenbanken (beispielsweise Microsoft SQL-Server) oder Backup-Systeme für Daten beinhalten. Nach /DRA20w02/ sind im

ICS-Bereich unter anderem die Firmen Honeywell und GE Digital betroffen. Außer dem erzwungenen Stopp der betroffenen Prozesse und der bei Ransomware üblichen Verschlüsselung der Daten, führt die Malware keine weiteren Aktionen aus und beeinflusst entsprechend ICS-zugehörige Prozesse nicht weiter.

Nach der Verschlüsselung betroffener Dateien werden die Dateinamen abgeändert, in-dem eine zufällige fünfstellige Buchstabenfolge an den Dateityp angehängt wird. Im Gegensatz zu einer uniformen Umbenennung erschwert dieses Vorgehen die Identifikation der Ransomware. Nach dem Stoppen der Prozesse und der Verschlüsselung der Daten wird im Root-Verzeichnis und auf dem Desktop eine Datei mit der Lösegeldforderung und einer E-Mail-Adresse als Kontaktmöglichkeit erstellt. Kritische Systemdateien oder -ordner sind nicht von der Verschlüsselung betroffen, sodass das System beispielsweise nicht heruntergefahren oder gesperrt wird, was dem Opfer Zugriff auf die verschlüsselten Daten erlaubt. Dies unterscheidet Snake von disruptiveren Vertretern von Ransomware wie beispielsweise LockerGoga (siehe Abschnitt B.11.5).

Die Schadsoftware Snake besitzt nach derzeitigen Informationen keinen Mechanismus zur Ausbreitung über ein infiziertes Netzwerk hinaus, sondern ist darauf angewiesen, dass sie aktiv gestartet oder innerhalb von Skripten ausgeführt wird, um ein Zielsystem zu infizieren. Innerhalb des Netzwerks breitet sich Snake über Skripte oder weitere Mechanismen aus, beispielsweise durch die Kompromittierung des Verzeichnisdienstes Active Directory. /DRA20w02/, /WAL20w01/

Im Verlauf des Jahres 2020 wurden vermehrt Cyberangriffe mit der Schadsoftware Snake beobachtet. Laut /ABR20w01/ startete am 4. Mai 2020 eine weltweite Kampagne von Cyberangriffen, bei der diverse Firmen, unter anderem im Gesundheitssektor, betroffen waren. Dabei wurde berichtet, dass Snake vor der Verschlüsselung der Daten außerdem Datendiebstahl betreibt und mit der Veröffentlichung der verwendeten Daten droht. Es ist unklar, ob dies tatsächlich der Fall ist, sich die Angreifer anderweitig Zugang zu Daten beschafft haben oder die Drohung tatsächlich in die Tat umgesetzt werden könnte. Eines der Opfer dieser Kampagne ist das deutsche Unternehmen Fresenius, ein Medizintechnik- und Gesundheitskonzern. Weiterhin ist Fresenius einer der größten privaten Krankenhausbetreiber Deutschlands und im Pharma- und Gesundheitsdienstleistungsbereich tätig. Ein Unternehmenssprecher bestätigte den Cyberangriff und gab an, dass es dadurch bzw. durch entsprechende Gegenmaßnahmen zwar zu Einschränkungen einiger Funktionen innerhalb des Unternehmens kam, die Patientenversorgung jedoch sichergestellt und fortgesetzt werde. /KRE20w01/

Generell sind die Opfer von Snake nach derzeitigen Informationen gezielt ausgesucht. Die Schadsoftware gleicht dazu das Netzwerk der Opfer mit eigenen IP-Listen ab. /JUN20w01/ Die Ziele sind weltweit verteilt und umfassen ein breites Spektrum. Neben Angriffen auf Unternehmen und Organisationen der kritischen Infrastruktur (wie beispielsweise Fresenius in Deutschland) stellt in diesem Zusammenhang der Cyberangriff auf das Unternehmen Honda, einem japanischen Konzern, der hauptsächlich im Bereich Motoren und Automobil tätig ist, im Sommer 2020 einen weiteren IT-Sicherheitsvorfall dar. Betroffen waren Netzwerke von Unternehmensniederlassungen in Europa und Japan. Die entsprechenden Honda-Domains wurden in der Ziel-Abfrage der Schadsoftware gefunden. /ILA20w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12.3 Cyberangriff auf die Stromversorgung von Mumbai

Übersicht

Am 13. Oktober 2020 waren etwa 20 Millionen Menschen in Mumbai von einem Stromausfall betroffen. Dem Ereignis waren politische Spannungen zwischen Indien und China vorrausgegangen. Bis heute ist jedoch unklar, ob es sich bei dem Stromausfall um einen Cyberangriff Chinas oder um technisches bzw. menschliches Versagen gehandelt hat.

Beschreibung

Am 13. Oktober 2020 kam es zu einem Stromausfall in Mumbai, von dem etwa 20 Millionen Menschen betroffen waren. Vermutlich war der Stromausfall die Folge eines chinesischen Cyberangriffs auf ein nahe gelegenes Stromlastmanagementzentrum. Dem Ereignis waren politische Spannungen zwischen Indien und China vorausgegangen. Seit Anfang 2020 sind indische Organisationen, darunter auch solche aus dem Energiesektor, das Ziel chinesischer Cyberangriffe /ECT21w01/. Im Februar 2020 führten indische IT-Angreifer eine Kampagne gegen chinesische Organisationen in Wuhan durch, bei denen sie Phishing-E-Mails verwendeten, die das Corona Virus thematisierten. Im Juni 2020 kam es zu Auseinandersetzungen zwischen indischen und chinesischen Truppen im Galwan-Tal, an der Grenze zwischen beiden Ländern /ECT21w01/.

Vier Monate später startete China Cyberangriffe auf die indische Technologie- und Bankeninfrastruktur. Dabei wurde auch Schadsoftware in die Leittechniksysteme und Knotenpunkte des indischen Stromnetzes eingeschleust, wobei ein Großteil der Schadsoftware jedoch nicht aktiviert wurde. Unter den Zielen befanden sich ein Umspannwerk und ein Kohlekraftwerk. /NYT21w02, REC21w03, WSJ21w02/

Das US-amerikanische IT-Sicherheitsunternehmen Recorded Future, das das Internet auf Aktivitäten staatlicher Akteure untersucht, entdeckte zwar den Datenfluss der Schadsoftwarekomponenten, war aber nicht in der Lage deren Programmcode zu untersuchen, da die indischen Behörden keine Auskunft darüber geben /WSJ21w02/. Recorded Future sendete seine Ergebnisse an das indische Computer Emergency Response Team CERT. Vermutlich ist für die Einschleusung der Schadsoftware in das indische Stromnetz die chinesische APT-Gruppierung Red Echo verantwortlich. Indische Militärexperten haben dazu geraten, in China gefertigte Hardware, welche im indischen Energiesektor eingesetzt wird, auszutauschen. /NYT21w02, REC21w03, WSJ21w02/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12.4 SolarWinds – Cyberangriffe über schadsoftwarebehaftete SolarWinds Produkte

Übersicht

Anfang Dezember 2020 wurde eine breit angelegte Angriffswelle von Supply-Chain-Angriffen über manipulierte, schadsoftwarebehaftete SolarWinds-Produkte bekannt /FIR20r01/. Von den Cyberangriffen ist hierbei die Software-Plattform SolarWinds Orion betroffen, die unter anderem Monitoring und Management von IT-Netzwerken, -Systemen und -Anwendungen ermöglicht und von 33.000 Solar Winds Kunden genutzt wird.

Beschreibung

Den IT-Angreifern gelang es, unbemerkt eine Reihe von SolarWinds Orion Versionen (2019.4 HF5 bis 2020.2.1) mit einem Trojaner zu infizieren, welche dann digital signiert und ab März 2020 über den offiziellen Update-Server von SolarWinds verteilt wurden.

Hierbei ist konkret die Programmbibliothek SolarWinds.Orion.Core.BusinessLayer.dll betroffen /BSI20i04/. Diese Programmbibliothek ist ebenfalls digital signiert. Die inzwischen als Sunburst betitelte Schadsoftware etabliert eine Backdoor mit weitreichenden Handlungsoptionen für die Angreifer /FIR20r01/. Es wurde bekannt, dass etwa 18.000 Kunden von SolarWinds die schadsoftwarebehafteten Updates heruntergeladen haben /DAR21w01/.

Entdeckt wurde die Schadsoftware von der IT-Sicherheitsfirma FireEye, welche am 13.12.2020 von einer sektor- und ländergreifenden Angriffskampagne mit Schadsoftware berichtet, einschließlich eines Angriffs auf FireEye selbst /FIR20r01/. Darüber hinaus werden immer weitere Berichte über nach dem Download der schadsoftwarebehafteten Solar Winds Updates weiterführende Kompromittierungen mit Sunburst bekannt. Unter anderem bei einer Reihe von US-Ministerien und Behörden (bspw. die US-Department of Homeland Security, Justice, Energy, Commerce und Treasury ebenso wie das US-Department of State und die National Institutes of Health) sowie unter anderem die Federal Energy Regulatory Commission (FERC), das Los Alamos National Laboratory und die Sandia National Laboratories /BUS20w01, POL20w01/. Auch Microsoft, VMware, CrowdStrike und Cisco haben inzwischen bestätigt, Ziel des Angriffs mit Sunburst geworden zu sein /NYT20w02, REU20w01, WSJ20w01/.

Bereits Anfang Januar 2020 wurde von mehr als 250 kompromittierten Angriffszielen ausgegangen /SEC21w05/. Es ist zu erwarten, dass es darüber hinaus noch weitere Opfer der Angriffswelle gibt, welche den Angriff bislang noch nicht entdeckt oder nicht öffentlich gemacht haben. Welche und wie viele Daten bei den bisherigen Angriffen gestohlen oder manipuliert wurden, lässt sich bislang noch nicht abschätzen, die Analyse und Aufarbeitung wird sich vermutlich über Jahre hinziehen. Auch ist derzeit noch keine Aussage dazu möglich, wie viele kompromittierte oder manipulierte Daten und Informationen von den direkt mit Sunburst angegriffenen Opfern an Dritte weitergegeben wurden. Darüber hinaus handelt es sich bei den Cyberangriffen nicht um eine vergangene, sondern eine aktuelle, derzeit noch andauernde Angriffskampagne. Dies schließt weitere Angriffsziele als auch die weitergehende Kompromittierung oder Ausschleusung und Manipulation von Daten und Informationen bisheriger Angriffsziele ein.

Kerntechnischer Bezug

Zu den von den Angriffen mit schadsoftwarebehafteten SolarWinds Produkten betroffenen Organisationen zählen auch das Los Alamos National Laboratory, welches sich mit der Forschung und Entwicklung hinsichtlich Nuklearwaffen und Kernfusion beschäftigt. Ein weiteres Opfer sind die Sandia National Laboratories, in welchen hauptsächlich die nicht-nuklearen Komponenten von Nuklearwaffen entwickelt und hergestellt werden. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r05/.

B.13 2021

B.13.1 Oldsmar Attack – Cyberangriff auf Wasserwiederaufbereitungsanlage in Tampa, Florida

Übersicht

Im Februar 2021 wurde von der amerikanischen Bundespolizei FBI ein Bericht veröffentlicht, wie im Rahmen eines Cyberangriffes auf eine Wasserwiederaufbereitungsanlage nördlich von Tampa die Trinkwasserversorgung vergiftet wurde. Die Angreifer nutzten hierbei einen Fernwartungszugriff, welcher auch von Mitarbeitern insbesondere in der Pandemiezeit genutzt wird.

Der Cyberangriff wurde bei anschließenden Ermittlungen der Sicherheitsbehörden als Bedienfehler durch einen verantwortlichen Mitarbeiter identifiziert.

Beschreibung

Die Angreifer nutzten den Fernzugriff, um den Regler für die Steuerung des Anteils von Natriumhydroxid im Wasser zu manipulieren und den Anteil von 100 ppm auf 11.000 ppm anzuheben. Dem schichthabenden Mitarbeiter fiel auf, wie sich der Mauszeiger von selbst bewegte und am Regler der Anteil des Natriumhydroxids erhöht wurde. Die Angreifer beendeten umgehend nach dem Eingriff ihre Verbindung.

Gemäß der Anlage wäre ohne Entdeckung durch den Mitarbeiter der Angriff durch die eingesetzten pH Scanner der Anlage aufgefallen, was dann jedoch zu einer Unterbrechung der Wasserversorgung geführt hätte. Der Fernwartungszugriff wurde auf den Cyberangriff folgend deaktiviert und es sollen Upgrades der Systeme durchgeführt werden. /NPR21r01/

Im Rahmen der offiziellen Ermittlungen wurde von den lokalen Behörden festgestellt, dass sich in Oldsmar kein Cyberangriff ereignet hatte. Ein verantwortlicher Mitarbeiter führte einen Bedienfehler aus, welcher zu dem 11.000 ppm Steuerungswert führte. Zur Verschleierung gab der Mitarbeiter an, dass es sich um einen Cyberangriff handelte.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.2 DarkSide – Cyberangriff auf brasilianischen Energiesektor

Übersicht

Die Nachrichtenagentur Reuters veröffentlichte im Februar 2021 eine kurze Meldung, dass nach Angaben des brasilianischen Betreibers Eletrobras sich ein Informationssicherheitsvorfall im Kernkraftwerk Angra ereignete. Dabei wurde der Betrieb des Kraftwerkes nicht beeinflusst, ein nicht näher beschriebenes Netzwerk des Kraftwerkes wurde von einer Ransomware infiziert. Die Nutzung eines Teils der administrativen Systeme wurde daraufhin untersagt und eine Untersuchung angeordnet.

Gemäß den vorliegenden Informationen wurde neben dem KKW Angra auch Eletrobras selbst sowie der Energiekonzern Copel angegriffen, mit nach Information von Reuters der neuartigen Ransomware Darkside, welche auch Informationen vom Unternehmen Copel entwendete. Weitere Informationen sind bisher nicht verfügbar. /REU21r01/

Kerntechnischer Bezug

Das Kernkraftwerk Angra war direkt von diesem Cyberangriff betroffen.

B.13.3 Codecov – Cyberangriff über Bash Uploader Dev Tool

Übersicht

Im April 2021 wurde ein Supply-Chain-Angriff über eine Kompromittierung des IT-Werkzeugs Codecov Bash Uploader entdeckt, der seit Ende Januar 2021 unentdeckt geblieben war. Beim Codecov Bash Uploader handelt es sich um ein Werkzeug, das im Rahmen einer Analyse der sogenannten Code Coverage (Testabdeckung von Programmcode im Zuge des Entwicklungsprozesses) zum Einsatz kommt.

Konkret dient das von der Manipulation betroffene Bash Uploader-Skript dazu, aus verschiedenen Entwicklungsplattformen heraus Code Coverage-Reports zur weiteren Auswertung an den Server von Codecov zu übermitteln. Von den Manipulationen betroffen sind nach Aussage des Unternehmens auch die verwandten Bash Uploader-Skripte für GitHub, CircleCI und Bitrise Step. Die manipulierte Version des Bash Uploaders verschaffte den IT-Angreifern unter bestimmten Voraussetzungen Zugangsdaten und andere Informationen aus Continuous-Integration-Umgebungen von Codecov-Kunden, die das kompromittierte Skript für ihre Repositories verwenden. /HEI21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.4 Kaseya – Globaler Cyberangriff

Übersicht

Am 2. Juli 2021 ereignete sich ein Cyberangriff auf VSA-Server verschiedener weltweit verteilter Unternehmen, wobei über 1000 Firmen betroffen waren. Die betroffene Software VSA (Virtual System Administrator) des amerikanischen IT-Dienstleisters Kaseya ist ein Remote-Monitoring und -Management-Tool, mit dem Dienstleistungen wie beispielsweise Fernwartung o. ä. durchgeführt werden können. Unter anderem wird VSA häufig zum Ausführen von Softwareupdates verwendet. Die Angreifer nutzten dabei eine Sicherheitslücke aus und verschlüsselten infolgedessen im Rahmen eines Ransomware-Angriffs die Daten der Kunden des IT-Dienstleisters, um Lösegeld für die Entschlüsselung der Daten zu erpressen. Kaseya hat weltweit mehr als 36.000 Kunden.

Die Anzahl der von dem Angriff betroffenen Unternehmen liegt nach Angaben der IT-Sicherheitsfirma Huntress bei mehr als 1.000. Kaseya selbst spricht von weniger als 40 betroffenen Kunden, wobei sich darunter wiederum auch IT-Dienstleister mit mehreren Kunden befanden, sodass eine Verbreitung über mehrere Schritte wahrscheinlich ist.

Bei den Tätern handelt es sich mutmaßlich um die russische Gruppierung REvil, die bereits durch Ransomware-Angriffe auf US-Unternehmen sowie Cyberangriffe gegen verschiedene Ministerien und Behörden insbesondere in der jüngeren Vergangenheit aufgefallen ist.

Es wurden bei diesem Cyberangriff mit Hilfe von Ransomware Daten auf den betroffenen VSA-Servern verschlüsselt. Insgesamt handelt es sich um 50 Server, die durch den Angriff betroffen waren. Über ein Softwareupdate wurde die Schadsoftware an tausende Firmenrechner verteilt, wobei die Angreifer für diesen Lieferkettenangriff einen Zero-Day-Exploit ausnutzten. Am 5. Juli 2021 folgte eine Lösegeldforderung im Darknet über 70 Millionen US-Dollar in Form von Kryptowährung (Monero) für die Entschlüsselung der Daten. Betroffen war neben überwiegend Unternehmen in den USA und Großbritannien sowie die schwedische Supermarktkette Coop, deren Zahlungsdienstleister die Software von Kaseya nutzt. Coop musste in der Folge am 3. Juli 2021 alle 800 Filialen schließen, da die Kassensysteme blockiert waren. Dem Bundesamt für Sicherheit in der Informationstechnik zufolge waren auch in Deutschland Unternehmen betroffen. Insgesamt spricht das BSI von einigen tausend betroffenen Computern und unter anderem einem betroffenen IT-Dienstleister. /HEI21w06/, /CIO21w01/, /BSI21i10/

Beschreibung

Am Abend des 2. Juli 2021 startete der Cyberangriff zunächst in den Vereinigten Staaten und hatte zeitnah bereits Auswirkungen in Europa. Kaseya berichtete am selben Tag von einem potenziellen Angriff auf die Fernwartungssoftware VSA und empfahl den Kunden, vorsorgliche ihre VSA-Server abzuschalten. Die Kunden wurden per E-Mail, Telefon und Online-Benachrichtigungen informiert, dies schnellstmöglich durchzuführen, da einer der ersten Schritte der Angreifer die Sperrung des administrativen Zugriffs auf diese Systeme beinhaltet. Bei dem Ransomware-Angriff über Kaseyas Software VSA handelte es sich um einen der bisher größten Cyberangriffe über die Lieferkette. Neben den über 1.000 direkt betroffenen Firmen, die mit Kaseya in Verbindung standen und den entsprechend tausenden von der Verschlüsselung betroffenen Computern, waren

auch Firmen betroffen, die selbst keinen direkten Bezug zu Kaseya haben, sondern deren IT-Dienstleister oder Zulieferer VSA nutzten.

Die Angreifer nutzten mehrere Sicherheitslücken und Zero-Day-Exploits aus, um die VSA-Server zu manipulieren und so ein schadsoftwarebehaftetes Update zu platzieren, welches entsprechend von den Servern an die Clients weitergegeben wurde. Dieses Update führte zur Verschlüsselung sämtlicher Daten betroffener Systeme und forderte zu einer Lösegeldzahlung auf. Einzelne Anwender erhielten Forderungen im Bereich von ca. 50.000 US-Dollar (in Form der Kryptowährung Monero), im Verlauf des Angriffs ergaben sich Lösegeldforderungen der Angreifer von bis zu umgerechnet 70 Millionen US-Dollar für die Entschlüsselung aller betroffenen Systeme.

Nach bisherigem Kenntnisstand war von dem Angriff lediglich der Update-Server von Kaseya betroffen und nicht die Infrastruktur, wie es beispielsweise bei SolarWinds der Fall war, wo Angreifer Zugriff auf den Build-Server des Unternehmens erlangt hatten.

Die Einschleusung der Schadsoftware bzw. das Einfallstor für diesen Lieferkettenabgriff waren mehrere Zero-Day-Exploits in der Software VSA von Kaseya. Die Existenz dieser Sicherheitslücken war bereits teilweise vor dem Angriff bekannt. Mitarbeiter des Dutch Institute for Vulnerability Disclosure (DVID) hatten vor dem Angriff mehrere Zero-Day Vulnerabilities entdeckt und die Erkenntnisse bereits an Kaseya weitergegeben. Nach-dem Kaseya von den Schwachstellen erfahren hatte, trat sie in Kontakt mit dem DIVD und arbeitete zusammen an Lösungen, unter anderem indem intern erste Patches zur Behebung getestet wurden. Der Cyberangriff auf die VSA-Server erfolgte, bevor Kaseya die Sicherheitslücken patchen und die Patches einer breiten Öffentlichkeit zur Verfügung stellen konnte. /HEI21w07/, /DIV21w01/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.13.5 DarkSide – Cyberangriff auf Colonial Pipeline

Übersicht

Am 7. Mai 2021 bemerkte der US-amerikanische Pipeline-Betreiber „Colonial“, dass die IT-Systeme der Firma Ziel eines Cyberangriffs mit Ransomware waren. Die Colonial-Pipeline ist mit ca. 8.850 km Länge die größte Pipeline für Erdölderivate (Diesel, Heizöl, Treibstoff für Flugzeuge uvm.) in den USA, wobei täglich mehrere 100 Millionen Liter an der Ostküste der USA von Texas bis an den Hafen von New York und New Jersey befördert werden. Um den Cyberangriff schnellstmöglich zu begrenzen und da zunächst unklar war, inwieweit IT- und OT-Systeme betroffen waren, stellte der Betreiber den Betrieb der Pipeline innerhalb weniger Stunden nach der Erkennung des Angriffs ein. Neben dem Einsatz von Ransomware gelang es den Angreifern vor der Verschlüsselung etwa 100 GB Daten zu stehlen. Als Gegenleistung für die Entschlüsselungstools und zur Verhinderung der Veröffentlichung der Daten verlangten die Angreifer Lösegeld in Höhe von ca. 4,4 Millionen Dollar in Form von Bitcoins.

Der Betreiber zahlte das Lösegeld am 8. Mai 2021, woraufhin ein Tool zur Entschlüsselung zur Verfügung gestellt wurde und am 12. Mai 2021 der Betrieb der Pipeline wieder aufgenommen wurde. Es handelte sich hierbei lediglich um einen rudimentären Grundbetrieb. Es dauerte Wochen bzw. Monate bis alle Auswirkungen des Cyberangriffs behoben waren. Am 7. Juni 2021 gab das amerikanische Justizministerium bekannt, dass 63,7 Bitcoins (ca. 2,3 Millionen Dollar) die für die Lösegeldzahlung verwendet wurden, zurückerlangt werden konnten. Im Rahmen der unmittelbaren Auswirkungen des Ausfalls der Pipeline kam es zu Lieferengpässen, sodass aufgrund der Treibstoffknappheit der Flugverkehr u. a. am Charlotte Douglas International Airport beeinträchtigt wurde, die Preise für Benzin rasant anstiegen und es zu Panikkäufen von Benzin kam, da in einzelnen Gebieten bis zu 80 % der Tankstellen kein Benzin mehr vorrätig hatten. Für die betroffenen Gebiete wurde der Notstand ausgerufen. /SEC21w07/, /SEC21w08/

Beschreibung

Die Colonial Pipeline Company gab am 07.05.2021 bekannt, Opfer eines Cyberangriffs mit Ransomware zu sein und stellte am gleichen Tag den Betrieb ein. Offen blieb zunächst, ob neben der Informationstechnik auch OT bzw. industrielle Steuerungssysteme vom Angriff direkt betroffen waren. Der Betreiber der Pipeline nahm vorsorglich auch bis zu dem Zeitpunkt nicht betroffene IT-Systeme, einschließlich Büro-IT und industriellen

Steuerungssystemen, außer Betrieb, da Umfang und Zielsetzung des Angriffs zunächst nicht bekannt waren. Es ist nicht bekannt, ob in der Systemarchitektur des Betreibers eine klare Trennung zwischen IT und OT vorliegt, sodass ggf. durch den Angriff auf IT-Systeme auch OT-Systeme bis hin zu industriellen Steuerungssystemen beeinflusst werden konnten. Nach derzeitigem Kenntnisstand betraf der Cyberangriff jedoch aus-schließlich IT-Systeme und zielte auf die Abrechnungsinfrastruktur ab. /CON21w02/, /CNN21w01/, /CIS21w08/

Die Angreifer setzten dem FBI zufolge eine Ransomware ein, die unter dem Namen DarkSide bekannt ist und von der gleichnamigen Gruppierung, die mutmaßlich Verbindungen nach Russland aufweist, eingesetzt wird /FBI21w01/. Außer der Verschlüsselung von Daten betreibt DarkSide gleichzeitig Spionage und Datendiebstahl, um die Opfer mit Androhung einer Veröffentlichung dieser Daten noch stärker unter Druck zu setzen. Die Gruppierung hinter DarkSide bietet im DarkNet mit Hilfe von Cloud Computing Ransomware-as-a-Service (RaaS) an, d. h. sie bietet auch Dritten, die selbst über keinerlei Programmierkenntnisse verfügen, eine maßgeschneiderte Version ihrer Ransomware gegen Bezahlung an.

Die eigentliche Erpressung wird dann von den Cyberkriminellen durchgeführt, welche die RaaS-Dienste in Anspruch nehmen. /DIG20w01/

Den Zugriff auf das Netzwerk von Colonial Pipeline erlangten die Angreifer nach Angaben des Geschäftsführers über einen veralteten, nicht mehr genutzten VPN-Zugang. Dieser war mit einem komplexen Passwort geschützt, jedoch nicht wie viele andere aktuelle Systeme des Betreibers weiter gesichert, beispielsweise mit einer Multi-Faktor-Authentifizierung. Es ist unklar, wie die Angreifer die Anmeldeinformationen (credentials) erlangten. /CYB21w01/ Die eigentliche Schadsoftware ist eine komprimierte ausführbare Datei mit komprimierten Konfigurationsdateien und nutzt hybride Verschlüsselungstools. DarkSide prüft im Verlauf der Ausführung, ob die Schadsoftware mit erhöhten Rechten ausgeführt wird. Wenn der mit dem Prozess verbundene Benutzer kein Administrator ist, verwendet DarkSide Techniken zur Erhöhung der Benutzerrechte, um sich selbst mit höheren Rechten neu zu starten. Es werden vorbereitende Schritte zur Verschlüsselung der Daten durchgeführt, die Kommunikation mit dem für den Angriff vorgesehenen Command & Control (C&C)-Server hergestellt und geprüft, ob die Systemsprache des Systems Russisch ist, wobei sich die Schadsoftware beendet, wenn dies der Fall ist. Zur Identifizierung der Opfersysteme werden systemspezifische Informationen verschlüsselt gespeichert und an den C&C-Server übertragen. Der Hauptangriff besteht anschließend

darin, die Kopien jedes Datenträgers mithilfe eines PowerShell-Skripts zu löschen, damit das Opfer die Daten nicht wiederherstellen kann. Außerdem werden Windows-Dienste und verschiedene Prozesse beendet. Anschließend verschlüsselt die Malware rekursiv Dateien, bis alle lokalen und Netzwerkspeicher verschlüsselt sind. Der Dateiname, die Daten und der Hash des Opfers werden an jede Datei angehängt, bevor sie an den entsprechenden C&C-Server des Angreifers übermittelt werden. In einem letzten Schritt löscht die Malware sich selbst. /VIR21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Darkside veröffentlichte nach dem Cyberangriff auf die Pipeline eine Meldung, dass ihre Ziele rein wirtschaftlicher Natur seien und dass direkte Auswirkungen für die Gesellschaft vermieden werden sollten. Demnach sollen u. a. die Angriffsziele nach eigenen Angaben, insbesondere auch im Rahmen der RaaS-Dienste, zukünftig abseits von Krankenhäusern, Schulen, Universitäten, Non-Profit-Organisationen und staatlichen Einrichtungen liegen. /CNB21w01/

Eigenen Angaben zufolge hat die Gruppierung aufgrund der Aktivitäten und des Drucks der Behörden der Vereinigten Staaten die Aktivitäten eingestellt, wobei der Gruppierung unter anderem der Zugang zu Teilen ihrer Infrastruktur nicht mehr möglich sei. Da es sich hierbei um eigene Angaben einer kriminellen Organisation mutmaßlich mit russischen Verbindungen handelt, ist die Glaubwürdigkeit zumindest fraglich. Für derartige Gruppierungen ist es zudem üblich, unter einem neuen Namen zu agieren. Nach Informationen der CISA operiert die Gruppierung neuerdings möglicherweise unter der Bezeichnung „BlackMatter“ (siehe Abschnitt B.13.7). /WSJ21w01, CIS21i07/

B.13.6 Cyberangriff auf Kisters AG

Übersicht

Am 12.11.2021 meldete das deutsche IT-Unternehmen Kisters AG, dass es in der Nacht vom 10. auf den 11. November 2021 Opfer eines Cyberangriffs geworden ist, wobei die Angreifer Ransomware einsetzten. Das Unternehmen arbeitet als IT-Dienstleister unter anderem im Bereich der kritischen Infrastrukturen und versorgt dabei beispielsweise Energieerzeuger, Netzbetreiber und Messstellenbetreiber mit Softwareprodukten.

Die Dienstleistungen umfassen dabei unter anderem die Steuerung von Regelleistungen. Die Kisters AG hat nach eigenen Angaben zunächst das komplette System heruntergefahren, um weiteren Schaden zu vermeiden und war vorübergehen weder per E-Mail noch über das Festnetz-Telefon erreichbar. Bis zum März 2022 konnte in fast allen Be-reichen wieder der Normalbetrieb eingerichtet werden. Die Kriminalpolizei und das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden umgehend eingeschaltet und die zuständigen Aufsichtsbehörden informiert. /KIS21w01/

Beschreibung

Das BSI schätzt den erfolgreichen Angriff auf die Kisters AG in ihren Meldungen zur IT-Bedrohungslage vom 16. bzw. 19.11.2021 unter anderem für Betreiber kritischer Infrastrukturen als potenziell kritisch ein, da zu diesem Zeitpunkt nach Aussage des Unternehmens nicht ausgeschlossen werden konnte, dass Kunden- oder Lieferantendaten kompromittiert wurden, was auch entsprechende Einwahldaten der Fernwartungszugänge betreffen könnte.

Nach Angaben der Kisters AG haben sich die Angreifer bei dem durchgeführten Ransomware-Angriff Zugang zu Daten des Unternehmens gesichert, diese verschlüsselt und damit gedroht, die erbeuteten Daten zu veröffentlichen. Bei einer Weigerung, entsprechende Lösegeldforderungen zu erfüllen, war demnach unter anderem mit einer Veröffentlichung der erbeuteten Daten zu rechnen. Am 21.11.2021 meldete die Kisters AG, dass nach den bisherigen forensischen Analysen keine Anzeichen gebe, dass aus-gelieferte Softwareprodukte kompromittiert sind /ENE21w01/. Allerdings geht das Unter-nehmen davon aus, dass Daten abgeflossen sein könnten, welche Informationen zu kritischen Infrastrukturen beinhalten, beispielsweise Netzpläne oder weitere sensible Daten. (BSI-Meldung)

Hinsichtlich der Frage, wie sich die Angreifer Zugriff zum Netzwerk der Kisters AG verschafft haben, gibt es bisher keine Informationen. Das Unternehmen veröffentlichte am 31. März 2022 eine Pressemitteilung, nach der in fast allen Bereichen wieder ein Nor-malbetrieb eingerichtet wurde, wobei über vier Monate Anstrengungen zur Wiederherstellung und Verbesserung der IT-Infrastruktur, wie beispielsweise eine technische Entkopplung der E-Mail-Server von der internen Infrastruktur, unternommen wurden. Zudem wurde durch weitere Sicherheitsvorkehrungen, wie umfangreiche Viren-Scans, Passwortänderungen und Prozessbeobachtungen die Sicherheit weiter erhöht. /ENE21w01/, /KIS22w01/, /ENE22w01/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.13.7 Black Matter – Cyberangriffe auf kritische Infrastrukturen

Übersicht

Am 18. Oktober 2021 wurde von der CISA, dem FBI und der NSA eine Warnmeldung bezüglich Ransomware-Angriffen von der Gruppierung „BlackMatter“ bzw. mit der gleichnamigen Ransomware veröffentlicht /CIS21i07/. Darin sind Informationen über die bei den Cyberangriffen verwendeten Taktiken, Techniken und Prozeduren (TTPs) enthalten.

Nach Angaben der CISA handelt es sich bei BlackMatter um eine Ransomware ein-setzende und Ransomware-as-a-Service (RaaS) anbietende, russisch-sprachige Gruppierung, die erstmals im Juli 2021 in Erscheinung getreten ist und seitdem diverse Ziele der amerikanischen kritischen Infrastruktur angegriffen hat. Darunter zwei Organisationen des US-amerikanischen Lebensmittel- und Landwirtschaftssektors. Der Hersteller für Antivirensoftware Emsisoft berichtet in der Zeit von Juli bis September 2021 von 44 Cyberangriffen mit der Ransomware BlackMatter und schätzt aufgrund einer erwarteten Dunkelziffer die Aktivitäten der Gruppierung auf über 100 Angriffe in dieser Zeit, wobei die Ziele neben den USA, dem Vereinten Königreich und Kanada weltweit verteilt sind. Hervorzuheben ist dabei ein Angriff auf den japanischen Konzern Olympus, der weltweit Produkte im Bereich Optik und Fotografie im Privatbereich und für die Medizin, Wissenschaft und Industrie anbietet. Nachdem verdächtige Aktivitäten in den Firmennetzwerken in Europa, Afrika und dem mittleren Osten beobachtet wurden, stellte Olympus den Datentransfer in die Systeme der betroffenen Regionen vorbeugend ein. /EMS21w01/

Beschreibung

Die Ransomware BlackMatter wird von der gleichnamigen Gruppierung eingesetzt und auch als RaaS angeboten, d. h. sie ist auch für Dritte, die selbst über keinerlei Programmierkenntnisse verfügen, in Form einer maßgeschneiderten Version der Ransomware gegen Bezahlung verfügbar. Die eigentliche Erpressung wird dann von den Cyberkriminellen durchgeführt, welche die RaaS-Dienste in Anspruch nehmen. Bei einem entsprechenden Cyberangriff werden die Daten der Opfer verschlüsselt, woraufhin eine

Lösegeldforderung zwischen in der Regel 80.000 $ und 15.000.000 $ in Kryptowährungen (Bitcoin oder Monero) und ggf. die Drohung der Veröffentlichung gestohlener Daten erfolgt. Bevor die Daten im Verlauf des Cyberangriffs mit Hilfe kryptographischer Tools (Sal-sa20 bzw. RSA 1024-bit) verschlüsselt werden, werden Daten vom kompromittierten System extrahiert und zur weiteren Erpressung der Opfer hinsichtlich einer möglichen Veröffentlichung missbraucht. Neben einer Version für Windows-Systeme existiert auch eine für Linux-Systeme entwickelte Version von BlackMatter. /EMS21w01/

Der Cyberangriff beginnt mit dem Eindringen in das Netzwerk des Opfers, was in der Regel über ein kompromittiertes Remote-Desktop-Protokoll, Phishing-Kampagnen, das Ausnutzen bekannter Schwachstellen oder gestohlene Anmeldedaten erfolgt. Nach der Ausführung der Schadsoftware überprüft BlackMatter zunächst die Nutzerrechte, um ggf. durch eine Rechteeskalation die Nutzerrechte zu erhöhen.

BlackMatter nutzt das Lightweight Directory Access Protocol (LDAP) und das Server Message Block (SMB) Protokoll, um auf das Active Directory (AD) zuzugreifen und alle Geräte im Netzwerk zu erkennen. Laufende Prozesse und Services werden gestoppt. BlackMatter verschlüsselt dann die gefundenen Systeme und freigegebenen Laufwerke per Fernzugriff, wobei neben den lokal und auf Netzwerklaufwerken gespeicherten Daten auch Wechseldatenträger verschlüsselt werden. Spezifische Verzeichnisse und Daten, die zum Betrieb des Systems benötigt werden, werden nicht verschlüsselt, sodass das Opfer weiterhin Zugriff auf das grundlegende System hat. /CIS21i07, EMS21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Nach eigenen Angaben verzichtet die Gruppierung auf Angriffe auf Ziele kritischer Infrastruktur, staatliche Behörden, Krankenhäuser und gemeinnützige Organisationen und hat lediglich monetäre Interessen. Diese Aussagen erscheinen, da es sich um eine kriminelle Gruppierung handelt unglaubwürdig und wurden durch die Meldung der CISA, des FBI und der NSA, die Angriffe auf kritische Infrastruktur der USA melden, bereits widerlegt. Generell befinden sich unter den Opfern große, über weitreichende (finanzielle) Ressourcen verfügende Organisationen /CIS21i07/, /EMS21w01/. Eigenen Angaben zufolge hat die Gruppierung aufgrund des Drucks der Behörden die Aktivitäten eingestellt /CPO21w03/. Auch diese Aussagen sind vor dem kriminellen Hintergrund der Gruppierung zu betrachten, wobei es zudem für derartige Gruppierungen nicht unüblich

ist, immer wieder unter einem neuen Namen zu agieren, wie es für BlackMatter hinsichtlich DarkSide bereits vermutet wurde.

B.13.8 APT28 – Cyberangriff auf Google

Übersicht

Die vom russischen Staat unterstützte APT-Gruppierung APT28, auch Fancy Bear genannt, führte einen Spear-Phishing Angriff auf die E-Mail-Postfächer von 1.4000 Gmail-Nutzern aus verschiedenen Geschäftsfeldern durch /VER21w01/. Der Angriff wurde Ende September 2021 entdeckt. Das Ziel der Angreifer bestand darin die Postfächer zu übernehmen und Zugriff auf vertrauliche Dokumente und Kommunikationen zu erhalten. Alle E-Mails, die von APT28 gesendet wurden, wurden von Google bereits blockiert. /BSI21i06/

Beschreibung

Ende September 2021 informierte Google 1.4000 Nutzer seines E-Mail-Servers Gmail, dass die APT-Gruppierung APT28 / Fancy Bear einen Spear-Phishing-Angriff auf ihre E-Mail-Postfächer durchgeführt hat mit dem Ziel deren Passwörter zu stehlen, um so Zugriff auf die Postfächer zu erhalten und an die darin enthaltenen Informationen zu gelangen. Nach der üblichen Vorgehensweise von APT28 wären diese Informationen dann genutzt worden, um auf die Postfächer weiterer Personen und die darin enthaltenen Informationen zuzugreifen. Alle schadhaften E-Mails wurden von Gmail jedoch automatisch als Spam-Nachrichten klassifiziert und blockiert. Der Angriff war zwar global, richtete sich aber gegen einen ausgewählten Personenkreis von Aktivisten, Journalisten, Regierungsmitarbeitern, Menschenrechtlern, Rechtsanwälten und Angestellten im Bereich der Nationalen Sicherheit. Insgesamt waren nur 0,1 % der Gmail-Nutzer betroffen. /BSI21i06/, /MAL21w03/, /MOT21w01/

Google empfiehlt Personen, aus den oben genannten Bereichen ihre Gmail-Konten durch die zusätzliche Aktivierung der Schutzmaßnahmen seines Advanced Protection Program (APP) abzusichern. Das APP bietet Schutz gegen Phishing-Angriffe und Malware. Es sieht die Verwendung von physischen USB-Sicherheitsschlüsseln vor, welche häufig in Kombination mit einer weiteren Sicherheitsinformation wie z. B. einem Passwort eingesetzt werden, d. h. einer Zwei-Faktor-Authentifizierung.

Zusätzlich scannt der Google Chrome Browser im APP alle Dateien, die heruntergeladen werden sollen. Dabei werden Dateien abgelehnt, die von unseriösen oder unbekannten Quellen stammen. /BSI21i06/, /VER21w01/, /ZDN21w02/, /MAL21w03/

Die APT-Gruppierung APT28 ist spätestens seit 2004 aktiv. Sie gehört zu Russlands militärischem Geheimdienst und ist Teil des Hauptnachrichtendienstes des russischen Generalstabes (GRU), 85. Haupt-Sonderdienstleistungszentrum (GTsSS), militärische Einheit 26165. APT28 führte 2016 die Cyberangriffe auf die Wahlkampagne von Hillary Clinton und das Nationale Komitee der Demokraten in den USA durch. /BAN21w01/, /REC21w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.9 APT28 – Cyberangriffe im Rahmen einer Brute Force Kampagne

Übersicht

Am 01.07.2021 veröffentlichten die NSA, CISA, das FBI und das britische National Cyber Security Center (NCSC) Advisories zu einer Spionagekampagne der APT-Gruppierung APT28, welche gegen US-amerikanische und europäische Organisationen gerichtet ist. Die Kampagne soll bereits 2019 begonnen haben. /BSI21i08/

Beschreibung

Im Sommer 2020 berichtete die Sicherheitsfirma TrendMicro bereits über die Cyberangriffe, die nach den oben genannten Advisories von 2021 der APT-Gruppierung APT28 zugeordnet werden, welche u. a. unter dem Namen Fancy Bear bekannt ist. Die APT-Gruppierung APT28 ist mindestens seit 2004 aktiv. Die Angriffe richten sich gegen Regierungen und Parteien, das Militär und Verteidigungsunternehmen, Energie- und Logistikkonzerne, Universitäten und Medien sowie Anwaltskanzleien und Medienunter-nehmen in den USA und Europa /NCS21i01/. Die Angriffe erfolgen über Microsoft Office 365 Cloud-Dienste und E-Mail-Server, die eine Vielzahl verschiedener Protokolle verwenden /NCS21i01/. Dabei setzen die Angreifer Brute-Force-Techniken ein und nutzen bekannte Schwachstellen aus, um sich Zugriff auf die Systeme zu verschaffen. /BSI21i08/

Bei einem Brute-Force-Angriff wird von einem Angreifer versucht ein Passwort, einen Benutzernamen, die Adresse einer verborgenen Webseite oder einen Schlüssel nach dem Versuch-und-Irrtum-Prinzip zu erraten. Je nach Komplexität des Passwortes kann dieser Versuch wenige Sekunden bis zu mehreren Jahren dauern. Die Brute-Force-Angriffe von APT28 sind auf geschützte Daten wie E-Mails und die Identifizierung von Kontenanmeldeinformationen ausgerichtet. Diese Informationen werden dann genutzt, um den Erstzugriff auf das Netzwerk, eine persistente Verbindung und eine Privilegien-Eskalation zu erreichen, sowie Schutzfunktionen zu umgehen. /KAS21w02/, /NCS21i01/

Im Zuge der Brute-Force-Kampagne verwendeten die Angreifer das Framework Kubernetes, um die Effektivität der Angriffe zu erhöhen. Ein solches Vorgehen ist zuvor noch nicht beobachtet worden. Das Kubernetes-Cluster, das bei den Angriffen eingesetzt wird, dient dazu Brute-Force-Authentifizierungsversuche zu verschleiern und sie über Tor- und kommerzielle VPN-Dienste weiterzuleiten. /BSI21i08/, /THR21w02/

Darüber hinaus nutzen die Angreifer die Schwachstellen CVE 2020-0688 und CVE 2020-17144 des Microsoft Exchange E-Mail-Servers aus, um per Fernzugriff Programmcode auszuführen und um den Zugriff auf das Zielnetzwerk zu erhöhen. /NCS21i01/ Da die Angriffe auf Default- oder schwache Passwörter abzielen, sind sie leicht zu verhindern, indem starke Passwörter, eine Zwei-Faktor-Authentifizierung (2FA), Sperrungen bei Fehlversuchen oder das Blockieren von VPN- und Tor-Verbindungen verwendet werden. Schutz bietet auch die Umsetzung des Zero Trust Security-Modells. /BSI21i08/, /NCS21i01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.10 REvil – Cyberangriff auf US-Fleischkonzern JBS

Übersicht

Nach einem Cyberangriff auf den weltgrößten Fleischkonzern JBS mit Hauptsitz in Brasilien und Aktivitäten vor allem in Australien, Nord- und Südamerika, der am 30.05.2021 entdeckt wurde, wurden große Teile des Betriebs in den USA, aber auch einige Betriebe in Australien und Kanada vorübergehend stillgelegt. /HEI21w08/, /BLO21w01/, /TEC21w01/

Beschreibung

JBS gab Anfang Juni 2021 bekannt, Opfer eines Cyberangriffs mit Ransomware zu sein. Der weltweit größte Produzent von Rind- und Schweinefleisch wurde dabei Ziel eines organisierten Cyberangriffs, der einige Server der nordamerikanischen und australischen IT-Systeme von JBS betraf. Unmittelbar nach dem Entdecken des Angriffs wurden nordamerikanische und australische IT-Systeme außer Betrieb gesetzt, um das weitere Eindringen zu verhindern, eine mögliche Infektion zu begrenzen und die Kernsysteme zu schützen. Alle Schlachtbetriebe in den USA wurden geschlossen, die Behörden informiert und Fachleute zu Rate gezogen. /SEN21w02/, /BLO21w01/, /TEC21w01/

Da die verschlüsselten Backup-Server von JBS nicht infiziert wurden, erfolgte eine relativ schnelle Wiederherstellung der Systeme und die Rückkehr zum Betrieb innerhalb weniger Tage. / BLO21w01/, /TEC21w01/ Nachdem die Anlagen wieder in Betrieb waren, erfolgte eine Zahlung von umgerechnet 11 Millionen Dollar Lösegeld in Form von Bitcoins. Die Bezahlung erfolgte, um weitere Störungen durch die Angreifer zu verhindern und den reibungslosen Betrieb wiederherstellen zu können. Es kam laut JBS zu keiner Kompromittierung von Unternehmens-, Kunden- und Mitarbeiterdaten. /BBC21w01/, /TAG21w02/

Laut Berichten mehrerer Medien unter Berufung auf das FBI wurde der Cyberangriff von der Gruppierung REvil/Sodinokibi ausgeführt, die aus Russland agiert. /HEI21w09/, /SEC21w13/ Dabei wurde Ransomware eingesetzt, wobei neben der Verschlüsselung von Daten gleichzeitig Spionage und Datendiebstahl betrieben werden sollte, um JBS mit der Androhung einer Veröffentlichung der Daten noch stärker unter Druck zu setzen. Die Gruppierung REvil bietet so genannten Ransomware-as-a-Service (RaaS) an, d. h. sie bietet auch Dritten, die über keinerlei Programmierkenntnisse verfügen, Ransomware gegen Bezahlung an. /SEC21w13/ Der Angriff auf JBS basierte vermutlich auf QBot-Malware, eine modulare Malware, die in der Lage ist, sensible Daten zu kompromittieren. Es wurden Hinweise entdeckt, dass bereits Mitte April 2021 eine QBot-Infektion bei JBS vorlag. /WTW21w01/ Der Zugang zu den IT-Systemen von JBS wurde über ein altes, nicht mehr genutztes Konto erreicht, welches mit einem schwachen Passwort geschützt und nicht deaktiviert worden war. /HIL21w01l/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.11 Conti - Cyberangriff auf den irischen Gesundheitsdienst

Übersicht

Am 14.05.2021 kam es zu einem Cyberangriff auf den irischen Gesundheitsdienst HSE (Health Service Executive), welcher diverse Dienste für alle Krankenhäuser und Gemeinden in ganz Irland bereitstellt. Aufgrund des Angriffs wurde das gesamte Computersystem des irischen Gesundheitsdienstes abgeschaltet, wodurch zahlreiche Krankenhäuser ihren Betrieb einschränken mussten.

Routinetermine wurden vielerorts abgesagt, der Betrieb in den Notaufnahmen lief weiter, war aber beeinträchtigt. /AER21w01, FAZ21w03, TAZ21w01/

Beschreibung

HSE wurde Ziel eines organisierten Cyberangriffs mit der Ransomware Conti, bei dem die IT-Systeme infiltriert wurden. Unmittelbar nach Entdecken des Angriffs wurde von der HSE der Prozess für die Reaktion auf Cyberangriffe in Gang gesetzt, wobei entschieden wurde, alle IT-Systeme abzuschalten und das „National Healthcare Network“ vom Internet zu trennen, um zu versuchen, die Auswirkungen des Angriffs einzugrenzen und zu bewerten. Dies führte dazu, dass alle Mitarbeiter im Gesundheitswesen keinen Zugang mehr zu allen von der HSE bereitgestellten IT-Systemen hatten. Dadurch kam es zu schweren Störungen der Gesundheitsdienste im ganzen Land. /HSE21r01/

Bei dem Angriff sind Dateien verschlüsselt und gestohlen worden und es wurde mit der Veröffentlichung der gestohlenen Patientendaten gedroht. Es wurde ein Lösegeld von 20 Millionen Euro für die Entschlüsselung und Nicht-Veröffentlichung der Daten gefordert, welches nicht gezahlt wurde. Später wurden vertrauliche medizinische Daten von über 500 Patienten sowie Unternehmensdokumente im Internet veröffentlicht. Am 23.06.2021, also mehr als einen Monat nach dem Angriff, waren lediglich 75 % der Daten entschlüsselt und 70 % der IT-Systeme wieder in Betrieb. Es dauerte noch bis Ende September 2021, bis nahezu alle Systeme wieder in Betrieb waren /TAZ21w01/, /IRT21w01/, /RTE21w01/, /BLE21w01/, /HSE21r01/

Laut Berichten mehrerer Medien wurde der Cyberangriff von der Gruppierung Conti ausgeführt, die aus Russland agiert. /TAZ21w01/, /IRT21w02/ Mittels der eingesetzten Ransomware wurde neben der Verschlüsselung von Daten gleichzeitig Spionage und

Datendiebstahl betrieben, um HSE mit der Androhung einer Veröffentlichung der Daten stärker unter Druck zu setzen. /BLO21w02/ Am 16.03.2021 wurde der Angriff mit dem Senden einer maliziösen Phishing-E-Mail an einen Arbeitsplatz begonnen. Dabei wurde eine maliziöse Excel-Datei geöffnet, über welche von den Angreifern der Zugriff auf die Systeme geschaffen wurde. In den darauffolgenden Wochen wurde der Zugriff auf weitere Systeme ausgeweitet. Bereits vor der Ausführung der Ransomware wurden Aktivitäten von einer Antivirensoftware entdeckt. Da diese allerdings nur im Überwachungsmodus arbeitete, wurden die Aktivitäten nicht blockiert. Begünstigt wurde der Cyberangriff durch die IT-Systeme der HSE, die veraltet und nicht gegen Cyberangriffe gewappnet waren. /HSE21r01/

Das National Cyber Security Center stellte fest, dass beim Angriff das käuflich zu erwerbende Penetrationstest-Tool Cobalt Strike verwendet wurde. Mit diesem konnten sich die Angreifer durch die Systeme von HSE bewegen, um diese zu infizieren, ausführbare Dateien zu installieren und eine Variante der Conti-Ransomware zu installieren. /NCS21r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.12 Cyberangriffe mit SparrowDoor

Übersicht

Seit August 2019 greift die APT-Gruppierung FamousSparrow hauptsächlich Hotels aber auch andere Organisationen und Unternehmen (z. B. aus dem Ingenieurwesen) auf der ganzen Welt mit der Backdoor SparrowDoor an. Das Ziel der Angriffe ist vermutlich die Durchführung von Spionageaktivitäten.

Beschreibung

Seit August 2019 nutzt die APT-Gruppierung FamousSparrow Schwachstellen im Microsoft Exchange E-Mail-Server, in Microsoft SharePoint und in Oracle Opera (Software für das Hotelmanagement), um initialen Zugriff auf IT-Netzwerke zu erhalten und dort die Backdoor SparrowDoor zu verbreiten. Die Angriffe richten sich hauptsächlich gegen Hotels aber auch gegen Regierungen, internationale Organisationen,

Ingenieurunternehmen, Anwaltsfirmen und private Organisationen auf der ganzen Welt, vermutlich mit dem Ziel der Spionage. Von den bisherigen Angriffen waren Kanada, Brasilien, Burkina Faso, Israel, Frankreich, Großbritannien, Guatemala, Litauen, Saudi-Arabien, Südafrika, Taiwan und Thailand betroffen. Am 2. März 2021 veröffentlichte Microsoft Patches für den Exchange Server, um vier unter dem Namen ProxyLogon bekannte Schwachstellen zu schließen /BOR21w01/, /ESE21w01/. Sie ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware, wobei Exchange-Online jedoch nicht von den Schwachstellen betroffen ist /BSI21i03/. Bereits einen Tag nach Veröffentlichung der Patches, wurden die Schwachstellen von FamousSparrow für die Verbreitung von SparrowDoor ausgenutzt. /ESE21w02/, /THP21w01/

Haben die Angreifer sich initialen Zugriff auf das Netzwerk einer Organisation verschafft, installieren sie eine Vielzahl von Schadsoftware-Werkzeugen: Eine Variante von Mimikatz für die laterale Bewegung im Netzwerk, eine Komponente, die die Befehlszeilenanwendung ProcDump installiert und diese vermutlich nutzt, um Zugangsdaten aus Speichern auszulesen, den NetBIOS-Scanner Nbtscan, um Dateien und Drucker in einem LAN-Netzwerk zu identifizieren und schließlich einen Loader für die Backdoor SparrowDoor. Der Loader wiederum installiert dann die Backdoor, wobei ein Eintrag in der Registry von Windows erzeugt wird, um eine persistente Verbindung herzustellen. SparrowDoor verbindet sich mit dem Command-and-Control-Server (C&C) der Angreifer über Port 443 (HTTPS) und stellt verschiedene Funktionen bereit. Über SparrowDoor können Dateien umbenannt oder gelöscht werden. Weitere Funktionen sind das Erstellen von Ordnern, das Beenden von Prozessen, das Senden von Dateiinformationen (Attribute, Größe und Erstellzeitpunkt) sowie das Auslesen von Dateien und das Schreiben von Daten in Dateien. Darüber hinaus besitzt die Backdoor einen Kill-Switch, um die Einstellungen für die persistente Verbindung und die Backdoor selbst löschen zu können. /ESE21w02/, /THP21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.13 Cyberangriff auf WestRock

Übersicht

Am 23.01.2021 kam es zu einem Cyberangriff auf WestRock, dem zweitgrößten Unternehmen zur Produktion von Verpackungen wie beispielsweise Kartons in den USA. Der An-griff hatte sowohl Auswirkungen auf das IT-Netzwerk (Büro-Netzwerk) als auch auf das OT-Netzwerk). Aufgrund des Angriffs wurden diverse Systeme proaktiv abgeschaltet, um eine weitere Ausbreitung zu verhindern. Durch den Angriff wurden mehrere Produktionsprozesse außer Betrieb gesetzt. /SEC21w14/, /THR21w03/, /SEC21w15/, /DAR21w03/

Beschreibung

WestRock wurde Ziel eines Cyberangriffs mit Ransomware, bei dem sowohl IT- als auch OT-Systeme betroffen waren.

Durch den Angriff wurden einige der wichtigsten OT-Systeme von WestRock beeinträchtigt, wodurch es zu Auswirkungen auf die Produktion kam. Hinsichtlich der eingesetzten Ransomware und der Fragen, ob ein Lösegeld gezahlt wurde, ggf. wie und von wem der Angriff eingeleitet wurde, liegen keine Informationen vor. /HEI21w10/, /SEC21w14/

Unmittelbar nach der Entdeckung des Angriffs wurde mit Untersuchungen zu dem Angriff und dessen Auswirkungen begonnen. Mit Unterstützung von externen Experten zur Informationssicherheit wurden Maßnahmen zur Eingrenzung der Auswirkungen getroffen. Außerdem wurden sofort Bemühungen aufgenommen, die Systeme wiederherzustellen und den Geschäftsbetrieb aufrechtzuerhalten und die Auswirkungen auf Kunden und Mitarbeiter zu minimieren. Es gibt keine Hinweise darauf, dass durch den Angriff Daten von Kunden oder Mitarbeitern kompromittiert wurden. /SEC21w14/, /THR21w03/

Trotz der sofortigen Aufnahme von Maßnahmen zur Eingrenzung der Auswirkungen und zur Wiederherstellung der Systeme waren auch mehr als zwei Wochen nach dem An-griff noch nicht alle Systeme wiederhergestellt. Dies führte zu Verzögerungen im Geschäftsbetrieb und bei der Warenproduktion, die um 85.000 Tonnen niedriger lag als geplant, was in etwa einem Produktionsausfall von zwei kompletten Tagen entspricht.

Der Angriff hatte Auswirkungen auf den Nettoumsatz von etwa 189 Millionen US-Dollar und auf das Quartalsergebnis von etwa 80 Millionen US-Dollar. Zusätzlich entstanden Kosten von etwa 20-Millionen US-Dollar für die Wiederherstellung der Daten, was hauptsächlich auf Ausgaben für externe Experten zurückzuführen ist. /SEC21w14/, /THR21w03/, /CSO22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.14 Cuba –IT- Angriffe auf kritische Infrastruktur

Übersicht

Eine russische APT-Gruppierung kompromittierte mit Hilfe der Cuba-Ransomware mindestens 49 Einrichtungen im Bereich der kritischen Infrastrukturen und erbeutete dabei 43,9 Millionen Dollar an Lösegeld für die Wiederherstellung der von ihnen verschlüsselten Daten. Bei den Angriffen kam eine Vielzahl an Schadsoftware-Komponenten und Angriffstechniken zum Einsatz.

Beschreibung

Bei den Angreifern, die die Cuba-Ransomware einsetzen, handelt es sich um eine russische APT-Gruppierung. Sie kompromittierten mindestens 49 Einrichtungen im Bereich der Kritischen Infrastrukturen und erbeuteten dabei 43,9 Millionen Dollar. Ursprünglich hatten die Angreifer sogar 74 Millionen Dollar Lösegeld für die Wiederherstellung der von ihnen verschlüsselten Daten gefordert. Zu den Angriffszielen gehören der Finanz-sektor, Behörden und Regierungen, Gesundheitsorganisationen sowie Produktions- und Informationstechnik-Unternehmen in den USA, Südamerika und Europa. /CPO21w02/, /ZDN21w03/

Die Cuba-Ransomware wurde bei den Angriffen unter Zuhilfenahme der Hancitor-Malware verteilt. Diese lädt Diebstahl-Ransomware wie Remote Access Trojaner (RATS) auf die Netzwerke der Opfer. Darüber hinaus verschaffen sich die Angreifer über Phishing-E-Mails, die Ausnutzung von Microsoft Exchange-Schwachstellen und kompromittierte Zugriffsrechte, sowie über Remote-Desktop-Protokolle (RDP) Zugriff auf die Netzwerke. Die Login-Rechte der RDP wurden zuvor durch den Einsatz des Programms

Mimikatz gestohlen. Die Angreifer nutzen legitime Windows Systemdienste wie PowerShell und PsExec und Windows Administratorrechte, um die Cuba-Ransomware auf dem infizierten Netzwerk auszuführen. Diese lädt zwei zusätzliche Payloads, eine zum Diebstahl von Passwörtern und eine zum Aufbau einer Kommunikationsverbindung zum C&C-Server der Angreifer, dessen URL sich in Montenegro befindet. Schließlich verschlüsselt die Cuba-Ransomware Dateien und benennt deren Dateiendung in .cuba um. /CPO21w02/

Die Angreifer verlangen eine Lösegeldzahlung, nach deren Überweisung die Dateien angeblich wiederhergestellt würden. Seit Beginn des Jahres 2021 betreibt die APT-Gruppierung eine Leak-Webseite, auf der sie erbeutete Daten veröffentlicht, sollte das Lösegeld nicht überwiesen werden. Darüber hinaus wurden einige der gestohlenen Daten von den Angreifern verkauft. /PRB21w01, ZDN21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.15 Conti – Cyberangriff auf ONTEC

Übersicht

Am 08.11.2021 wurde festgestellt, dass es zu einem Cyberangriff auf die ONTEC Automation GmbH, einem Unternehmen des Maschinen- und Anlagenbaus und Spezialist für den Bau von Automatisierungssystemen und Sondermaschinen für die industrielle Produktion, gekommen ist. Damit ist durch diesen Angriff ein Unternehmen betroffen, welches industrielle Steuerungssysteme herstellt. Aufgrund des Angriffs kam es zur Verschlüsselung der IT-Infrastruktur des Unternehmens. /UNT21w01/

Beschreibung

Die deutsche ONTEC Automation GmbH wurde Ziel eines Cyberangriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Conti bekannt hat /RED21w01/. Laut /FRA21w01/ mit Bezug auf eine ONTEC Presseerklärung wurde der Angriff frühzeitig erkannt und es umgehend Gegenmaßnahmen eingeleitet. Im Zuge dieser Maßnahmen wurden IT-Systeme abgeschaltet, es kam aber dennoch zu einer Verschlüsselung weiter Teile der IT-Systeme.

Dadurch, dass die Daten wiederhergestellt und Systeme neu aufgesetzt werden mussten, kam es möglicherweise zu Verzögerungen in der Geschäftsabwicklung, wobei die Produktion und die Erreichbarkeit laut /UNT21w01/ nicht betroffen waren. Konkrete Angaben zum Angriffszeitpunkt und zu den detaillierten Auswirkungen liegen nicht vor. Ebenfalls liegen keine Angaben zur Höhe eines möglicherweise geforderten Lösegeldes vor.

Conti ist eine bekannte Ransomware-Gruppierung, die von einer russischen Gruppierung betrieben wird und bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. In der Regel verschafft sich Conti Zugang zu einem Unternehmensnetzwerk, nachdem ein Gerät durch einen Phishing-Angriff mit den Schadprogrammen Bazar-Loader oder TrickBot infiziert wurde. Darauffolgend breitet sich Conti lateral im Opfernetzwerk aus und stiehlt Daten, die auf Conti-Server geladen werden. Dann erfolgt die Verschlüsselung der Daten und die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie. Es wird ein Lösegeld für die Entschlüsselung der Daten verlangt. Wird dieses nicht gezahlt, werden die Daten nicht entschlüsselt und außerdem veröffentlicht. /BLE22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.16 Tiny Turla- Globale Cyberangriffe

Übersicht

Im Rahmen der Cyberangriffe der APT-Gruppierung Turla (siehe Abschnitt 2.10.13) kam es zum Einsatz der neuen Schadsoftware Tiny Turla. Die Schadsoftware Tiny Turla wurde im September 2021 entdeckt, aber bereits seit 2020 genutzt, um Systeme in den USA, Afghanistan und Deutschland zu kompromittieren. /BSI21r04/

Beschreibung

Tiny Turla soll als heimliche Rückfall-Backdoor genutzt worden sein, um den Zugriff auf das System aufrechtzuhalten, wenn die primär von der APT-Gruppierung Turla genutzte Schadsoftware entfernt wurde. Die Schadsoftware ist dabei nicht aufgefallen, da sie über einen recht einfachen, aber effizienten Code verfügt. Sie ist auf die Nutzung

grundlegender Aufgaben beschränkt, wie das Herunterladen, Hochladen und Ausführen von Dateien. /TAL21r01/, /BLE21w02/, /BSI21r04/ Die primäre Schadsoftware ist in Abschnitt 2.10.13 zur APT-Gruppierung Turla und in Abschnitt B.6.4 zum Cyberangriff mittels Epic Turla, der als erster Schritt zur Infektion durchgeführt wird, beschrieben.

Tiny Turla wurde als Dienst auf dem infizierten Rechner installiert. Dabei wurde eine .bat-Datei genutzt, um den Dienst als harmlos aussehenden, gefälschten Windows Time-Dienst zu installieren. Um nicht entdeckt zu werden, wurde der Dienst wie ein tatsächlich existierender Windows-Dienst „Windows Time Service“ genannt. Beschreibung und Dateiname lassen ihn wie eine gültige Microsoft-DLL aussehen. Die Schadsoftware kontaktiert den Command-and-Control-Server der APT-Gruppierung Turla über einen verschlüsselten HTTPS-Kanal alle fünf Sekunden, um zu prüfen, ob neue Befehle vorliegen. /TAL21r01/, /BLE21w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Laut /BFV16l01/ zeigten die Angreifer bei Epic Turla ein Interesse an Wirtschaft und Forschung in den Bereichen Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung. Aus diesem Grund ist ein kerntechnischer Bezug bei Tiny Turla nicht auszuschließen.

B.13.17 Cyberangriff auf Vestas

Übersicht

Am 19.11.2021 wurde festgestellt, dass es zu einem Cyberangriff auf Vestas Wind Systems A/S, einem der weltweit größten Hersteller von Windenergieanlagen (kritische Infrastruktur) mit Hauptsitz in Dänemark, gekommen ist. Aufgrund des Angriffs wurden vor-sorglich diverse IT-Systeme an mehreren Standorten abgeschaltet, um eine weitere Ausbreitung zu verhindern. /BSI21r06/, /BLO21w04/

Beschreibung

Vestas wurde Ziel eines Cyberangriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Lockbit bekannt hat. Nach Entdeckung des Angriffs wurden umgehend Ge-genmaßnahmen eingeleitet, wobei als Vorsichtsmaßnahme mehrere

IT-Systeme an mehreren Standorten heruntergefahren wurden. Des Weiteren wurde in Zusammenarbeit mit externen Experten damit begonnen, das Problem einzugrenzen und die Systeme wiederherzustellen. OT-Systeme sind von den Angriffen laut Vestas nicht betroffen gewesen, außerdem sollen keine Daten von Kunden oder Lieferketten entwendet worden sein. Aufgrund der Abschaltung der IT-Systeme können allerdings Kunden, Mitarbeiter und andere Interessengruppen betroffen gewesen sein. Auf bereits betriebene Windenergieanlagen oder die Wartung der Anlagen hatte der Angriff laut Vestas keine Auswirkungen. /BSI21r06/, /BLO21w04/

Trotz der sofort eingeleiteten Maßnahmen zur Eingrenzung der Auswirkungen und Wiederherstellung der Systeme, waren laut /ITD21w01/ am 06.12.2021 zwar die meisten, aber noch nicht alle Systeme wieder betriebsbereit.

Bei dem Angriff wurden von der Ransomware-Gruppierung Lockbit unrechtmäßig Daten gestohlen und es wurde mit einer Veröffentlichung dieser Daten gedroht. Bei den gestohlenen Daten handelte es sich auch um personenbezogene Daten, wobei diese vermutlich nicht in erster Linie das Ziel des Angriffs waren. Es handelte sich ausschließlich um Daten, die auf Vestas internen File-Sharing-Systemen gelagert werden.

Bei den gestohlenen personenbezogenen Daten handelte es sich größtenteils um Namen, Adressen, Telefonnummern sowie Details zur Anstellung wie z. B. Gehalt und Lebenslauf von Mitarbeitern von Vestas. In wenigen Fällen wurden aber auch sensiblere Daten von Vestas-Mitarbeitern wie z. B. Pässe oder Bankdaten gestohlen. Es gibt keine Hinweise darauf, dass personenbezogene Daten gestohlen wurden, die nicht Mitarbeiter von Vestas betreffen. Da Vestas nach eigenen Angaben kein Lösegeld gezahlt hat, wurden alle gestohlenen Daten von Lockbit am 08.12.2022 veröffentlicht, wobei es sich um insgesamt mehr als 7.700 Dateien handelte. Über eine Höhe des geforderten Lösegeldes oder weitere Einzelheiten sind keine Informationen bekannt. /ITD21w01/, /WIN21w01/, /INS21w02/, /SEC21w16/

LockBit ist eine Ransomware-Gruppierung, deren erste Angriffe im September 2019 bekannt geworden sind, wobei die Gruppierung zu diesem Zeitpunkt noch ABCD genannt wurde. /FBI22r01/ Bei LockBit handelt es sich um eine Ransomware-as-a-Service-Gruppierung (RaaS), die laut /REC22w01/ eine der produktivsten aktiven Gruppierungen ist und im Jahr 2022 bereits mindestens 650 Organisationen angegriffen hat (Stand: Ende Juni 2022). Die Gruppierung führt zielgerichtete Angriffe auf Unternehmen und Regierungsorganisationen aus, Privatpersonen sind eher keine Angriffsziele. Es werden

Unternehmen weltweit angegriffen, wobei bewusst Unternehmen mit Standort in Russland gemieden werden.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

B.13.18 Cyberangriffe auf die Vereinten Nationen

Übersicht

Von April 2021 bis August 2021 wurden die Computersysteme der Vereinten Nationen (UN) Opfer mehrerer Cyberangriffe, bei denen Angreifer in die Computersysteme der UN eingedrungen sind. Die Cyberangriffe dienten vermutlich dem Sammeln von Informationen. Systeme oder Dateien wurden nach Aussage der UN nicht beschädigt. Wer für die An-griffe verantwortlich ist und ob außer dem Sammeln von Informationen weitere Motive hinter den Angriffen stehen, ist unklar. /BSI21r05/, /Hei21w11/, /BLO21w03/

Beschreibung

Der erste Angriff dieser Angriffswelle (es gab schon frühere Angriffe auf die UN, die hier nicht betrachtet werden) auf die Computersysteme der UN erfolgte vermutlich am 05. April 2021. Dieser Angriff wurde laut UN erkannt und es wurde darauf reagiert, wobei keine detaillierten Angaben zur Reaktion bekannt sind. Auf diesen Angriff folgten weitere Angriffe, die entdeckt und auf die nach Aussage der UN ebenfalls angemessen reagiert wurde. Nach Recherchen der Cyber-Sicherheitsfirma Resecurity, die den Angriff als erste entdeckt hat, waren die Angreifer bis zum 07. August 2021 im Netzwerk der UN aktiv. /BSI21r05/, /Hei21w11/, /BLO21w03/

Laut Aussage der UN haben die Angreifer keine Systeme beschädigt und keine Dateien entwendet oder verschlüsselt. Laut UN haben sie sich lediglich im Netzwerk umgesehen und Screenshots gemacht. Es existieren gegensätzliche Aussagen von Resecurity, denen zufolge es Beweise zu gestohlenen Daten geben soll. Ungeachtet dessen, ob tatsächlich Dateien gestohlen oder ausschließlich Screenshots gemacht wurden, konnten durch den Angriff Informationen über die Computernetzwerke der UN gesammelt werden. Die somit gesammelten Daten könnten von den Angreifern zum Kauf angeboten oder verwendet werden, um weitere Angriffe auf die UN oder andere Organisationen

durchzuführen. In der Zeit von April bis August 2021 wurde mit den gesammelten Daten aus dem ersten Angriff versucht, mindestens 53 weitere Konten von Nutzern des UN-Netzwerks zu kompromittieren, möglicherweise mit dem Motiv langfristig weitere Daten sammeln zu können. /BSI21r05/, /Hei21w11/, /BLO21w03/

Der Zugriff auf das Computersystem der UN durch die Angreifer erfolgte über die Projektmanagement-Software Umoja, einer proprietären, UN-eigenen Software. Es ist keine Sicherheitslücke in der Software bekannt, der Zugriff auf die Software erfolgte über einen gestohlenen Benutzernamen und das Passwort eines UN-Mitarbeiters, die von den Angreifern im Darknet erworben wurden. Die Zugangsdaten wurden im Darknet von mehreren russischsprachigen Personen angeboten und waren Teil eines Paketes mit Dutzenden Benutzernamen und Passwörtern von verschiedenen Organisationen, welches für 1.000 US-Dollar verkauft wurde. Der Zugriff über die Software Umoja ermöglichte einen tieferen Zugang zum Computersystem der UN und die Auskundschaftung des Netzwerkes. Es wurde der Versuch unternommen, die Rechte zu erweitern. Zum Zeitpunkt der ersten Angriffe verfügte die Software Umoja nicht über eine Multifaktor-Authentifizierung beim Login, welche den Angriff möglicherweise hätte verhindern können. Erst im Juli 2022 gab das Entwicklungsunternehmen von Umoja bekannt, dass eine Multifaktor-Authentifizierung beim Login implementiert wurde. /BSI21r05/, /Hei21w11/, /BLO21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.19 Ransomware – Cyberangriff auf Sogin

Übersicht

Im Dezember 2021 bestätigte das italienische Unternehmen Sogin, Opfer eines Cyberangriffs geworden zu sein. Bei Sogin handelt es sich um eine staatliche Firma, die vom italienischen Wirtschafts- und Finanzministerium finanziert wird und die sich um den Rückbau der italienischen Kernkraftwerke und nukleare Entsorgung einschließlich sonstiger radioaktiver Stoffe kümmert. Parallel dazu wurden bei diesem Angriff mutmaßlich gestohlene Unterlagen im Darknet zum Verkauf angeboten.

Beschreibung

Am 13.12.2022 gab das italienische Unternehmen Sogin bekannt, Opfer eines Cyberangriffs geworden zu sein. Sogin betonte dabei, dass die konventionelle und die nukleare Sicherheit der betreuten Anlagen und ihres Betriebes zu jeder Zeit gewährleistet gewesen seien. Details zum Angriff gab Sogin nicht bekannt. Gleichzeitig tauchten aber im Darknet mutmaßlich bei Sogin entwendete Daten zum Verkauf auf. Betroffen waren sensible Dokumente verschiedener Art. Darunter befanden sich beispielsweise Passwörter im Klartext, Ausschreibungen, technische Zeichnungen von Maschinen und Anlagen, Kostenvoranschläge, eine Karte eines von Sogin verwalteten Standorts, eine Liste der angeforderten Software- und Hardware-Updates, Lebensläufe von Mitarbeitern, Reiseberichte, Fotos von Besprechungen sowie Informationen zum Betrieb eines Arbeitsplatzes, der auf industrieller Ebene zur Anlagenüberwachung eingesetzt wird. Zusätzlich enthielten die angebotenen Daten auch persönliche Inhalte, was darauf hindeutet, dass das Material durch das Eindringen in einen Firmencomputer gestohlen worden sein könnte, der gleichzeitig für private Zwecke genutzt wurde. Es wird vermutet, dass die Angreifer über diese private Nutzung Zugang zu dem betroffenen Rechner erhielten. Eine offizielle Bestätigung hierfür liegt aber nicht vor. /WOR21w01/

Kerntechnischer Bezug

Da es sich bei Sogin um ein Unternehmen handelt, das für den Rückbau kerntechnischer Anlagen und die Entsorgung bzw. Lagerung radioaktiver Stoffe verantwortlich ist, besteht ein klarer kerntechnischer Bezug.

B.13.20 SquirrelWaffle-Loader

Übersicht

Im September 2021 wurde der Schadsoftwareloader SquirrelWaffle-Loader von IT-Sicherheitsforschern entdeckt, analysiert und veröffentlicht. SquirrelWaffle ist ein weiterer auf E-Mail Spam basierter Loader, welcher die Erstinfektion eines IT-Systems erreichen soll. Die hierzu genutzten E-Mails enthalten mit Makros versehene Microsoft Word oder Excel Dokumente und ermöglichen bei Ausführung der Makros eine vollautomatische Installation der Schadsoftware. /SEN21w03/

Beschreibung

Moderne Schadsoftwares sind zumeist modular aufgebaut, wobei bestimmte Aufgaben von verschiedenen Schadsoftwares übernommen werden. So übernimmt ein Modul die Verbreitung innerhalb eines Netzwerkes, ein anderes Modul die Ausspähung von wichtigen Daten auf betroffenen Systemen, ein weiteres Modul führt die Verschlüsselung aus und schließlich übernehmen Loader die Aufgabe der erstmaligen Infektion. Die Ansprüche an Schadsoftwareloader sind daher stetig mit steigenden Sicherungsmaßnahmen gewachsen. Ein und derselbe Schadsoftwareloader wird zum Teil bei völlig unterschiedlicher Schadsoftware, z. B. Ransomware oder Bankingtrojaner eingesetzt. Die Loader werden von den Entwicklern verkauft, vermietet oder zur freien Benutzung bereitgestellt. /SEN21w03/

Im September 2021 wurde eine neue Kampagne der Schadsoftwares Cobalt Strike und QakBot, zwei multifunktionalen Schadsoftwares, entdeckt. Beide nutzten für die Verbreitung sogenannte E-Mail-Antwortkettenangriffe, wobei bestehende Email-Korrespondenzen übernommen werden oder neue Emails den Anschein einer längeren Korrespondenz erzeugen sollen. Werden die mitversendeten Word oder Excel Dateien des E-Mail Anhangs von den Nutzern ausgeführt, wird mittels Makro-Kette die Schadsoftware initialisiert. /SEN21w03/

Die Infektion findet dabei über ein PowerShell Skript statt, mit welchem die Daten des SquirrelWaffle Loaders auf dem betroffenen System festgeschrieben werden. Der Loader nutzt hierbei zur Verschleierung z. B. zufällige Dateinamen und besitzt damit Fähigkeiten zur Nichterkennung durch Sicherungssoftwares.

Nach erstmaliger Installation des SquirrelWaffle Loaders kontaktiert der Loader die C&C Infrastruktur, um Schadsoftware nachzuladen. Die Kommunikation zur C&C Infrastruktur wird dabei so weit wie möglich verschleiert. Konkrete Schadwirkungen werden über die als .txt Dateien nachgeladenen Schadsoftwares Cobalt Strike und Qakbot erreicht. /SEN21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14 2022

B.14.1 WhisperGate – Cyberangriffe auf ukrainische Einrichtungen

Übersicht

Mitte Januar 2022 wurde eine neue Schadsoftware bekannt, die Berichten zufolge vornehmlich gegen Ziele in der Ukraine – darunter Regierungseinrichtungen, Non-profit-Organisationen und IT-Organisationen – eingesetzt wurde und wird. Dabei handelt es sich um einen Wiper, der unter dem Deckmantel eines Ransomware-Angriffs den Master Boot Record des angegriffenen Systems zerstört. Die Schadsoftware wurde unter dem Namen WhisperGate bekannt.

Beschreibung

Bei WhisperGate handelt es sich um einen sogenannten 3-stufigen MBR (Master Boot Record) Wiper. In Schritt 1 wird der Master Boot Record überschrieben, ebenso Teile aller verbundenen Laufwerke. In Schritt 2 wird die Schadsoftware für Schritt 3 heruntergeladen und ausgeführt. In Schritt 3 werden alle Dateien mit einer Liste von 191 Dateiendungen abgeglichen und bei Übereinstimmung der Dateiendungen gelöscht.

Insgesamt beschädigt WhisperGate ein Windows-System so weit, dass Dateien und Laufwerke nicht mehr funktionsfähig und auch nicht wiederherstellbar sind. In Schritt 1 gibt WhisperGate Meldungen heraus, wie sie üblicherweise im Rahmen eines Ransomware-Angriffs angezeigt werden. So wird nach dem Reboot eine Ransomware-Nachricht angezeigt, die allerdings nur als Maskerade dient. WhisperGate besitzt keinerlei Wiederherstellungsmechanismen und versetzt ein erfolgreich kompromittiertes System in einen nicht wiederherstellbaren Zustand. Zusätzlich zur Maskerade als Ransomware nutzt die Schadsoftware auch Verschleierungsmechanismen, um einer Detektion oder Analyse zu entgehen. /REC22w02/

IT-Sicherheitsforscher sehen Parallelen zwischen WhisperGate und NotPetya (siehe Abschnitt B.14.1 und B.9.6), allerdings gilt WhisperGate als weniger komplex. Ein wesentlicher Unterschied zu NotPetya besteht darin, dass WhisperGate gleichzeitig zum Überschreiben des Master Boot Record auch versucht, die Partition C:/ zu überschreiben. /COM21w01/

Ein weiterer Aspekt, der von IT-Sicherheitsforschern hervorgehoben wird, bezieht sich auf die Einschleusung der Schadsoftware bei den Angriffszielen. Demnach ist es wahrscheinlich, dass die Angreifer über gestohlene Zugangsdaten bereits einige Zeit vor den Angriffen Zugriff auf Systeme bei den Angriffszielen hatten.

WhisperGate ist eine destruktive Schadsoftware, bei der weder Manipulation noch finanzieller Gewinn als Zielsetzung im Vordergrund steht, sondern vielmehr das Ziel, IT-Systeme in einen nicht wiederherstellbaren, funktionsunfähigen Zustand zu versetzen.

Hinter den Angriffen mit WhisperGate wird eine staatlich geförderte Angreifergruppierung vermutet. Bislang konnten die Angriffe keiner bekannten APT-Gruppierung zugeordnet werden, die Aktivitäten werden zunächst unter DEV-0586 weiterverfolgt.

Es wurde festgestellt, dass ein Großteil der angegriffenen Websites – hauptsächlich ukrainische Regierungswebsites – dasselbe Content-Management-Programm benutzen. Daher lag die Vermutung nahe, dass die Angreifer eine Schwachstelle in eben diesem Programm, OctoberCMS, ausnutzten. In der weiteren Folge wurde bekannt, , dass die Mehrheit der Websites von ein und derselben ukrainischen Firma erstellt und betreut wurden, welche im Vorfeld -kompromittiert worden war. Dies machte es den Angreifern möglich, die Rechte und Zugangsdaten der betreuenden Firma bei deren Kunden zu missbrauchen. Dies legt den Verdacht nahe, dass WhisperGate in vielen Fällen über die Lieferkette eingebracht wurde.

Kerntechnischer Bezug

Der Fokus der bislang mit WhisperGate durchgeführten Angriffe lag auf ukrainischen Einrichtungen. Momentan ist nicht davon auszugehen, dass deutsche kerntechnische Anlagen derzeit zu den anvisierten Angriffszielen zählen. Bislang gibt es weder einen Bezug zu kerntechnischen Anlagen und Einrichtungen noch zu kritischen Infrastrukturen. Allerdings ist WhisperGate auf die Kompromittierung und Zerstörung von Windows-Systemen ausgerichtet, welche auch in deutschen kerntechnischen Anlagen in großer Anzahl vorhanden sind. Daher muss davon ausgegangen werden, dass die Schadsoftware bei entsprechendem Zugang zu den IT-Systemen, auch in deutschen kerntechnischen Anlagen einsetzbar wäre.

B.14.2 AcidRain – Cyberangriff auf die Satellitenkommunikation via KA-Sat

Übersicht

Am 26.02.2022 informierte Paxex.aero über einen Ausfall der Satelliten-basierten Kommunikation via KA-SAT, der auch Auswirkungen auf die Satelliten-basierte Breitbandversorgung in Europa hat. Vom BMUV wurde am 01.03.2022 eine kurzfristige Ersteinschätzung dieses Sachverhalts erbeten.

Beschreibung

Bei KA-SAT (KASAT Viasat) handelt es sich um einen Kommunikationssatelliten der US-amerikanischen Firma Viasat. Ursprünglich wurde KA-Sat im Auftrag der französischen Firma EUTELSAT Ende 2010 ins All befördert. Im April 2021 erwarb Viasat den Anteil von EUTELSAT an der Euro Broadband Infrastruktur (EBI), seither wird der Satellit auch unter der Bezeichnung KASAT Viasat geführt /VIA21w01/. EUTELSAT betreut derzeit noch die Infrastruktur am Boden, während Viasat die bereitgestellten Dienste betreut. Der Satellit bewegt sich auf einem geostationären Orbit bei 13 Grad Ost.

Der Satellit verwendet für den Uplink 28-30 GHz, dieser erfolgt also im Ka-Frequenzband (26 bis 40 GHz), während der Downlink im Bereich 18,4 bis 20,2 GHz und daher im K-Frequenzband (18 bis 26 GHz) erfolgt. Mit 82 Spotbeams erreicht er eine europaweite Abdeckung (siehe Abb. B 1).

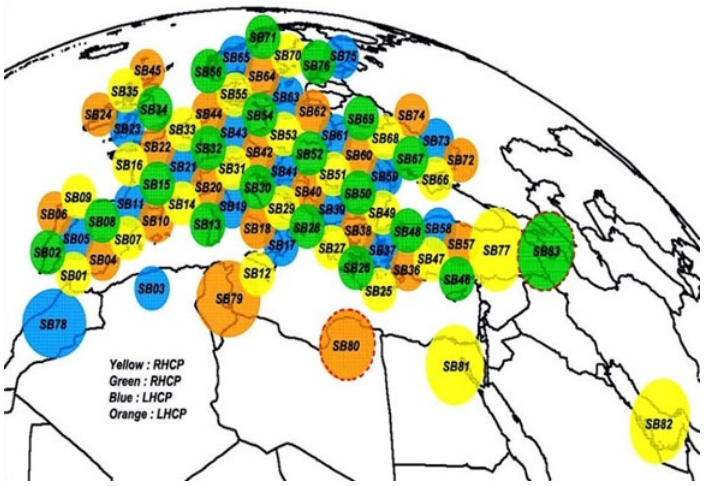

Abb. B 1 Europaweite Abdeckung durch Spotbeams des KA-SAT

Unterschiedliche Farben weisen unterschiedliche Frequenzen bzw. Polarisierungen aus /FRE16w01/

Jeder Spotbeam erlaubt eine Datenübertragung von bis zu 900 Megabit/s, insgesamt erreicht KA-SAT daher eine Gesamtkapazität von etwa 80 Gigabit/s. KA-SAT ist für das Routing des Datenverkehrs mit einem Netzwerk aus Bodenstationen verbunden. Über KA-SAT bietet Viasat Satelliteninternet für Europa und den Mittelmeerraum mit Daten-übertragungsraten von bis zu 50 MBit/s im Download. /BSI22r01/, /TEC10w01/

Die Spotbeams werden über acht europaweit verteilte Bodenstationen angebunden, sog. Gateways. Zwar sind die Beams relativ unabhängig voneinander, ein Ausfall eines Gateways wirkt sich aber auf alle damit verbundenen Beams aus. /IDW22w01/

Der Sachverhalt des Ausfalls der Satelliten-basierten Kommunikation via KA-SAT stellt sich auf Basis der bis zum 02.03.2022 vorliegenden Informationen folgendermaßen dar:

Am 24. Februar 2022 erfuhr die Kommunikation über den KA-SAT eine Unterbrechung, welche einen teilweisen Ausfall der Dienste des KA-SAT Satellitennetzwerks über Europa nach sich zog. Der Ausfall betraf sowohl Satelliten-basiertes Internet als auch Satelliten-basierte Telefonie. Der Einbruch der Konnektivität ist in Abb. B 2 dargestellt.

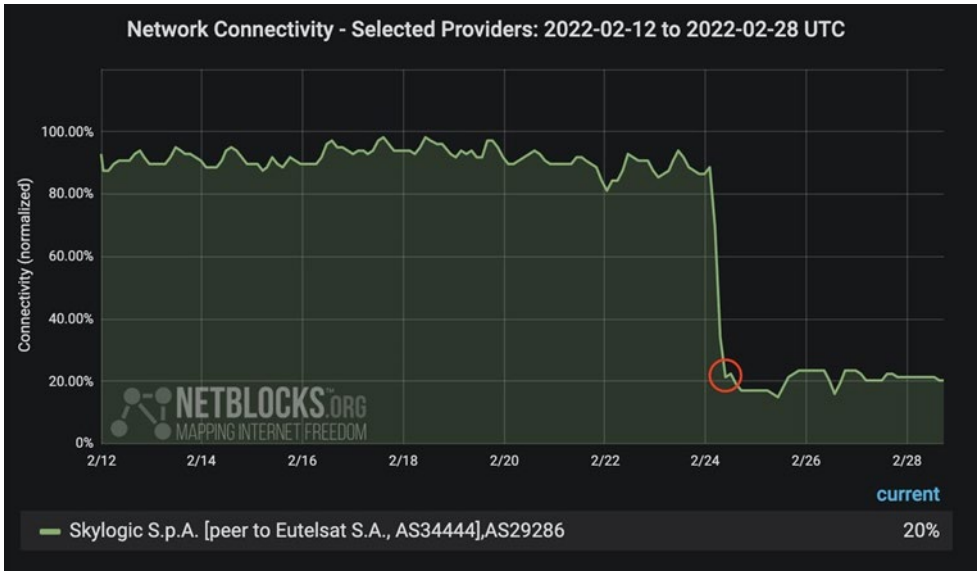

Abb. B 2 Einbruch der Konnektivität von KA-SAT am 24.02.2022

Grafik unverändert übernommen von netblocks.org

Die Störung begann am Donnerstag, den 24.02.2022, um 4 Uhr UTC morgens (entspricht 6 Uhr ukrainischer Zeit) /BSI22r01/, nahezu zeitgleich mit dem Angriff durch russische Streitkräfte auf die Ukraine. Hierbei wird ein Zusammenhang vermutet, Beweise hierzu liegen bisher allerdings nicht vor. Die Störung begann zunächst mit dem KA-SAT

Dienst in der Ukraine und breitete sich anschließend über fast die gesamte KA-SAT-Ausleuchtzone aus /GOL22w01/. Mehrere Internet Service Provider (ISP) melden als Folge des Ausfalls Probleme mit der Satelliten-basierten Breitbandversorgung in Europa. Darunter befinden sich der deutsche ISP EUSANET /BSI22r01/, /PAX22w01/, der tschechische ISP intv.cz /PAX22w01/, ein französischer ISP /PAX22w01/ sowie die schwedische NORDNET /NUM22w01/. Der Betreiber Viasat gab an, dass in Europa „zehntausende“ Kunden von dem Ausfall betroffen waren /REU22w02/.

Der Ausfall von KA-SAT hatte und hat auch Auswirkungen auf kritische Infrastruktur in Deutschland. Hierzu berichtet das BSI: „Der Windkraftanlagenhersteller Enercon berichtet gegenüber der Webseite Golem, dass der KA-SAT-Ausfall auch tausende Windkraft-anlagen betreffe. Demnach sei eine Entstörung in Falle eines Fehlers von 5.800 Anlagen mit einer Gesamtleistung von elf Gigawatt aus der Ferne nicht möglich. Die Anlagen laufen jedoch autark weiter und die Steuerung ist weiterhin möglich. Nach Angaben des Bundesverbands Windenergie sei nur der Anbieter Euroskypark betroffen. Der KA-SAT Hersteller Viasat teilte der Webseite ZDNet mit, dass die Untersuchung des Ausfalls noch andauere. Man glaube, dass die Störung durch ein "cyber event" verursacht wurde.“

Das BSI fügt dieser Beschreibung folgende Bewertung des BSI-Fachreferats hinzu: „In Folge des KA-SAT-Ausfalls gingen im BSI mehrere Meldungen ein, da der Dienst u. a. zur Fernwartung von Windenergieanlagen genutzt wird. Der Dienst wird durch Wartungsunternehmen von Windanlagen zur Entstörung aus der Ferne genutzt. Durch den Ausfall des Dienstes ist eine zeitnahe Entstörung der Anlagen nicht mehr gegeben. Eine Entstörung im Fehlerfall kann aber bspw. von vor Ort erfolgen. Die betroffenen Anlagen sind weiterhin in der Lage, Strom zu erzeugen und ins Netz einzuspeisen. Für Netzbetreiber, die u. U. netzstabilisierende Maßnahmen ergreifen müssen, stehen redundante Verbindungsmöglichkeiten zur Verfügung. Daher sind Auswirkungen auf die Stromnetzstabilität nicht zu erwarten.“ /BSI22r02/

Die Dienste von KA-SAT kommen auch in anderen kritischen Infrastrukturen wie beispielsweise bei Einsatzfahrzeugen von Feuerwehren und Rettungsdiensten zum Einsatz. Das BSI bezieht sich hierbei auf eine ihm vorliegende Meldung „die beschreibt, dass von der Störung auch Geräte der Gefahrenabwehr wie beispielsweise Satellitenkommunikationssysteme von Einsatzleitfahrzeugen betroffen sind“ /BSI22r03/. In einer Veröffentlichung, die sich hauptsächlich an Betreiber von Leitstellen zur Gefahrenabwehr wendet, heißt es in einem entsprechenden Bericht: „Immer mehr Einsatzleitfahrzeuge werden mit einer selbstausrichtenden 77-cm-Sende-Empfangs-Antenne und einem ViaSat-Modem nachgerüstet. Bei der Beschaffung neuer ELW taucht in den Ausschreibungen immer öfter das Ausstattungsmerkmal „Satellitenverbindung“ auf. Viele deutsche Feuerwehren und Rettungsdienste nutzen den schnellen Datensatelliten bereits, so z. B. das BRK Traunstein und Berchtesgadener Land, der Kreisfeuerwehrverband Südpfalz, die Feuerwehren in Paderborn und im Landkreis Darmstadt. In der französischen Region Rhône-Alpes sind die Feuerwachen bereits via KA-SAT miteinander verbunden und sogar die Administration des Service de Secours in Luxemburg hat sich für eine Satellitenlösung entschieden“ /BOS17r01/. Da sich dieser Bericht auf den Stand von 2017 bezieht, ist davon auszugehen, dass die Kommunikation über KA-Sat bei Ein-satzfahrzeugen inzwischen breiter verbreitet ist, als hier umrissen. Auf eine Reihe von Anfragen im Rahmen der Informationstransparenz äußerten sich die Kreisverwaltung Südliche Weinstraße und die Kommunalverwaltung Paderborn zur Frage der Betroffenheit durch den KA-SAT Ausfall sowie vorhandene Rückfall-Lösungen. Beide bestätigten die Betroffenheit und gaben an, die Anbindung über KA-SAT nicht standardmäßig, sondern als Rückfallebene zu nutzen. Es wurde angegeben, dass die Primärlösungen im Gegensatz zur Kommunikation über KA-SAT von der Störung nicht betroffen, sondern voll funktionsfähig seien.

Es ist inzwischen bekannt, dass über KA-SAT auch Satellitenkommunikation für die ukrainische Polizei und das ukrainische Militär bereitgestellt wird /REU22w02/. Am 15.03.2022 sprach der stellvertretende Leiter der ukrainischen Behörde für Sonderkommunikation und Informationsschutz, Victor Zhora, in diesem Zusammenhang von einen „sehr großen Verlust an Kommunikation gleich zu Beginn des Krieges". /REU22w03/

Da Viasat KA-SAT erst 2021 erworben hat, war dessen Netzwerk zum Zeitpunkt der Störung noch nicht in das Netzwerk von Viasat integriert, sondern operierte nach Aussage von Viasat in einem Stand-Alone-Netzwerk. Daher waren die vier anderen von Viasat betriebenen Satelliten von der Störung nicht betroffen. /SAN22w01/

Die betroffenen ISPs gaben in eigenen – von Seiten des Betreibers unbestätigten – Meldungen bereits frühzeitig erste Informationen zu einer möglichen Ursache bekannt. So berichtete intv.cz von einem nicht näher spezifizierten Angriff auf die Bodeninfrastruktur von KA-SAT während EUSANET angab, derzeit noch keine Ursachen zu kennen, aber einen zeitlichen Zusammenhang mit dem Ereignissen in der Ukraine herstellte. /HEI22w01/, /PAX22w01/ Der Betreiber Viasat beauftragte ein externes Cybersicherheitsunternehmen mit der Untersuchung und gab frühzeitig an „die Untersuchung des Ausfalls dauert noch an, aber bislang halten wir einen Cyberevent für die Ursache“ /REU22w01/. Der britische Nachrichtensender Sky News stellte unter Berufung auf einen Insider eine Verbindung zwischen dem teilweisen Ausfall von KA-SAT und den DDoS-Angriffen her, die kurz vor Beginn der russischen Invasion auch eine Reihe von Webseiten von Banken und Regierungseinrichtungen lahmlegte /SKY22w01/. Sky News berichtete darüber hinaus, dass bei der Ursachenklärung auch eine russische Beteiligung untersucht werde /SKY22w01/. Das französische Verteidigungsministerium bestätigte schließlich am 03.03.2022, dass der Ausfall von KA-SAT auf einen Cyberangriff zurückgeht /NUM22w01/. Kurz darauf erfolgte auch die Bestätigung von Viasat, dass der Ausfall von KA-SAT auf einen vorsätzlichen Cyberangriff zurückgeht.

Die derzeit öffentlich verfügbaren Informationen legen nahe, dass der Angriff zunächst den KA-SAT SATCOM Terminals (Terminals bestehen aus Antenne und Mo-dem) in der Ukraine galt, sich der Angriff aber schnell in andere Länder ausbreitete. Konkret genannt werden neben der Ukraine, Deutschland, Tschechien und Frankreich auch Griechenland, Polen, Italien und Ungarn. Auch mehren sich die Aussagen dazu, dass eine große Anzahl Terminals nachhaltig beschädigt wurden /HEI22w01/. So berichtet beispielsweise das BSI in seinem Tageslagebericht vom 02.03.2022 von einer Meldung eines Providers, der von der KA-SAT-Störung betroffen ist.

Dieser Provider berichtet nach Angaben des BSI, „dass bei allen aktiven Consumer-Modems ein Update durchgeführt wurde, welches die Modems nachhaltig zerstöre.“ /BSI22r03/

Der Angriff stellt sich auf Basis der aktuell verfügbaren Informationen wie folgt dar:

Viasat selbst beschreibt den Angriff als mehrstufig. Zunächst erfolgte ein DoS-Angriff, der von mehreren SurfBeam2 Modems und anderem in der Ukraine befindlichen Equipment ausging. Aufgrund dieses DoS-Angriffs gingen viele KA-Sat Modems zeitweise offline. Anschließend war zu beobachten, wie zahlreiche Modems nach und nach ihre Verbindung verloren. Die Angreifer erlangten über die Fehlkonfiguration einer VPN Anwendung Zugriff auf das sogenannte Trusted Management Segment des KA-Sat-Netzwerks. Anschließend erfolgte eine laterale Bewegung des Angreifers durch dieses Segment zu einem Segment, das für Management und Betrieb des Netzwerks verwendet wird. Von diesem Segment aus führten die Angreifer zeitgleich bei einer großen Anzahl Modems gezielte Befehle zum Netzwerkmanagement aus. Unter Anwendung von legitimen Befehlen zum Netzwerkmanagement führten die Angreifer eine ausführbare Schadsoftware auf den Modems aus. Dabei handelte es sich um einen Wiper namens „AcidRain“, der wesentlichen Daten im Flash-Speicher der Modems überschrieb, so dass diese nicht mehr betrieben werden konnten. Eine Wiederherstellung war nur noch durch Reflashing beim Hersteller möglich. /SEN22w02/

Zunächst empfahl Viasat allen Kunden, bei offline befindlichen Modems keinen Versuch der Verbindungsherstellung zu unternehmen, um Schäden von diesen abzuwenden. Ab dem 10.03.2022 konnten Modems laut Viasat wieder in Betrieb genommen werden. Gleichzeitig wurde bekannt gegeben, dass dabei „durch den Angriff in Mitleidenschaft gezogene Modems ersetzt“ werden müssten. Viasat gab an, etwa 30.000 neue Modems an Kunden ausgeliefert zu haben, um eine Wiederherstellung der Dienste zu beschleunigen. Durch den notwendigen Austausch zog sich die Wiederherstellung über Wochen hin. So gab beispielsweise der deutsche Windkraftanlagenhersteller ENERCON am 15.03.2022 bekannt, dass noch 85 % seiner Modems offline seien und die vollständige Wiederherstellung wohl noch Wochen dauern könne /REU22w03/. Am 19.04.2022 gab ENERCON bekannt, dass 95 % der betroffenen Anlagen wieder in die Fernwartung und -überwachung eingebunden seien.

Kerntechnischer Bezug

Satelliten-basierte Kommunikation wird auch in deutschen Kernkraftwerken und anderen kerntechnischen Anlagen eingesetzt, beispielsweise als diversitäre Kommunikationsmöglichkeit im Krisenfall, beispielsweise für die Polizeidirektverbindung. Bislang ist der GRS aus keiner deutschen kerntechnischen Anlage der Einsatz von KA-SAT bekannt. Grundsätzlich ist der Ablauf des Angriffs allerdings auch auf andere Kommunikationssatelliten, wie sie auch in deutschen Kernkraftwerken eingesetzt werden, möglich. Der Einsatz einer vergleichbaren Wiper-Schadsoftware könnte auch Modems anderer Anbieter, unabhängig vom genutzten Kommunikationssatelliten, in ihrer Funktionalität nachhaltig beeinträchtigen. Aus Sicht der GRS besteht eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Ersteinschätzung ausgewertet, eine Stellungnahme wird derzeit erstellt.

B.14.3 Killnet – Cyberangriffe auf Webseiten von Regierungseinrichtungen

Übersicht

Bei Killnet handelt es sich um eine prorussische Hacktivistengruppierung, die durch kriegsbegleitende Angriffe vornehmlich in Europa auffällt. Dabei greift sie zumeist zu DDoS-Angriffen, mit denen sie Webseiten, häufig von Regierungseinrichtungen, lahm-legt. Angegriffen wurden seit Beginn des Krieges in der Ukraine beispielsweise Ziele in Deutschland, Rumänien, Litauen und Norwegen.

Beschreibung

Die Hacktivisten-Gruppierung Killnet formierte sich vor dem Hintergrund der wachsen-den Spannungen zwischen Russland und der Ukraine und trat im Januar 2022 erstmalig in Erscheinung. Seit Beginn des Krieges in der Ukraine fällt sie regelmäßig durch pro-russisch motivierte Cyberangriffe auf. Dabei handelte es sich um DDoS-Angriffe, die darauf ausgelegt sind, die Verfügbarkeit von Webseiten ausgewählter Angriffsziele zeitweise zu stören.

Anfang Mai wurden unter anderem Webseiten in Italien und Deutschland angegriffen, darunter Webseiten des italienischen Verteidigungsministeriums und des italienischen Senats sowie Webseiten des deutschen Verteidigungsministeriums, des Bundestags

und des BKA. Bereits im April waren Angriffe in Rumänien und weiteren NATO-Mitgliedsstaaten erfolgt. /DWE22w01/

Am 17.05.2022 kündigte Killnet DDoS-Attacken auf E-Mail-Provider aus mehreren europäischen Ländern an, darunter Deutschland, Estland, Lettland, USA, Rumänien, Italien und Polen. Das BSI bestätigte drei Tage später, dass es zu einer teilweisen Nichtverfügbarkeit der aufgezählten E-Mail-Provider gekommen sei. In Deutschland war hierbei der E-Mail-Provider Postero betroffen. /BSI22r17/

Beispielsweise erfolgten Angriffe auf Ziele in Litauen und Norwegen. In Norwegen wurden Ende Juni Behörden-Webseiten und Webseiten aus der Privatwirtschaft über Stunden attackiert und teilweise lahmgelegt. Wenige Tage zuvor waren bereits 130 Webseiten von Behörden und Privatwirtschaft in Litauen lahmgelegt worden. /SPI22w02/

Killnet verbindet seine Angriffe typischerweise mit prorussischen politischen Botschaften, so ergeht häufig die Forderung, die Unterstützung für die Ukraine einzustellen oder die Umsetzung der Sanktionen gegen Russland einzustellen. Auch sind häufig Drohungen enthalten, so beispielsweise gegen den norwegischen NATO-Generalsekretär Stoltenberg bei den Angriffen auf norwegische Ziele. /SPI22w02/

Kerntechnischer Bezug

Ein direkter kerntechnischer Bezug ist derzeit nicht festzustellen.

B.14.4 Cyberangriff auf Rosneft

Übersicht

Am 11.03.2022 wurde festgestellt, dass es zu einem Cyberangriff auf die deutsche Niederlassung des russischen Ölproduzenten Rosneft gekommen ist. Rosneft ist Russlands größter Ölproduzent und in den vergangenen Jahren für ein Viertel aller Rohölimporte nach Deutschland zuständig und damit ein Unternehmen der kritischen Infrastruktur. Aufgrund des Angriffs wurden vorsorglich alle IT-Systeme heruntergefahren und der E-Mail-Verkehr unterbrochen, der operative Betrieb wurde laut Rosneft Deutschland nicht beeinträchtigt. /HEI22w09/, /SEC22w05/, /HAN22w01/

Beschreibung

Die Rosneft Deutschland GmbH wurde im März 2022 Opfer eines Cyberangriffs, zu dem sich das Hackerkollektiv Anonymus bekannt hat. Nach Angaben von Anonymus konnte sich über zwei Wochen hinweg kontinuierlich und ohne Pause in den Systemen der Rosneft Deutschland GmbH bewegt und Daten kopiert werden. Nachdem der Angriff erkannt wurde, wurden aus Sicherheitsgründen alle IT-Systeme heruntergefahren und der E-Mail-Verkehr unterbrochen. Durch den Angriff wurden verschiedene Prozesse gestört, u. a. die Möglichkeit, Verträge abzuschließen. Trotzdem die IT-Systeme erheblich betroffen waren, wurde das operative Geschäft und der Betrieb von Pipelines und Raffinerien durch den Angriff laut Rosneft Deutschland nicht eingeschränkt; auch hatte der Angriff keine Auswirkungen auf die Versorgungslage. Um die Ursachen des Angriffs zu klären, wurde ein externer IT-Dienstleister hinzugezogen. /HEI22w09/, /SEC22w05/, /HAN22w01/, /SPI22w01/

Bei dem Angriff wurden insgesamt ca. 20 Terabyte an Daten gestohlen, u. a. Festplattenimages von Mitarbeiterrechnern und eines Mailservers, Backups der Laptops von Führungskräften des Unternehmens, Archiv-Dateien, Software-Pakete, Anleitungen und Lizenz-Schlüssel für Software. Außerdem wurden Inhalte Dutzender Geräte gelöscht. Laut Anonymus war man ca. 2 Wochen lang unbemerkt im System der Rosneft Deutschland GmbH und hatte Zugriff auf diverse Dateien in Backup-Ordnern, weiteren Ordnern mit Dokumenten sowie iPhones und iPads der Mitarbeiter. Anonymus hatte nach eigenen Angaben zu keinem Zeitpunkt Zugriff auf kritische Systemteile oder Steuerungsanlagen, wobei daran laut Anonymus auch kein Interesse bestand. Laut Anonymus wurde bewusst keine kritische Infrastruktur gefährdet und es wurden keine Steuerungssysteme in Mitleidenschaft gezogen. Eine Veröffentlichung der gestohlenen Daten ist laut Anonymus nicht geplant. /HEI22w09/, /SEC22w05/, /SEC22w06/, /SPI22w01/

Laut Anonymus gelang der Zugriff auf die Systeme der Rosneft Deutschland GmbH über die Steuerung und Verwaltung von Druckern, indem Service Accounts von Druckern im Active Directory kompromittiert wurden. Bei dem Angriff konnte weit in interne Systeme vorgedrungen werden und es ist laut Anonymus gelungen, Administratorrechte zu erlangen. Das Kopieren der Daten erfolgte dann über eine einfache FTP-Verbindung. Das Löschen der Inhalte Dutzender Geräte erfolgte dank eines erratenen Security Pins („1234“). /HAN22w01/, /SEC22w05/, /SPI22w01/

Anonymus ist ein Hackerkollektiv, welches vermutlich nicht besonders straff organisiert ist. Es gibt keinen eng umrissenen Mitgliederkreis, jeder kann sich zum Aktivisten erklären. Nach dem Angriff Russlands auf die Ukraine im Februar 2022 hat Anonymus der russischen Regierung offiziell den Cyberkrieg erklärt. Laut Anonymus wurden bereits diverse Cyberangriffe auf russische Einrichtungen durchgeführt, Opfer waren u. a. der Kreml, das Verteidigungsministerium, das Unterhaus der Duma, diverse russische Webseiten, russische Banken und russische TV-Sender. Auch Rosneft wurde bereits früher von Anonymus angegriffen, Ende Februar 2022 wurde beispielsweise die Webseite von Rosneft International durch einen DDos-Angriff blockiert. /SEC22w05/, /SEC22w06/, /SEC22w07/, /HAN22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.5 Industroyer-2 – Cyberangriff auf die ukrainische Energieversorgung

Übersicht

Am 12.04.2022 informierten das CERT-UA und die IT-Sicherheitsfirma ESET über einen Cyberangriff auf das ukrainische Stromnetz vom 08.04.2022, bei dem die Schadsoftware Industroyer2 eingesetzt wurde. Der Angriff wurde rechtzeitig entdeckt und Schäden konnten verhindert werden.

Beschreibung

Am 24.02.2022 begann die Invasion der Ukraine durch Russland. Parallel zu den physischen Kampfhandlungen werden auch Cyberangriffe gegen die Ukraine durchgeführt. Am 08.04.2022 sollte durch den Einsatz der Schadsoftware Industroyer2 ein Blackout im ukrainischen Stromnetz hervorgerufen werden. Der Angriff wurde nach ukrainischen Informationen rechtzeitig erkannt und Schäden konnten verhindert werden. Die Schadsoftwarekomponente Industroyer2 basiert auf der Schadsoftware Industroyer/Crashoverride, die 2016 bei einem Cyberangriff gegen das ukrainische Stromnetz eingesetzt wurde, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert.

Während Industroyer die Industrieprotokolle IEC-101, IEC-104, IEC-61850 und OPC DA verwendete, nutzt Industroyer2 ausschließlich das Protokoll IEC-104, um mit industriellen Steuerungssystemen (Industrial Control System, ICS) zu kommunizieren. Dieses Protokoll wird allgemein für die Überwachung und Steuerung von Energienetzen verwendet. Jedes System, in dem das Protokoll IEC-104 zum Einsatz kommt, ist prinzipiell durch die in der Schadsoftware Industroyer2 beinhalteten Methoden und Werkzeuge angreifbar. /BSI22i03/, /BSI22i04/, /ESE22w01/, /HIT22i01/, /MAN22w02/

Eigentliches Ziel des Angriffs war die Sabotage der industriellen Steuerungssysteme in den Hochspannungsumspannwerken, um einen Blackout hervorzurufen. Etwa zwei Millionen Menschen wären in der Ukraine von dem Blackout betroffen gewesen. Der Cyberangriff wird der APT-Gruppierung Sandworm zugeschrieben, welche dem russischen Nachrichtendienst GRU zugeordnet wird. Die Angreifer besitzen weitreichende Kenntnisse bezüglich des Protokolls IEC-104 und des kompromittierten Netzwerks einschließlich IP-Adressen und der Konfiguration des ICS-Netzwerks. Dass Industroyer2 hart codiert ist spricht dafür, dass die Schadsoftware für den Einsatz in verschiedenen Umgebungen speziell angepasst und jeweils neu kompiliert werden muss. Auf der anderen Seite erschwert dies die Detektion der Schadsoftware, da die Hashes für die Schad-software als Indicator of Compromise (IoC) angriffsspezifisch sind. Darüber hinaus verwendet Industroyer2 nur eine geringe Anzahl von Methoden, um die Detektion der Schadsoftware zu erschweren. Dies lässt vermuten, dass die IT-Angreifer über die Sicherheitsmaßnahmen im kompromittierten Netzwerk Bescheid wussten. /BBC22w01/, /BSI22i03/, /ESE22w01/, /HIT22i01/, /MAN22w02/, /NOZ22w01/, /WAT22w01/

Im Zuge des Angriffs wurden zusätzlich Wiper für Windows-, Linux- und Solaris-Betriebssysteme eingesetzt, um Daten zu löschen. Eines der Angriffswerkzeuge, CaddyWiper, löscht Benutzerdaten und Partitionsinformationen von Laufwerken auf Windows- Systemen, indem es diese mit Nullen überschreibt. Auf diese Weise sind die Systeme nicht wiederherstellbar. Die anderen eingesetzten Wiper Orcshred, Soloshred und Awfulshred sollen Schäden an Linux- und Solaris-Servern verursachen. /ESE22w01/, /WAT22w01/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.6 Khouzestan Steel Co. – Cyberangriff auf iranisches Stahlwerk

Übersicht

Die Hackergruppierung Predatory Sparrow gab am 27.06.2022 bekannt, einen Cyberangriff auf die drei größten Stahlwerke des Iran durchgeführt zu haben. Hierzu veröffentlichten sie auch ein Video einer Überwachungskamera aus dem iranischen Stahlwerk Khouzestan Steel Company. Darauf ist zu sehen, wie die Komponenten einer Produktionslinie zunächst noch wie vorgesehen funktionieren, dann Fehlfunktionen auftreten und schließlich ein massives Feuer ausbricht.

Beschreibung

Im Iran ist es parallel zu den wachsenden Spannungen in der Region in den letzten Monaten immer wieder zu Cyberangriffen gekommen. Für einige davon hat die Hackergruppierung Predatory Sparrow (Gonjeshke Darande) die Verantwortung übernommen. Hierzu zählen Angriffe auf die iranische Eisenbahn, den iranischen Rundfunk, zahlreiche Überwachungskameras und iranische Tankstellen /BBC22w01/. Während zwei der am 27.06.2022 angegriffenen Stahlwerke zwar einen Cyberangriff einräumten, aber keine An-gaben zu physischen Schäden machten, gab Khouzestan Steel Co. an, aufgrund technischer Probleme wegen eines Cyberangriffs die Produktion bis auf weiteres einzustellen.

Iran ist einer der Hauptproduzenten für Stahl weltweit und führend im Mittleren Osten. Die drei angegriffenen Firmen haben zusammen das Monopol auf Stahlproduktion im Iran. In dem von Predatory Sparrow veröffentlichten Video ist zunächst der normale Ablauf der Produktion zu sehen. Zudem ist sichtbar, wie das Personal nach und nach das Umfeld der Maschinen verlässt. Anschließend kommt es zu Störungen des Produktionsablaufes bis hin zu einem Feuer. Das Video endet mit Beginn der Löscharbeiten. In den Tagen nach der Veröffentlichung dieses Videos sind weitere Videos aus der Anlage auf-getaucht, die dieselbe Szene aus teils anderen Blickwinkeln zeigen. Darin sind Rufe der Arbeiter nach der Feuerwehr sowie Ausrufe zu Schäden an Komponenten zu hören.

Davon ausgehend, dass es sich bei dem veröffentlichten Bildmaterial um authentisches Bildmaterial handelt, stellt sich der Angriff wie folgt dar: Zum einen müssen die Angreifer Zugriff auf die Überwachungskameras gehabt haben. Zum anderen müssen sie es geschafft haben, sich von außen in die industriellen Steuerungssysteme der betroffenen

Produktionslinie einzuhacken. Predatory Sparrow gibt an, mit dem Beginn des Angriffs auf einen Moment gewartet zu haben, zu dem sich keine Arbeiter in der Nähe befunden haben. Dies ist nur mit direktem, unverzögertem Zugriff auf die betroffenen Systeme möglich.

Über den tatsächlichen Angriffsvektor ist derzeit nichts bekannt.

Aufgrund ihrer Vorgehensweise sowie der Komplexität und Auswirkung ihrer Angriffe wird vermutet, dass es sich bei Predatory Sparrow entgegen deren eigenen Angaben nicht um eine Hackergruppierung, sondern vielmehr um eine hochentwickeltem staatlich geförderte Angreifergruppierung handelt.

Kerntechnischer Bezug

Zunächst hat dieser IT-Sicherheitsvorfall keinen kerntechnischen Bezug. Da bislang aber keine Informationen über den Angriffsvektor oder über die angegriffenen industriellen Steuerungssysteme vorliegen, kann eine Übertragbarkeit derzeit nicht eingeschätzt werden.

B.14.7 LockBit – Cyberangriff auf Top Aces

Übersicht

Laut /FBI22r01/, /KAS22w02/ ist LockBit eine Ransomware-Gruppierung, deren erste Angriffe im September 2019 bekannt geworden sind. Zu diesem Zeitpunkt wurde die Gruppierung noch ABCD genannt, da diese Dateierweiterung bei verschlüsselten Daten verwendet wurde. Bei LockBit handelt es sich um eine Ransomware-as-a-Service-Gruppierung, die laut /REC22w01/ eine der produktivsten aktiven Gruppierungen ist und im Jahr 2022 bereits mindestens 650 Organisationen angegriffen hat (Stand: Ende Juni 2022). Die Gruppierung führt zielgerichtete Angriffe auf Unternehmen und Regierungsorganisationen aus, Privatpersonen sind eher keine Angriffsziele. Es werden Unternehmen weltweit angegriffen, wobei bewusst Unternehmen mit Standort in Russland gemieden werden. Die Schadsoftware von LockBit ist dabei darauf ausgelegt, den Zugriff zum angegriffenen System zu sperren, Daten zu verschlüsseln und damit eine Lösegeldzahlung zu erzwingen.

Beschreibung

Laut /BSI22r11/, /REC22w01/ kam es im Mai 2022 zu einem Cyberangriff von LockBit auf Top Aces, einem kanadischen Verteidigungsunternehmen und damit einem Unternehmen einer kritischen Infrastruktur. Top Aces bietet luftgestütztes Training für Luftwaffen-verbände weltweit an und ist exklusiver Anbieter gegnerischer Flugziele bei Übungen der kanadischen und deutschen Streitkräfte. Neben diversen Ländern weltweit hat Top Aces auch einen Vertrag mit den USA, in dem ausdrücklich die Bereitstellung von Werkzeugen zur Verteidigung gegen russische Waffen erwähnt wird. Bei dem Ransomware-Angriff von LockBit auf Top Aces wurden 44 GB an Daten gestohlen, die am 16.05.2022 bei Nichtzahlung eines Lösegeldes unbekannter Höhe veröffentlicht werden sollten. Da das Lösegeld nicht gezahlt wurde, erfolgte eine Veröffentlichung der Daten, wobei am 18.05.2022 nur Fragmente der Daten öffentlich zu finden waren. Ob der komplette gestohlene Datensatz veröffentlich wurde, ist nicht bekannt.

Die Ransomware-Angriffe von LockBit laufen laut /KAS22w02/ folgendermaßen ab: In der ersten Angriffsphase wird versucht, Schwachstellen in Unternehmensnetzwerken auszunutzen. Dabei wird gezielt nach attraktiven Zielen gesucht, es werden also keine breit gestreuten Angriffe ausgeführt. Um Zugang zu einem Unternehmensnetzwerk zu erhalten, werden dann Social-Engineering-Techniken angewendet oder es wird versucht, gewaltsam in das Netzwerk einzudringen. In der darauffolgenden Angriffsphase wird die Angriffsstruktur vervollständigt. Ab diesem Zeitpunkt sind keine manuellen Aktionen mehr notwendig, die Ransomware führt alle Aktionen automatisiert aus. Die Lock-Bit-Ransomware ist dabei so programmiert, dass sie von speziell entwickelten automatisierten Prozessen gelenkt wird und hebt sich damit von anderen Ransomware-Versionen ab, bei denen die Ransomware-Gruppierungen mitunter wochen- oder monatelang in Netzwerken verharren, um Aufklärungs- und Überwachungsarbeit durchzuführen. Nach der manuellen Erstinfektion wird automatisch nach anderen zugänglichen Systemen gesucht. Zur Verbreitung der Ransomware werden dann Tools wie Windows PowerShell oder Server Message Block (SMB) genutzt. Des Weiteren werden Tools genutzt, um sich Berechtigungen zu verschaffen und diese weiter zu eskalieren. Die verwendeten Tools werden dabei in Mustern genutzt, die in nahezu allen Windows-Systemen nativ vorzufinden und damit schwer aufzudecken sind. In dieser Phase werden auch Sicherheitsprogramme ausgeschaltet, über die das System wiederhergestellt werden könnte. In der letzten Angriffsphase beginnt die Ransomware, sich über das infiltrierte Netzwerk auszubreiten.

Dazu genügt ein einziges System mit hoher Zugangsberechtigung, um andere Systeme im Netzwerk ebenfalls zu infizieren. Alle Daten werden verschlüsselt, was nur durch einen speziellen Schlüssel rückgängig gemacht werden kann.

Zu Beginn des Auftretens von LockBit erfolgten ausschließlich Verschlüsselungen von Windows-Systemen, wobei die automatische Verschlüsselung über Active-Directory-Gruppenrichtlinien erfolgte. Im Januar 2022 wurde bekannt, dass LockBit auch eine Verschlüsselungssoftware für VMWare ESXi-Linux-Server in sein Toolkit aufgenommen hat. Außerdem versucht LockBit aktiv Innentäter zu rekrutieren, indem Gewinnbeteiligungen an möglichen erpressten Lösegeldern versprochen werden. Die Innentäter sollen über Virtual Private Network (VPN) oder Remote Desktop Protocol (RDP) Zugang zu Unternehmensnetzwerken gewähren. /BLE22w05/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.8 Conti – Cyberangriff auf Regierungsstellen Costa Ricas

Übersicht

Im April 2022 wurden mehrere Regierungsstellen Costa Ricas laut /BSI22r04/ Opfer der Ransomware-Gruppierung Conti. Von den Angriffen waren Finanz-, Zoll- und Steuerbehörden, das Ministerium für Arbeit und Soziales sowie eine Universität betroffen. Durch die Angriffe wurden bedeutende Teile von Behörden und Regierungsstellen lahmgelegt, aufgrund dessen wurde in Costa Rica der nationale Cyber-Notstand ausgerufen. /BSI22r04/, /HEI22w05/ Bisher wurden laut /BSI22r04/ keine derart umfangreichen Cyberangriffe auf staatliche Einrichtungen mit Ransomware beobachtet, laut /WIR22w01/ war es sogar das erste Mal, dass eine Ransomware-Gruppierung explizit die Regierung eines Landes angegriffen hat. Die Angriffe erfolgten durch Conti, eine pro-russische Ransomware-as-a-Service-Gruppierung, die Verbindungen zur russischsprachigen Gruppierung Wizard Spider hat und unter anderem für Angriffe auf HSE in Irland (siehe Abschnitt B.13.11) und Angriffe auf US-amerikanische Unternehmen des Gesundheitswesens und der Rettungsdienste verantwortlich ist. /BLE22w01/

Beschreibung

Laut /WIR22w01/ erfolgten die ersten Angriffe von Mitte April bis Anfang Mai 2022, wo-bei insgesamt 27 Regierungsstellen betroffen waren. Am 18. April 2022 wurden als erstes Dateien des Finanzministeriums verschlüsselt, in den darauffolgenden Tagen bis zum 02. Mai 2022 wurde nahezu täglich versucht, in verschiedene weitere lokale Behörden sowie zentrale Regierungsorganisationen einzudringen. Digitale Dienste des Finanzministeriums waren daraufhin seit dem 18.04.2022 nicht mehr verfügbar, wodurch der gesamte „produktive“ Sektor des Landes beeinflusst wurde, da staatliche Verfahren zur Vergabe von Unterschriften, Stempeln, etc. nicht mehr ausgeführt werden konnten. /BLE22w01/ Ein zweiter Angriff Ende Mai 2022, der von der Gruppierung HIVE, welche Verbindungen zu Conti haben soll, ausgeführt, betraf Systeme des Sozialversicherungsfonds Costa Ricas, durch den auch die Gesundheitsversorgung organisiert wird, womit also auch das Gesundheitssystem Costa Ricas getroffen wurde. /WIR22w01/

Durch diese beiden Cyberangriffe wurden laut /WIR22w01/ viele wichtige Dienste von Costa Rica lahmgelegt, wodurch der internationale Handel Costa Ricas zum Erliegen kam. Die Ein- und Ausfuhren des Landes mussten ausgesetzt werden, was große Auswirkungen auf den Handel hatte. /WIR22w01/ Insgesamt wurden mehr als 30.000 Arzttermine verschoben und es kam zum Ausfall von Millionenbeträgen.

Laut /BSI22r04/, /HEI22w05/, /BLE22w01/ wurden bei dem Cyberangriff Daten gestohlen und verschlüsselt. Zur Freigabe der Daten wurde ein Lösegeld in Höhe von 10 Millionen US-Dollar gefordert, welches aber nicht gezahlt wurde. Daraufhin wurden 97 % der gestohlenen 672 GB an Daten auf der Webseite von Conti veröffentlicht. Die Drohungen gegen Costa Rica wurden von Seiten Contis verschärft und die Summe des verlangten Lösegeldes wurde auf 20 Millionen US-Dollar erhöht. /WIR22w01/, /HEI22w06/

Die genaue Motivation hinter dem Angriff ist unklar. Es könnte sich laut /BSI22r04/ um einen Testlauf gehandelt haben, der gegen Costa Rica gerichtet war, um ein Exempel zu statuieren. Aber auch ein zufälliger Angriff auf eine Einrichtung und eine von dort er-folgte Kompromittierung weiterer Einrichtungen aufgrund von bei dem Erstangriff aufgedeckten Möglichkeiten ist denkbar. Laut /WIR22w01/ führte Conti zur gleichen Zeit, zu der die Angriffe auf Costa Rica ausgeführt wurden, auch Angriffe auf das Finanzministerium und den Geheimdienst Perus durch, wobei über Schäden oder Auswirkungen dieser Cyberangriffe nichts bekannt geworden ist.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.9 Cyberangriff auf israelische Regierungswebseiten

Übersicht

Laut /HEI22w08/, /IND22w02/, /REG22w02/ kam es am 14.03.2022 zu einem Cyberangriff auf den nationalen israelischen Kommunikationsdienstleister Cellcom. Bei dem Angriff handelte es sich um einen DDoS-Angriff (Distributed-Denial-of-Service-Angriff), infolgedessen diverse Internetseiten der israelischen Regierung nicht mehr zu erreichen waren.

Beschreibung

Der nationale israelische Kommunikationsdienstleister Cellcom wurde Opfer eines DDoS-Angriffs, der zu einer Unterbrechung der Dienste auf verschiedenen Regierungswebseiten führte. Betroffen waren dabei alle Seiten unter der Domain „gov.il“, wobei ins-besondere Webseiten des Gesundheits-, Innen-, Justiz- und Sozialministeriums betroffen waren. /REG22w02/, /HEI22w08/, /MAL22w02/

Für den Angriff auf die israelischen Regierungswebseiten ist laut /REG22w02/ ein nationalstaatlicher Akteur oder eine große Organisation verantwortlich, wobei nicht geklärt ist, welche Gruppierung den Angriff begangen hat. Laut /MAL22w02/ ist möglicherweise eine iranische Gruppierung für den Angriff verantwortlich.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.10 Cyberangriffe mit Bumblebee

Übersicht

Seit März 2022 wird vermehrt ein neuer Schadsoftwareloader mit dem Namen Bumblebee durch Sicherheitsforscher beobachtet.

Schadsoftwareloader dienen als erste Stufe von Schadsoftwareangriffen, sie öffnen für die Angreifer einen Zugang zum betroffenen IT-System, stellen die Verbindung mit den Befehlsstrukturen (Command & Control Server) her, führen das Nachladen von weiterer Schadsoftware aus und können zur Verbreitung innerhalb des angegriffenen Netzwerkes beitragen. Bumblebee hat nach bisherigen Angaben von Sicherheitsforschern eine Reihe früherer genutzter Schadsoftwareloader verdrängt und wird insbesondere von verschiedenen Ransomware-Gruppierungen als erste Stufe eines Cyberangriffes eingesetzt. /BLC22r01/, /MED22r01/

Beschreibung

Moderne Schadsoftwares sind zumeist modular aufgebaut, wobei bestimmte Aufgaben von verschiedenen Schadsoftwares übernommen werden. So übernimmt ein Modul die Ausbreitung innerhalb eines Netzwerkes, ein anderes Modul die Ausspähung von wichtigen Daten auf betroffenen Systemen, ein weiteres Modul führt die Verschlüsselung aus und schließlich übernehmen Loader die Aufgabe der erstmaligen Infektion. Die Ansprüche an Schadsoftwareloader sind mit steigenden Sicherungsmaßnahmen stetig gewachsen. Ein und derselbe Schadsoftwareloader wird zum Teil zur Verbreitung von völlig unterschiedlichen Schadsoftwares, z. B. Ransomware oder Bankingtrojaner eingesetzt, die Loader werden von den Entwicklern verkauft, vermietet oder zur freien Benutzung bereitgestellt. Seit März 2022 ist mit dem Bumblebee-Loader ein neuartiger hochmoderner Schadsoftwareloader entdeckt worden. Ransomwaregruppierungen wie Conti, Quantum und Mountlocker haben in den Monaten April bis Juni 2022 ihre bisherigen Loader wie BazarLoader oder Trickbot durch Bumblebee ersetzt. Hierdurch erhoffen sich diese Gruppierungen vermutlich eine höhere Erfolgsquote in der Verbreitung ihrer Schadsoftware. /BLC22r01/, /MED22r01/

Der Bumblebee-Loader wird in den meisten Fällen per E-Mail verteilt u. a. über Archive, dem CD-Abbildformat ISO und manipulierte HTML-Dateien. Diese Dateien sind entweder direkt an die Emails angehangen oder aber als Link z. B. zu Cloud Speichermedien in Emails verknüpft. Werden die entsprechend verteilten Dateien ausgeführt, wird die Bumblebee-DLL ausgeführt und die Infektion des ausführenden IT-Systems startet. Bumblebee verbindet sich mit einer Command & Control Infrastruktur und führt anschließend alle 15 Minuten ein VBS Script aus.

Mit zeitlichem Abstand wird die zweite Stufe des Cyberangriffs, eine von Bumblebee unabhängige Schadsoftware wie die Ransomware Software Quantum heruntergeladen, mit welcher die Dateien des betroffenen IT-Systems verschlüsselt werden und die weitere Ausbreitung der Infektion durchgeführt werden kann. /MED22r01/

Die Besonderheiten des Bumblebee-Loaders sind seine komplexen Fähigkeiten zur Verschleierung der eigenen Entdeckung, der Entdeckung möglicher Virtualisierungsbemühungen von Schutzprogrammen und die Eskalation der Rechte des Loaders zur Ausführung beliebigen Codes. Bumblebee nutzt eine bisher nicht bekannte Routine, um seinen Code erstmalig auszuführen, wozu Bumblebee den Zugriff auf den Speicher des Systems nutzt, eine fiktive DLL Datei lädt und den Ladevorgang dieser DLL Datei zum Ausführen seines Codes nutzt. Bumblebee sucht bei jeder Ausführung nach bestimmten Prozessen, die auf Virenscanner, andere Schutzfunktionen oder Virtualisierungssoftware hinweisen. Die Anzahl der gesuchten Prozesse hat in den Monaten seit Erscheinen im März 2022 stetig zugenommen, was auf eine konsequente Weiterentwicklung des Bumblebee-Loaders hindeutet. Der Bumblebee-Loader zeigt damit die konsequente innovative Weiterentwicklung von Schadsoftware auf und ist daher von Sicherheitsforschern intensiv analysiert worden. /BLC22r01/, /MED22r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

B.14.11 Cyberangriff auf Dienstleister von Okta

Übersicht

Im März 2022 veröffentlichte die Angreifergruppierung „Lapsus$“ Informationen zu Kundenaccounts des amerikanischen Unternehmens „Okta“, welches Cloud-Produkte für Identitäts- und Zugriffsmanagement anbietet. Okta bestätigte am 22. März, dass das Unternehmen Hinweisen auf einen Cyberangriff in der Zeit vom 16. bis zum 21. Januar 2022 über einen Dienstleister nachgeht. Die Angreifer erlangten ihren Zugriff mutmaßlich über den Laptop eines Unterauftragnehmers. /CNN22w01/

Beschreibung

Durch eine forensische Untersuchung eines im Januar 2022 registrierten IT-Sicherheitsvorfalls erkannte das Unternehmen Okta, dass sich die Angreifergruppierung „Lapsus$“ für einen Zeitraum von fünf Tagen Zugang zu einem Laptop eines Support-Ingenieurs der Firma Sitel verschafft hat. Das Unternehmen bietet für seine Kunden unter anderem technischen Support als Dienstleistung an. Okta grenzte den potenziellen Zugriff der Angreifer zunächst auf 2,5 % des Kundenstamms ein, was auf Grundlage der veröffentlichten Quartalszahlen etwa 366 Kunden betreffen würde. Im April 2022 veröffentlichte Okta die finale forensische Analyse des IT-Sicherheitsvorfalls. Demnach wurde festgestellt, dass sich die Angreifer für eine Zeitspanne von 25 Minuten Zugang zum Laptop des Support-Ingenieurs verschafft haben und nur zwei Kunden betroffen waren. Die Angreifer hatten Zugriff auf die Software SuperUser, die für grundsätzliche Managementfunktionen genutzt wird. Außerdem hatten die Angreifer limitierten Zugriff auf Informationen in anderen Programmen wie „Slack“ oder „Jira“, die nicht für Aktionen im Rahmen Oktas Software verwendet werden können. Nach Angaben von Okta konnten die Angreifer weder Änderungen an Konfigurationen durchführen noch eine Multi-Faktor-Authentifizierung bzw. Passwörter zurücksetzen oder sich in irgendeiner Form direkt gegenüber Okta-Accounts authentifizieren.

Der Grad der Kompromittierung ist gemäß Okta signifikant kleiner als ursprünglich befürchtet, wobei dennoch auf die Kritikalität eines solchen Vorfalls hingewiesen wurde. Okta beschreibt in diesem Zusammenhang mehrere Bereiche, in denen das Unternehmen angesichts des IT-Sicherheitsvorfalls Verbesserungspotenzial sieht. Dabei geht es unter anderem um das Thema Third-Party-Riskmanagement, welches angesichts vermehrter IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette von IT-Systemen von großer Bedeutung ist. /BSI22r16/, /OKT22w01/, /OKT22w02/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.14.12 Cyberangriffe im Jahr 2021 und 2022 auf den VPN Client Pulse Connect Secure

Übersicht

Bei Pulse Connect Secure handelt es sich um eine als besonders sicher beworbene VPN-Softwarelösung, welche an Geschäftskunden vertrieben wird und von Pulse Secure, einem Tochterunternehmen von Ivanti betrieben wird. Vormals als Juniper SSL VPN bekannt, wird Pulse Connect Secure insbesondere mit seinen Sicherheitsfeatures beworben, wozu unter anderem die Nutzung von Secure Sockets Layer (SSL) gehört, welches ein Netzwerkprotokoll für die sichere Übertragung von Daten ist. Weiterhin verfügt der Pulse Connect Secure VPN gemäß Anbieter über verschiedene Verifizierungsmaßnahmen für den sicheren Zugriff und eine Ende-zu-Ende-Sicherheitsfunktion, welche die Nutzung von Sicherungsmaßnahmen auf den Endgeräten prüft. Am 23.04.2021 wurde die kritische Schwachstelle CVE-2021-22893 der Pulse Connect Secure Software bekannt. /PUL22w01/, /FOR20w02/

Beschreibung

Pulse Connect Secure gilt als sichere VPN-Anwendung zur Anbindung von Fernzugriffen, Unternehmensnetzwerken und ähnlichen über räumliche Distanzen und ist in Unternehmen und Behörden im westlichen Raum weit verbreitet. Insbesondere durch die Pandemie 2020/2021 kam es zu einer weiten Verbreitung von Anwendungen für Fernzugriffe in Unternehmen und Behörden, um das isolierte mobile Arbeiten zu ermöglichen. So stieg Pulse Connects Umsatz im ersten Quartal 2020 um 300 %, insbesondere auch weil Pulse Connect durch den Einsatz von Verschlüsselungstechnologien und Authentifizierungstechnologien als sicher beworben wird. /PUL22w01/, /FOR20w02/

Am 23.04.2021 wurde die Schwachstelle CVE-2021-22893 für Pulse Connect Secure bekannt, wobei erstmalig am 20.04.2021 vom IT-Sicherheitsdienstleister Mandiant bezüglich laufender Cyberangriffe berichtet wurde. Für die sogenannte Zero-Day Schwachstelle stand zu diesem Zeitpunkt kein Sicherheitsupdate zur Verfügung, während IT-Angreifer die Schwachstelle bereits vor der Bekanntwerdung ausnutzten. Zu den Opfern zählen gemäß AP der Telekommunikationskonzern Verizon, die kalifornische Wasserbehörde, die New Yorker U-Bahn sowie nicht spezifizierte dutzende weiterer hochwertiger Ziele der USA. Die Schwachstelle erhielt einen CVSS Base Score von 10 von 10 Punkten und gilt damit als überaus kritisch.

Mittels der Schwachstelle können Angreifer über die Webschnittstelle der Pulse Connect Secure Software beliebigen Code ohne Authentifizierung ausführen und somit die betroffenen IT-Systeme vollständig kontrollieren. Es gibt eindeutige Hinweise, dass die Schwachstelle durch APT-Gruppierungen vor Alarmierung der Öffentlichkeit in Europa und den USA ausgenutzt wurde. Betroffen sind kritische Infrastrukturen, Verteidigungsunternehmen, Regierungsbehörden und Telekommunikation. Für die Schwachstelle wurde am 03.05.2021 ein Sicherheitsupdate veröffentlicht, welches die Schwachstelle behob. /BSI21w08/, /MAN21r01/

Für weitere Schwachstellen wie CVE-2021-22908, die anschließend bekannt, und mit einem CVSS Base Score von bis zu 8,5 von 10 Punkten bewertet wurden, erfolgte die Veröffentlichung von Sicherheitsupdates durch den Hersteller erst mit Verzögerungen von einigen Wochen nach Bekanntwerden . Der Hersteller veröffentlichte darüber hinaus mögliche Mitigationsmaßnahmen, welche vom BSI auch weiterhin insbesondere für solche IT-Systeme empfohlen werden, die kein Update erhalten haben oder erhalten können. /BSI21w08/, /MAN21r01/

Die auf der Schwachstelle CVE-2021-22893 basierenden Cyberangriffe wurden den APT Gruppierungen UNC2630 und UNC2717 zugeordnet. Mit der Veröffentlichung der Schwachstellen von Pulse Connect Secure kam es zu weiteren Cyberangriffen unter Ausnutzung der Schwachstellen. Es besteht bisher keine vollständige Übersicht, welche Unternehmen sowie staatlichen Stellen und Bereiche der kritischen Infrastruktur tatsächlich vom Cyberangriff betroffen waren, insbesondere dutzende „Hochwert“ Ziele, die betroffen sein sollen, wurden nicht namentlich veröffentlicht. Mittels der Schwachstelle konnten betroffene IT-Systeme vollständig von den IT-Angreifern kontrolliert werden. Von hier aus konnte auf angeschlossene IT-Netzwerke je nach Umständen zugegriffen werden, wobei die Entwendung von Daten und Informationen Ziel der Angriffe gewesen sein soll. /MAN21r01/

Am 15. März 2022 wurde die Schwachstelle CVE-2022-0778 bekannt, welche die Software OpenSSL betrifft. OpenSSL wird von Pulse Connect Secure für die SSL Verschlüsselung angewendet und ist in die Software integriert. Die Schwachstelle mit einem CVSS Base Score von 7,5 von 10 ermöglicht Angreifern die Überführung betroffener IT-Systeme in einen Denial-of-Service Zustand. /PUL22w02/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.14.13 Cyberangriff auf T-Mobile US und folgende SIM-Swaps

Übersicht

T-Mobile US ist die amerikanische Tochtergesellschaft der deutschen Telekom und mit über 100 Millionen Kunden der größte Mobiltelekommunikationsanbieter der USA. T-Mobile US veröffentlichte seit 2018 insgesamt sieben verschiedene Datenabflüsse durch Cyberangriffe, wovon mehrere als schwerwiegend anzusehen sind. Im Rahmen der Datenabflüsse wurden Millionen Kundendaten verschiedener Kundenkategorien durch IT-Angreifer entwendet. Die so entwendeten Zugangsdaten der Mitarbeiteremailaccounts und die Cyberangriffe ermöglichten im Jahr 2021 auf zwei unterschiedliche Arten sogenannte SIM Swap Attacks. Bei diesen Angriffen erhalten die Angreifer eine funktionierende SIM-Karte, der die Telefonnummern und Telefonverträge der Opfer zugeordnet sind. Damit können Angreifer die Mobilkommunikation der Kunden vollständig übernehmen. /BLE21w03/

Beschreibung

Der bekannteste Cyberangriff auf T-Mobile US wurde im August 2021 bekannt. IT-Angreifer erlangten Zugriff auf das IT-Netzwerk des Telekommunikationskonzerns und erbeuteten laut T-Mobile US Datensätze zu 7,8 Millionen Vertragskunden, 40 Millionen früheren oder potenziellen Kunden und 850.000 Kunden mit Prepaid-Konten. Gemäß T-Mobile US wurden hierbei Namen, Sozialversicherungsnummern, Geburts- und Führerscheindaten entwendet, jedoch keine finanziellen Daten oder Passwörter. Die Angreifer selbst gaben an, dass Sie Daten von mehr als 100 Millionen Kunden erlangten und forderten für den Kauf eines Datensatzes mit Millionen Führerscheindaten und Sozialversicherungsnummern insgesamt 285.000 Dollar. Gemäß T-Mobile US erlangten die Angreifer Zugang zu einer Testumgebung und nutzten von hier aus Brute Force-Angriffe, um auf das IT-Netzwerk des Konzerns zuzugreifen. Der Angriff reiht sich in eine Reihe von Datendiebstählen bei T-Mobile US ein, im Jahr 2018, 2019 und 2020 kam es zu weiteren Datendiebstählen durch Cyberangriffe.

Dazu wurden die Zugangsdaten der Mitarbeiter durch einen Cyberangriff auf einen externen Dienstleister im Jahr 2020 entwendet. /BLE21w03/

Besondere Aufmerksamkeit erhielten insbesondere zwei Cyberangriffe, bei welchen sogenannte SIM-Swaps durch IT-Angreifer durchgeführt wurden. SIM-Karten dienen in Telefonen und anderen IT-Systemen als Identifikationsobjekte der Nutzer und werden zur Bereitstellung von mobilen Telekommunikations- und Datenanschlüssen von Telekommunikationsunternehmen genutzt. SIM-Karten werden durch PINs und PUKs vor unbefugten Zugriffen geschützt. Falls SIM-Karten verloren gehen, bieten Telekommunikationsdienstleister verschiedene Formen an, neue SIM-Karten zu beantragen, ebenso gibt es die Möglichkeit mehrere gleiche SIM-Karten für verschiedene Endgeräte zu erhalten. Im Rahmen der SIM-Swap Angriffe können die Verfahren zum Erlangen von Ersatz-SIM-Karten, welche entweder durch menschliche Bediener betrieben werden oder vollautomatisiert sind, beeinflusst werden, um die neuen SIM-Karten zu erhalten. Mit den SIM-Karten haben die IT-Angreifer Zugriff auf alle eingehenden SMS sowie Telefonanrufe der Opfer und können selbst SMS verschicken bzw. Telefonanrufe mittels der Telefonnummer der Opfer durchführen. Die Opfer erhalten bis auf den Ausfall der eigenen Telekommunikation zum Teil keinen Hinweis auf durchgeführte SIM-Swaps. /ZDN21w05/

Im Rahmen von Multi-Faktor-Authentifizierungen werden häufig SMS zur Zweifaktorprüfung von Anmeldungen auf IT-Systemen, Fernzugriffe und IT-Services wie Emailaccounts, Onlinebanking oder soziale Medien genutzt. Zusammen mit Passwörtern erhalten die IT-Angreifer mittels SIM-Swaps somit einen umfassenden Zugriff auf entsprechende Services und IT-Systeme der Opfer. Zumeist bieten IT-Services sogenannte Accountwiederherstellung an, falls Passwörter vergessen wurden. So kann auch ohne Kenntnis der Passwörter der Opfer mittels SIM-Swap ein Zugriff erreicht werden. Mit dem Zugriff auf zentrale Emailaccounts können zumeist weitere Accounts, die den Emailaccount zur Wiederherstellung nutzen, übernommen werden. /ZDN21w05/

Im Februar 2021 gab T-Mobile US bekannt, dass insgesamt 400 Kunden von einer Form von Informationsdiebstahl betroffen waren. Zu den Informationen gehörten PINs, Sicherheitsfragen und -antworten, Kundeninformationen und persönliche Informationen, wodurch es zu SIM-Swaps kam. Die Angreifer nutzten die von T-Mobile US angebotene Möglichkeit zur Beschaffung von Ersatz-SIM-Karten.

Im Dezember 2021 kam es zu einem weiteren Vorfall, bei welchem T-Mobile US bekannt gab, dass es nicht autorisierte Aktivitäten in den von den Kunden einsehbaren Nutzerinformationen gab. Mittels dieser Daten ist es zum SIM-Swap durch die IT-Angreifer gekommen. /BLE21w03/

Nach bisherigen Erkenntnissen wurden die SIM-Swaps nicht spezifisch durchgeführt, führten bei Betroffenen jedoch zum Teil zu erheblichen finanziellen Schäden. So wurde eine Klage eingereicht, weil ein Kunde von T-Mobile US insgesamt mehr als 8,7 Millionen Dollar in Form von Kryptowährungen verlor, nachdem durch einen SIM-Swap Zugriff auf Handelsplattformen von Kryptowährungen durch die Angreifer erlangt wurde. /BLE21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.14 Cyberangriffe mit DeadBolt

Übersicht

Im Januar 2022 kam es zu einem breiten Cyberangriff mittels Ransomware auf NAS-Systeme des Anbieters QNAP. Im Rahmen dieses Cyberangriffs wurden die betroffenen NAS-Systeme durch die Schadsoftware verschlüsselt, wodurch gespeicherte Daten nicht mehr abrufbar waren, und anschließend ein Lösegeld verlangt. /QNA22r01/

Beschreibung

QNAP ist ein taiwanesischer Anbieter für NAS-Systeme und vertreibt diese weltweit. Die NAS-Systeme des Herstellers bieten umfassende Funktionalitäten an, um einen Zugriff auf die NAS-Systeme aus dem Internet zu ermöglichen. Am 25. Januar 2022 kam es zu einer Angriffsserie auf NAS-Systeme von QNAP, bei welchen die Angreifer eine hohe Anzahl an NAS-Systemen, welche über das Internet ansteuerbar waren, mit Ransomware angriffen. Die Ransomware verschlüsselte sämtliche gespeicherte Dateien und fügte diesen anschließend die Endung „.Deadbolt“ an. Die Angreifer nutzten schließlich die HTML-basierten Zugriffsmöglichkeiten auf die NAS-Systeme um den Opfern eine Aufforderung zur Überweisung von 0,03 Bitcoin (zum damaligen Zeitpunkt ca. 1.100 US Dollar) anzuzeigen.

Nach eingegangener Überweisung wurde den Opfern ein Entschlüsselungscode zugeschickt. Insgesamt 5.000 von 130.000 Online identifizierbaren NAS-Systemen von QNAP wiesen Anzeichen auf eine Infektion mit Deadbolt auf. Es bestand für Betroffene kein direkter Kontakt zu den IT-Angreifern, die Übersendung der Entschlüsselungscodes erfolgte vollautomatisch mittels in Bitcoin-Transaktionen inkludierter Informationen. /QNA22r01, ENI22r01/

Bekanntheit erlangte der Cyberangriff insbesondere durch die Aussagen der Angreifer, dass diese eine bis dahin unerkannte Zero-Day-Schwachstelle ausnutzen würden und für 5 Bitcoin (zum damaligen Zeitpunkt ca. 117.000 US Dollar) die Informationen über diese Schwachstelle sowie für 50 Bitcoin (zum damaligen Zeitpunkt ca. 1,7 Millionen US Dollar) den Hauptschlüssel zur Entschlüsselung aller betroffenen IT-Systeme zum Kauf anboten. QNAP reagierte auf die Cyberangriffe durch Deadbolt am 02. Februar 2022 mit dem Hinweis, dass eine Schwachstelle ausgenutzt wurde, welche am 13. Januar 2022 durch QNAP in einem Security Advisory bekanntgemacht wurde und für welche ein Update für alle betroffenen QNAP Systeme seit dem 13. Januar 2022 bereitsteht. Weiterhin wies QNAP die Nutzer daraufhin besondere Sicherungsmaßnahmen für die eigenen NAS-Systeme zu treffen, z. B. die direkte Konnektivität zum Internet für die Systeme abzuschalten oder aber spezielle VPN-Verbindungen für Zugriffe zu etablieren. /ENI22r01/

Im Mai 2022 kam es zu einer weiteren Welle an Deadbolt Ransomware-Angriffen auf NAS-Systeme von QNAP. Gemäß eines Security Advisorys von QNAP vom 17. Juni 2022 waren ausschließlich nicht aktualisierte Versionen der NAS-Systeme betroffen. Weiterhin kam es zu Ransomware-Angriffen mit der Schadsoftware ECh0raix (auch SunCrypt genannt) sowie weiteren Ransomwares. NAS-Systeme wurden in den letzten Jahren zu einem typischen Ziel für IT-Angreifer, besonders für Ransomware-Angriffe. NAS-Systeme werden vielfach mit Anbindungen ans Internet genutzt, als Speichersysteme werden sie für eine hohe Onlinezeit selten aktualisiert und insbesondere im Fall von QNAP meiden Nutzer aktiv die Updates aufgrund von früheren und aktuellen Komptabilitätsproblemen und Systemfehlfunktionen nach Updates. /TRE22r01, QNA22r02/

Da NAS-Systeme neben Privatanwendern insbesondere von Unternehmen und Behörden angewendet werden, werden diese häufig insbesondere aufgrund ihrer konstanten Verfügbarkeit eingesetzt, sodass Updates verzögert oder überhaupt nicht aufgespielt werden.

NAS-Systeme werden zudem häufig „out of the box“ in Betrieb genommen ohne umfassende IT-Sicherungsmaßnahmen oder Konfigurationen, sodass diese, aber auch andere typische IoT-Systeme vermehrt von Angreifenden als Ziel genommen werden. Neben Ransomware-Angriffen sind so auch Angriffe zum Erlangen der gespeicherten Daten sowie zur Etablierung in Netzwerkstrukturen bekannt geworden. QNAP allein hat für die eigenen vom Januar 2022 bis zum Juni 2022 insgesamt 22 Security Advisories veröffentlicht oder aktualisiert.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.15 Cyberangriff über USB-Sticks

Übersicht

Seit August 2021 kam es in den USA laut /FBI22l01/, /HEI22w03/ zum Verschicken von USB-Sticks, welche Ransomware enthalten. Diese werden getarnt als Geschenkbox oder Covid-19-Leitlinien an diverse US-Firmen, insbesondere aus der Transport-, Versicherungs- und Rüstungsbranche (kritische Infrastrukturen) verschickt. Welche Auswirkungen diese Attacke bisher hatte, wurde von /FBI22l01/, /HEI22w03/ nicht genannt. Die Angriffe erfolgten durch eine bereits seit dem Jahr 2013 bekannte Gruppierung namens FIN7 (auch bekannt als Carbanak), welche bekannt ist für Phishing Attacken sowie Schadsoftware in Bankservern, Geldautomaten und Bezahlterminals mit dem Ziel, finanziellen Gewinn damit zu erzielen. Die Gruppierung FIN7 hat laut /HEI22w04/ bereits einen Schaden von mehr als einer Milliarde US-Dollar verursacht und mehrere hundert US-Unternehmen angegriffen.

Beschreibung

Die USB-Sticks wurden seit August 2021 verschickt, wobei die Lieferung über den US Postal Service oder UPS erfolgte. Die USB-Sticks wurden in zwei Varianten verschickt: Bei der ersten Variante ist der Absender das US Department of Health and Human Services (Gesundheitsministerium) und das Paket enthält den USB-Stick und Briefe, die sich auf Covid-19-Leitlinien beziehen. Bei der zweiten Variante enthält das Paket eine Geschenkbox von Amazon mit dem USB-Stick und einem gefälschten Dankesschreiben.

Durch die falsche Vorspiegelung, die USB-Sticks stammten von den genannten Institutionen, sollen die Empfänger in Sicherheit gewogen und dazu verleitet werden, diese tatsächlich zu nutzen. Es wird somit gezielt der Faktor Mensch ausgenutzt, um als Schwachstelle zu fungieren und Zugriff auf interne Netzwerke zu erhalten. /FBI22l01, HEI22w03, WIN22w01/

In beiden verschickten Varianten enthielten die Pakete USB-Sticks der Marke LilyGO, welche die Malware BadUSB oder Bad Beetle USB enthalten, die im Internet käuflich zu erwerben sind. Diese Malware ermöglicht die Ausführung von Programmen aus der Ferne oder das Einschleusen von Malware in den betroffenen PC. Nach dem Einstecken der USB-Sticks wird durch die enthaltene Malware BadUSB bzw. Bad Beetle USB eine inhärente Schwachstelle der USB-Firmware ausgenutzt, welche es ermöglicht, die USB-Sticks so zu programmieren, dass sie als menschliche Schnittstellengeräte fungieren. Dabei registriert sich der USB-Stick beim Einstecken als Tastatur, womit eine mögliche Einstellung, dass externe Speichermedien nicht automatisch ausgeführt werden, umgangen wird. Bei einem Einstecken des USB-Sticks in einen privaten oder dienstliches PC werden diese mit Malware infiziert, worauf weitere Erpressungen oder Cyberangriffe erfolgen können. /FBI22l01/, /HEI22w03/

Nach dem Einstecken der USB-Sticks werden Programmroutinen ausgeführt, die vorkonfigurierte, automatische Tastatureingaben ablaufen lassen, um einen PowerShell-Befehl namens KillACK auszuführen, welcher dem dauerhaften Zugriff auf das Zielsystem und dem Diebstahl von Informationen dienen soll. Außerdem wird Malware von einem von FIN7 kontrollieren Server heruntergeladen und ausgeführt. Daran anschließend wird seitens der Täter der Versuch unternommen, administrativen Zugang zu erhalten und anschließend durch Seitwärtsbewegungen im betroffenen Netzwerk auf andere lokale Systeme überzugreifen. Die verwendete Malware ist dabei z. B. Metasploit, Cobalt Strike, PowerShell-Skripte, Carbanak, Griffon, Diceloader und Trion sowie Ransomware wie BlackMatter oder REvil. /FBI22l01/, /HEI22w03/, /ZDN22w02/

Ähnliche Attacken wurden von FIN7 bereits im Jahr 2020 durchgeführt, damals im Namen des Elektronikhändlers BestBuy. Ziel der Attacken waren Hotels, Restaurants und Einzelhandelsgeschäfte in den USA. Bei diesen Attacken wurden Flash-Laufwerke verschickt, die Malware beinhalteten. Außerdem wurde Kontakt per E-Mail oder telefonisch aufgenommen, um darauf zu drängen, die Laufwerke mit dem Rechner zu verbinden. /FBI22l01/, /HEI22w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.16 Cyberangriff auf Oiltanking

Übersicht

Laut /HEI22w07/ wurde am 29.01.2022 festgestellt, dass es zu einem Cyberangriff auf das Unternehmen Oiltanking gekommen ist. Oiltanking ist ein Tanklagerlogistikunternehmen und betreibt diverse Tanklager in Deutschland sowie anderen Ländern in Europa, Amerika, Afrika und Asien und ist damit ein Unternehmen einer kritischen Infrastruktur. Von den Angriffen waren allerdings nur deutsche Anlagen betroffen.

Beschreibung

Oiltanking wurde Opfer eines Cyberangriffs mit Ransomware, für den laut /COM22w01/ die Gruppierung BlackCat verantwortlich ist. Nach Entdeckung des Angriffs, wurden umgehend externe Spezialisten und Behörden zur Klärung hinzugezogen. Von den Angriffen waren alle Be- und Entladesysteme von Oiltanking in Deutschland betroffen, was dazu führte, dass Tankwagen nicht mehr beladen werden konnten. Dies wiederum führte dazu, dass viele Tankstellen in Norddeutschland, u. a. die des Unternehmens Shell, nicht mehr von Oiltanking beliefert werden konnten. Insgesamt waren 233 Tankstellen in Norddeutschland betroffen, in denen außerdem keine Kartenzahlung und keine automatische Anpassung der Preise mehr möglich war. Die Versorgungslage in Deutschland war durch den Angriff nicht gefährdet, da insgesamt 26 Unternehmen im Bereich der Tanklagerlogistik in Deutschland aktiv sind und diese die ausgefallenen Kapazitäten übernehmen konnten. /HEI22w07/

BlackCat ist eine bekannte Ransomware-Gruppierung, deren Angriffe erstmals im November des Jahres 2021 bekannt wurden und die seitdem bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. BlackCat ist dabei die erste Organisation, die ihre Ransomware in der Programmiersprache Rust geschrieben hat, wodurch die Ransomware relativ einfach auf mehrere Betriebssysteme und Prozessarchitekturen anzupassen ist und damit speziell auf ein ausgewähltes Ziel zugeschnitten werden kann. Wie üblich erfolgt bei einem Angriff eine Verschlüsselung der Daten und eine Erpressung von Lösegeld für deren Entschlüsselung.

Für den Fall des Nichtbezahlens des Lösegeldes, wird mit der Veröffentlichung der Daten gedroht. Weitere Informationen zur BlackCat-Gruppierung finden sich in Abschnitt B.14.19.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.17 Cyberangriff auf Nordex

Übersicht

Am 31.03.2022 wurde festgestellt, dass es zu einem Cyberangriff auf Nordex, einem der weltweit größten Hersteller und Service Provider von Windenergieanlagen (kritische Infrastruktur) mit Niederlassungen in mehr als 30 Ländern und Hauptsitz in Deutschland, gekommen ist. Aufgrund des Angriffs wurden vorsorglich IT-Systeme an mehreren Standorten abgeschaltet, um eine weitere Ausbreitung zu verhindern. /BIS22r09/, /CYB22w01/, /NOR22w01/

Beschreibung

Nordex wurde Ziel eines Cyberangriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Conti bekannt hat. Der Angriff wurde frühzeitig bemerkt und es wurden umgehend Gegenmaßnahmen eingeleitet, wobei als Vorsichtsmaßnahme IT-Systeme an mehreren Standorten und in mehreren Geschäftsbereichen abgeschaltet wurden. Außerdem wurde der Fernzugriff auf von Nordex verwaltete Anlagen vorsorglich abgeschaltet. Der Angriff blieb auf interne Systeme bei Nordex beschränkt, ein Übergreifen auf Anlagen der Kunden von Nordex konnte nicht festgestellt werden. Die von Nordex betreuten Windenergieanlagen blieben ebenfalls ohne Beeinträchtigung weiter in Betrieb. /BLE22w04/, /NOR22w01/

Trotz der sofort eingeleiteten Maßnahmen zur Eingrenzung der Auswirkungen und zur Wiederherstellung der Systeme waren laut /SEC22w04/ auch mehr als eine Woche nach dem Cyberangriff noch nicht alle IT-Systeme wieder in Betrieb.

Conti ist eine bekannte Ransomware-Gruppierung, die von einer russischen Gruppierung betrieben wird und bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit

durchgeführt hat. In der Regel verschafft sich Conti Zugang zu einem Unternehmensnetzwerk, nachdem ein Gerät durch einen Phishing-Angriff mit den Schadprogrammen Bazar-Loader oder TrickBot infiziert wurde. Darauffolgend breitet sich Conti lateral im Opfernetzwerk aus und stiehlt Daten, die auf Conti-Server geladen werden. Dann erfolgt die Verschlüsselung der Daten und die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie: Es wird ein Lösegeld für die Entschlüsselung der Daten verlangt. Wird dieses nicht gezahlt, werden die Daten nicht entschlüsselt und zusätzlich veröffentlicht. /BLE22w04/

Laut /BSI22r10/ wurden ca. 40 % (etwa 24 GB) der gestohlenen Daten von Conti auf deren Webseite veröffentlicht. Bei den Daten handelt es sich um insgesamt 18 Archive im tar- und rar-Format. Dies lässt darauf schließen, dass von Nordex kein Lösegeld bezahlt wurde und mit der Veröffentlichung der Daten begonnen wurde. Über eine Höhe des geforderten Lösegeldes oder weitere Einzelheiten sind keine Informationen verfügbar.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.18 Cyberangriff mit Black Basta Ransomware

Übersicht

Laut /BSI22r07/ ist seit April 2022 eine neue Ransomware-Gruppierung mit dem Namen Black Basta aktiv. Bis heute kam es bereits zu diversen erfolgreichen Cyberangriffen dieser Gruppierung, womit sie innerhalb eines kurzen Zeitraums zu einer bedeutenden Bedrohung geworden ist. Dabei wurden weltweit Unternehmen aus diversen Branchen, wie beispielsweise Fertigungsindustrie, Baugewerbe, Transportwesen, Telekommunikationsunternehmen, pharmazeutische Industrie, Kosmetikindustrie oder Autohändler angegriffen. /HAC22w02/ Black Basta nutzt dabei die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie. Vor dem Verschlüsseln der Daten werden diese extrahiert. Wird dann kein Lösegeld für das Entschlüsseln der Daten gezahlt, werden diese nicht entschlüsselt und außerdem veröffentlicht. /BSI22r07/

Beschreibung

Die ersten bekannt gewordenen Angriffe der Ransomware-Gruppierung Black Basta er-folgten in der zweiten Aprilwoche 2022. Die Angriffe erfolgten weltweit, wobei in Deutschland unter anderem die Deutsche Windtechnik aus Bremen ein Opfer der Angriffe wurde. /BSI22r07/ Innerhalb weniger Wochen wurden bereits diverse Unternehmen weltweit erfolgreich angegriffen, wobei die Lösegeldforderungen von Opfer zu Opfer variierten, aber im Bereich einiger Millionen US-Dollar lagen. /BLE22w02/ Der Angriff auf die Deutsche Windtechnik war dabei einer der ersten Angriffe der Gruppierung Black Basta. Er erfolgte am 11.04.2022. Infolge des Angriffs wurden die Datenüberwachungsverbindungen zu den Windenergieanlagen aus Sicherheitsgründen abgeschaltet. Diese konnten nach 1-2 Tagen wieder aktiviert werden. An den Windenergieanlagen ist kein Schaden entstanden. Als Folge der Angriffe hat die Deutsche Windtechnik eine neues IT-Sicherheitskonzept implementiert. /DEU22w01/

Laut /BSI22r07, BLE22w02/ handelt es sich bei der Gruppierung Black Basta vermutlich nicht um eine neue Gruppierung, sondern eher um eine Neuauflage einer früheren, hochrangigen Ransomware-Gruppierung. Hinweise darauf liefert die Tatsache, dass in kurzer Zeit viele erfolgreiche Angriffe durchgeführt wurden sowie die routinierte Verhandlungsweise mit den Opfern. Die Angriffe der Gruppierung Black Basta zeigen Ähnlichkeiten zur Gruppierung Conti (ähnlicher Verhandlungsstil, ähnliches Design der Webseite), wobei sich die von Black Basta genutzte Software zur Verschlüsselung der Dateien von der von Conti genutzten deutlich unterscheidet. Laut /HAC22w02/ bestreitet Conti, mit Black Basta in Verbindung zu stehen. Laut /SEC22w03/ gibt es Hinweise, die darauf hindeuten, dass es sich bei Black Basta um eine russische Gruppierung handelt.

Laut /SEC22w03/, /BLE22w02/ wird bei den Angriffen von Black Basta folgendermaßen vorgegangen: Nach dem Eindringen in das Opfernetzwerk wird gezielt nach dem Domain Controller gesucht und sich anschließend seitwärts im Netzwerk bewegt. Dabei werden auf kompromittierten Domain Controllern von Black Basta Gruppenrichtlinienobjekte erstellt, um Windows Defender zu deaktivieren. Gleichzeitig wird versucht, Antivirenprodukte auszuschalten. In der letzten Phase des Angriffs wird die Ransomware auf den Zielgeräten installiert. Dies geschieht mittels eines verschlüsselten PowerShell-Befehls, der Windows Management Instrumentation (WMI) nutzt, um die Ransomware an ausgewählte IP-Adressen zu senden. Anschließend löscht die Ransomware die virtuellen Schattenkopien und andere Sicherungsdateien, bevor die Verschlüsselung durchgeführt wird.

Die Ransomware startet den Computer im abgesicherten Modus neu, darauffolgend wird ein gekaperter Windows-Dienst (z. B. Fax) gestartet, der wiederum die Verschlüsselung startet. Die Verschlüsselungssoftware selbst muss mit Administratorrechten ausgeführt werden, ansonsten ist eine Datenverschlüsselung nicht möglich. Des Weiteren wird durch die Ransomware der Bildschirmhintergrund geändert und eine Nachricht angezeigt, dass Daten verschlüsselt wurden. Die Verschlüsselungssoftware verwendet den ChaCha20-Algorithmus zur Verschlüsselung der Dateien, wobei der ChaCha20-Schlüssel mit einem öffentlichen RSA-4096-Schlüssel verschlüsselt wird. Laut /MAL22w01/ ist ChaCha20 ein kryptografischer Algorithmus, der für seine Geschwindigkeit bekannt ist. Er wird parallel mit Multithreading ausgeführt, um die Verschlüsselung zu beschleunigen, eine Entdeckung zu vermeiden und den Durchsatz der Ransomware zu erhöhen. Verschlüsselten Dateien wird die Endung .basta angefügt, außerdem wird ein benutzerdefiniertes Symbol angezeigt.

Laut /BSI22r08/, /UPT22w01/ wurde die Software von Black Basta weiterentwickelt und ist mittlerweile in der Lage, neben Windows-Systemen auch virtuelle Maschinen auf VMWare-ESXi-Servern unter Linux zu verschlüsseln. Dabei verschaffen sich die Angreifer Zugang zu ESXi-Servern und nach dem Start der Ransomware sucht diese nach dem Ordner /vmfs/volumes. Daran anschließend beginnt die Software mit der Verschlüsselung des Ordners, der standardmäßig alle virtuellen Maschinen des Linux-Servers enthält. Die Verschlüsselung erfolgt auch hier mit dem ChaCha20-Algorithmus.

Laut /BLE22w03/ hat sich die Black Basta-Gruppierung mit der Gruppierung QBot (QuakBot) zusammengeschlossen, um sich über gehackte Unternehmensumgebungen zu verbreiten. QBot ist eine Malware für Windows-Systeme, die ursprünglich zum Ausspähen von Bankdaten entwickelt und in Richtung des Ausspähens von Windows-Domänen-Zugangsdaten weiterentwickelt wurde. Außerdem ist QBot in der Lage, Malware-Programme auf infizierte Geräte zu übertragen. Die Opfer werden in der Regel durch Phishing-Angriffe mit maliziösen Anhängen mit QBot infiziert. QBot wird dabei für den Erstzugriff auf ein Ziel-Netzwerk verwendet, Black Basta hat es weiterhin genutzt, um sich seitlich im Netzwerk zu verbreiten. Eine Zusammenarbeit zwischen einer Ransomware-Gruppierung und QBot ist nicht unüblich, QBot werden zahlreiche Kooperationen mit anderen Ransomware-Gruppierungen nachgesagt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.19 Cyberangriff mit BlackCat Ransomware

Übersicht

Laut /FBI22l02/, /BSI22r05/ kommt es seit mindestens Mitte November des Jahres 2021 zu Angriffen einer neuen Ransomware-Gruppierung mit dem Namen BlackCat (auch bekannt als ALPHV oder Noberus). Hierbei handelt es sich um eine Ransomware-as-a-Service-Gruppierung, bei der es Hinweise darauf gibt, dass sie bereits über umfangreiche Erfahrungen und Netzwerke mit Ransomware-Operationen verfügt. Laut /FBI22l02/ sind weltweit bis Mitte April 2022 mindestens 60 Fälle bekannt geworden, bei denen es zu einem erfolgreichen Angriff von BlackCat gekommen ist. Dabei wurden laut /SEC22w01/ Firmen wie Moncler, Swissport oder Inetum Opfer der Angriffe. Laut /BSI22r05/ ist BlackCat die erste bekannte Ransomware, die in der Programmiersprache Rust entwickelt wurde.

Beschreibung

Die ersten bekannt gewordenen Cyberangriffe der Ransomware-Gruppierung BlackCat erfolgten laut /FBI22l02/ im November 2021. Es wurden diverse Firmen weltweit angegriffen, wobei in Deutschland laut /BSI22r06/, /SEC22w02/ zwei Unternehmen, die im Bereich der Lagerung und Lieferung von Öl und Mineralöl-Produkten tätig sind, betroffen waren. Dies waren die Oiltanking Deutschland GmbH, die Tanklager in Deutschland betreibt, sowie die Mabanaft-Gruppierung, die Importeur, Großhändler und Lieferant von Heizöl, Benzin, Dieselkraftstoff, Düsentreibstoff und anderen Ölprodukten ist. /SEC22w02/ Weltweit wurden laut /ZDN22w03/ mehrere Unternehmen in Europa, Afrika, Asien und den USA angegriffen, wobei meist Firmen mit kritischer Infrastruktur das Ziel waren und mehr als 30 % der Angriffe auf US-Firmen abzielte. Laut /WAT22w02/ erfolgte Mitte Mai des Jahres 2022 ein Angriff von BlackCat auf staatliche IT-Systeme des österreichischen Bundeslandes Kärnten. Von diesem Angriff waren die Regierung, Bezirksverwaltungen, der Rechnungshof und das Verwaltungsgericht betroffen. Eine Lösegeldforderung von 5 Millionen US-Dollar wurde nicht bezahlt. Außerdem erfolgte laut /WAT22w02/ durch BlackCat ein Cyberangriff auf die ecuadorianische Hauptstadt Quito, wobei mehrere staatliche Systeme lahmgelegt wurden.

Ein weiterer Cyberangriff der Ransomware-Gruppierung BlackCat auf Unternehmen der kritischen Infrastruktur erfolgte am 22. Juli 2022 auf den luxemburgischen Netzbetreiber Creos und den luxemburgischen Energieversorger Enovos, die beide zur Encevo-Gruppierung gehören und eine Gaspipeline sowie die Stromversorgung in Luxemburg betreiben. Bei dem Angriff wurden Daten verschlüsselt und außerdem 150 GB Daten (180.000 Dateien) gestohlen, darunter vertrauliche Daten wie Verträge, Ausweiskopien, E-Mails und Daten zu Bankkonten. Unmittelbar nach Bekanntwerden des Angriffs wurde von den Geschädigten Anzeige erstattet, die zuständigen Behörden informiert und ein Krisenstab eingerichtet. Die Täter forderten ein Lösegeld in unbekannter Höhe, welches aber nicht gezahlt wurde. Daraufhin wurden die Daten zumindest in Teilen veröffentlicht. Der Angriff hatte Auswirkungen auf den Betrieb der Kundenportale, die Strom- und Gasversorgung wurden aber nicht beeinflusst. Die verschlüsselten Daten wurden aus gesicherten Servern wieder hergestellt, die Überwachung der Systeme wurde verstärkt und alle Passwörter geändert. /BOR22w01/, /SEC22w09/, /ENC22w01/, /SEC22w08/

Die Vorgehensweise war in allen bekannten Fällen ähnlich. Laut /FBI22l02/ werden von BlackCat zuvor kompromittierte Benutzeranmeldeinformationen genutzt, um einen ersten Zugang zum System des Opfers zu erhalten. Die anfängliche Bereitstellung der Ransomware erfolgt mittels Power-Shell-Skripten in Verbindung mit Cobalt Strike. Sobald ein Zugang hergestellt werden konnte, werden Active Directory-Benutzer und Administratorkonten kompromittiert. Außerdem wird der Windows Task Scheduler verwendet, um maliziöse Gruppenrichtlinienobjekte zu konfigurieren und die Ransomware so im System des Opfers weiter zu verteilen. Während der Kompromittierung werden auch legitime Windows-Tools wie das Windows-Verwaltungstool Microsoft Sysinternals genutzt, um Anti-Malware-Tools zu deaktivieren und Ransomware-Programme zu starten. Bevor die Ransomware zur Verschlüsselung der Daten auf dem Opfernetzwerk ausgeführt wird, werden die Daten des Opfers, darunter auch Informationen von Cloud-Anbietern, extrahiert.

Laut /KAS22w01/ umfasst das Arsenal von BlackCat diverse Elemente. Neben Kyrptor zur Verschlüsselung von Dateien wird auch das Programm Fendr zum Exfiltrieren von Daten aus dem Opfernetzwerk verwendet. Dieses Tool deutet darauf hin, das BlackCat enge Verbindungen zur Gruppierung BlackMatter (auch bekannt als Darkside, verantwortlich für Angriffe auf Colonial Pipeline (siehe Abschnitt B.13.5)) hat, da diese bis-lang als einzige bekannte Akteure dieses Tool eingesetzt haben.

Zudem verwendet BlackCat das PsExec-Tool für Seitwärtsbewegungen im Netzwerk des Opfers sowie die Software Mimikatz und Nirsoft zum Extrahieren von Netzwerkpasswörtern.

Laut /SEC22w01/ ist BlackCat die erste professionell genutzte Ransomware, die in der Programmiersprache Rust geschrieben wurde. Laut /BSI22r05/ ist Rust eine von Mozilla seit dem Jahr 2010 entwickelte Programmiersprache, die eine praxisnahe Alternative zu C++ darstellt. Dabei bietet Rust die Möglichkeit, relativ einfach auf mehrere Plattformen übersetzt zu werden, was es leichter macht, die Ransomware auf mehrere Betriebssysteme und Prozessarchitekturen anzupassen. BlackCat kann laut /SEC22w01/ auf Windows-, Linux- und VMWare ESXi-Systeme abzielen. Laut /REG22w01/ hat Rust im Gegensatz zu C++ Sicherheitsmaßnahmen eingebaut, was bedeutet, dass die Malware stabiler und zuverlässiger sein könnte. Laut /HAC22w01/ gilt Rust als speichersicher und leistungsfähig und bietet neben Entwicklungsvorteilen auch eine geringere Erkennungsrate von statischen Analysetools, die nicht an alle Programmiersprachen angepasst sind.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.20 Cyberangriffe mit Quietexit

Übersicht

Im Dezember 2019 wurde vom IT-Sicherheitsunternehmen Mandiant aufgedeckt, dass die APT-Gruppierung UNC3524 Unternehmen in einem Zeitraum von teilweise 18 Monaten ausspioniert und deren E-Mails mitgelesen hat. Um sich Zugriff auf die Firmennetzwerke zu verschaffen, hatten die Angreifer Backdoors auf IoT-Geräten (Internet of Things) und anderen Systemen installiert, die üblicherweise nicht überwacht und durch Sicherheitssoftware geschützt werden können. Eine der Backdoors wird als Quietexit bezeichnet. Da die Angreifer systemeigene Programme und Prozesse geschickt nutzten, konnten ihre Aktivitäten so lange unerkannt bleiben.

Beschreibung

Die im Dezember 2019 vom IT-Sicherheitsunternehmen Mandiant aufgedeckte APT-Gruppierung UNC3524 hat Unternehmen in einem Zeitraum von teilweise 18 Monaten ausspioniert und deren E-Mails gelesen. Um nicht entdeckt zu werden, schleusten die Angreifer Backdoors auf IoT-Geräte (Internet of Things) ein, die üblicherweise nur wenig überwacht werden (keine Endpoint-Detektion oder Response-Werkzeuge), keine Sicherheitsupdates erhalten und für die keine spezielle Sicherheitssoftware existiert (keine Antivirenprogramme). Zu den mit den Backdoors infizierten Geräten gehören SAN-Arrays (Storage Area Networks), Load Balancer und Controller für das WLAN, auf denen oft ältere Versionen von Berkeley Software Distribution (BSD) oder Community Enterprise Operating System (CentoS) installiert sind. Von diesen Geräten aus wurde dann der Angriff auf weitere Teile des Firmennetzes ausgeweitet. Die Angreifer setzten dabei Router und sogar aus dem Internet erreichbare Kameras von Konferenzräumen als Command-and-Control-Server (C&C) ein. Die Suche nach der Schadsoftware gestaltet sich entsprechend schwierig. Mandiant empfiehlt deshalb den Einsatz des Programms grep, mit dem sich Dateien nach bestimmten Textfolgen (in diesem Fall Programmcode) durchsuchen lassen. /HEI22w16/, /ART22w01/, /MAN22w03/

Eine der von UNC3524 eingesetzten Backdoors wird als Quietexit bezeichnet. Sie nutzt das zur Verschlüsselung verwendete SSH-Protokoll und eine modifizierte Version der frei verfügbaren Software Dropbear (Ressourcen schonender SSH-Server und -Client /NET20w01/), um eine TCP-Verbindung vom infizierten Gerät im Firmennetzwerk zum externen C&C-Server der Angreifer aufzubauen. Die anschließend aufgebaute SSH-Verbindung ist dagegen vom C&C-Server auf das infizierte Gerät gerichtet. Ein alternativer Zugriffsweg der Backdoor Quietexit nutzt die Webshell[24] Regeorg zur Einrichtung eines SOCKS-Proxys[25]. Dabei achteten die Angreifer darauf die Namen der Webshell-Dateien auf den Webservern so zu wählen, dass sie zum infizierten System passten. Falls die Backdoor Quietexit entfernt wurde, konnte sie über die Webshell neu installiert werden. Um nicht aufzufallen, nutzten die Angreifer eine Vorgehensweise, die unter dem Namen Living off the Land (LotL) bekannt ist.

---

[24] Eine Webshell ist ein schadhafter Programmcode, der einem Angreifer die Kompromittierung von Webservern ermöglicht /IMP22w01/.

[25] Ein SOCKS-Proxy ist ein Proxy-Server, der das Protokoll SOCKS (Abkürzung von SOCKetS) verwendet, welches die Kommunikation von Servern über eine Firewall erleichtert /FIN22w01/.

Dabei werden für den Angriff Standard-Programme und Standard-Prozesse des infizierten Systems eingesetzt /DIG22w01/. Zum Beispiel verwendeten sie Zeichenfolgen für Domänennamen, die für den Gerätehersteller plausibel erscheinen. Datenverkehr und Datenvolumen wurden nach Möglichkeit beschränkt. Aufgrund dieser Maßnahmen konnten die Angreifer ihre Aktivitäten über Monate verbergen. /HEI22w16/, /ART22w01/, /MAN22w03/

Auf welche Weise sich die Angreifer initialen Zugriff auf die Firmennetzwerke verschafften ist nicht bekannt. Sie nutzten die mit der Backdoor Quietexit infizierten Systeme für die laterale Ausweitung ihrer Aktivitäten auf weitere Teile des Firmennetzwerks. Die APT-Gruppierung UNC3524 zielte darauf ab Zugriff auf die Exchange-E-Mail-Postfächer von Führungskräften und Mitarbeitern zu erhalten, deren Tätigkeiten die Unternehmensentwicklung, Fusionen und Übernahmen oder die IT-Sicherheit betreffen und deren E-Mails mitzulesen. Dabei wurden integrierte Windows-Protokolle genutzt. Es wird vermutet, dass der Angriff auf das IT-Sicherheitsteam dazu diente, um zu testen, ob die installierte Schadsoftware unentdeckt bleibt. Das professionelle Vorgehen der APT-Gruppierung UNC3524 spricht dafür, dass diese staatlich gefördert wird. Die Angriffstechniken sind vergleichbar mit denen russischer APT-Gruppierungen wie APT28 und APT29. Das IT-Sicherheitsunternehmen Mandiant war jedoch nicht in der Lage UNC3524 einer dieser Gruppierungen oder einer staatlichen Organisation zuzuordnen. /HEI22w16/, /ART22w01/, /MAN22w03/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.21 Cyberangriffe mit Hyperbro

Übersicht

Seit März 2022 greift die APT-Gruppierung APT27, auch bekannt unter dem Namen Emissary Panda, verstärkt deutsche Unternehmen mit der Schadsoftware Hyperbro an. Dabei sind hauptsächlich Pharma- und Technologieunternehmen betroffen. Das Ziel der Angriffe scheint der Diebstahl von Geschäftsgeheimnissen und geistigem Eigentum zu sein.

Beschreibung

Das Bundesamt für Verfassungsschutz (BfV) warnt in seinem Cyberbrief 01/2022, dass seit März 2021 die APT-Gruppierung APT27 Schwachstellen im Microsoft Exchange Server nutzt, um sich initialen Zugriff auf die IT-Netzwerke deutscher Unternehmen zu verschaffen. Weiterhin gibt das BfV an, dass die Zahl der Angriffe durch APT27 auf deutsche Unternehmen zunimmt. Dabei nutzen die Angreifer das Remote Access Tool (RAT) Hyperbro, um die Netzwerke auszuspionieren und Geschäftsgeheimnisse sowie geistiges Eigentum zu stehlen. Von den Angriffen sind hauptsächlich Unternehmen aus der Pharmaindustrie und Technologieunternehmen betroffen. Zudem kann das BfV nicht ausschließen, dass die Angreifer versuchen werden, die Netzwerke von Kunden und Dienstleistern zu kompromittieren, um Lieferkettenangriffe durchzuführen. Die APT-Gruppierung APT27, welche auch unter dem Namen Emissary Panda bekannt ist, ist seit 2010 aktiv und soll im Auftrag des chinesischen Staates handeln. /HEI22w17/, /ITS22w01/

Die RAT-Schadsoftware Hyperbro besteht aus vier Komponenten: Einem legitimen ausführbaren Loader msmpeng.exe oder vfhost.exe der Software CyberArk, der mit einem gültigen, aber abgelaufenen Zertifikat ausgestattet ist, der schadhaften DLL3-Datei vftrace.dll, die über den Loader per DLL-Hijacking geladen wird, der Payload thumb.dat, den ausführbaren Shellcode, eine schadhafte DLL-Datei sowie Informationen über den Command-and-Control-Server (C&C) der Angreifer beinhaltet und der Konfigurationsdatei config.ini der Schadsoftware. Bei der Installation von Hyperbro lädt der Loader zunächst die Dateie vtrac.dll, die wiederum die Payload thumb.dat lädt und entschlüsselt. Ohne Administratorrechte werden die Daten von Hyperbro im Ordner %ProgrammData%\windefenders\ abgelegt. Liegen Administratorrechte vor, werden die Daten dagegen im Ordner %ProgrammFiles%\Common Files\windefenders\ gespeichert. Die Schadsoftware wird am neuen Speicherort neu gestartet und imitiert den Windows Defender. Ist Hyperbro bereits installiert und wird die Schadsoftware einfach nur ausgeführt, laufen zunächst die gleichen Schritte ab wie beim Installationsprozess. Nach dem Laden der Payload thumb.dat erfolgen jedoch andere Schritte. Ohne Administratorrechte wird ein Run Key in der Windows Registry erzeugt. Mit Administratorrechten wird dagegen ein Service erstellt. Auf beide Arten wird eine persistente Verbindung sichergestellt. Die Datei config.ini baut dann die Kommunikation mit dem C&C-Server der Angreifer über den TCP-Port 443 auf.

Über den C&C-Server erhält die Schadsoftware Hyperbro weitere Anweisungen von den Angreifern und es können weitere Schadsoftware-Werkzeuge wie z. B. Key-Logger geladen werden. /PRS22w01/

In seinem Cyberbrief veröffentlicht das BfV auch Angriffsindikatoren (Indicators of Compromise IOC). Dazu gehören die IP-Adressen (104.168.236.46, 103.79.77.200 und 87.98.190.184) der C&C-Server der Angreifer sowie die Namen von bestimmten Dateien, Pfaden und Prozessen. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu reduzieren, sollten daher nicht nur die entsprechenden Sicherheitsupdates für Microsoft Exchange und den Zoho AdSelf Service Plus 1 installiert werden, um deren Schwachstellen zu schließen, sondern die Systeme sollten auch auf die IOCs überprüft werden. /HEI22w17/, /PRS22w01/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.22 Cyberangriff auf WatchGuard Firewalls

Übersicht

Seit Juni 2019 wurden Firewalls von WatchGuard mit der Schadsoftware Cyclops Blink infiziert, über die von den Angreifern Daten aus dem Netzwerk gestohlen werden konnten. Zudem konnte die Schadsoftware das befallene Gerät zum Teil eines Botnetzes machen und für Angriffe auf andere Ziele nutzen. Nach Angaben von WatchGuard waren etwa ein Prozent ihrer Geräte von der Schadsoftware betroffen. 2022 konnte das Botnet vom FBI zerschlagen werden.

Beschreibung

Nach einem gemeinsamen Bericht des britischen Cyberabwehrzentrums NCSC, des CISA, der NSA und des FBIs erfolgt seit Juni 2019 eine Angriffswelle gegen die Firebox-Router des Herstellers WatchGuard /CIS22i02/. Dabei nistet sich die Schadsoftware Cyclops Blink in den Router ein. Sie kann Geräteinformationen an den Command-and-Control-Server (C&C) der Angreifer übermitteln. Danach kann die Schadsoftware je nach Einsatzbedarf weitere Schadsoftwarekomponenten nachladen.

Mit diesen können Daten aus dem Netzwerk gestohlen werden. Darüber hinaus kann Cyclops Blink den Router zum Teil eines Botnetzes machen und für Angriffe auf andere Ziele nutzen. Er kann dabei von den Angreifern als C&C-Server oder auch als Drohne eingesetzt werden /HEI22w10/. Zusätzlich kapert die Schadsoftware den Update-Prozess, indem sie sich als Firmware-Update installiert, wodurch sie einen Neustart übersteht. Nach den Angaben von WatchGuard war etwa ein Prozent ihrer in Umlauf befindlichen Geräte infiziert. Eine Infektionsgefahr bestand nur dann, wenn in den Geräten die externe Steuerung über das Internet eingeschaltet war, welche aber in den Standardeinstellungen deaktiviert ist. Wenn ein Gerät mit Cyclops Blink infiziert ist, müssen sämtliche Passwörter als kompromittiert betrachtet werden. Auch wenn kein Router von WatchGuard verwendet wird, ist Vorsicht geboten. Nach den Angaben des NCSC ist die Schadsoftware flexibel genug, um schnell auf andere Geräte übertragen werden zu können. /STE22w01/, /HEI22w10/, /KUD22w01/

Die Cyberangriffe mit Cyclops Blink sind die Fortsetzung einer weiter zurückliegenden Kampagne mit Namen VPNFilter, die 2018 von US-Behörden erfolgreich beendet wurde. Für beide Angriffe soll die APT-Gruppierung Sandworm verantwortlich sein, welche dem russischen Auslandsgeheimdienst GRU zugeordnet wird. /STE22w01/, /HEI22w10/, /KUD22w01/

WatchGuard hat eine entsprechende Anleitung mit Softwarewerkzeugen zusammengestellt, mit denen Administratoren eine Infektion erkennen und beheben können. Nach Angaben des Herstellers sind keine Fälle bekannt, in denen Daten von Kunden oder von WatchGuard selbst gestohlen wurden. Im April 2022 wurde das von Cyclops Blink gebildete Botnet vom FBI zerschlagen, bevor es für Cyberangriffe genutzt werden konnte. Das FBI entfernte zudem die Schadsoftware Cyclops Blink von WatchGuard-Geräten, die es als C&C-Server identifiziert hatte und benachrichtigte zuvor die entsprechenden Nutzer in den USA und im Ausland. Diese sollten zusätzlich die Anleitungen von WatchGuard befolgen. /HEI22w10/, /BLE22w06/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.23 Physischer Angriff auf IT-Infrastruktur in Frankreich

Übersicht

In der Nacht des 27.04.2022 wurden in Frankreich von unbekannten Angreifern an verschiedenen Stellen Glasfaserkabel durchtrennt, die die Städte Paris, Lyon, Rouen und Straßburg miteinander verbinden. In der Folge kam es zu Netzwerkausfällen von Internet- und Telefonanschlüssen in mehreren Städten entlang der Strecken.

Beschreibung

Mehrere Medien berichteten am 27.04.2022 über eine vorsätzliche Zerstörung von Glasfaserkabeln in Frankreich. Die Kabel waren in der vorrausgegangenen Nacht zwischen 2:00 Uhr und 4:00 Uhr durchtrennt worden. Dabei wurde die Netzinfrastruktur von zwei Anbietern unterbrochen, darunter Free. Es wurden drei Backbone-Strecken an verschiedenen Stellen zerstört, welche von Paris nach Lyon, Rouen und Straßburg führen. Die Kabel sind Eigentum des Netzwerkbetreibers SFR und werden von Free gemietet. In der Folge kam es in mehreren Städten entlang der Strecken zur Verlangsamung von Netzwerkverbindungen und zu Netzwerkausfällen von Internet- und Telefonanschlüssen. Insgesamt waren zehn Internet- und Infrastrukturorganisationen betroffen. Bereits am Vormittag des 27.04.2022 konnten die teils massiven Störungen aber wieder abgefangen werden, indem der Datenverkehr vielfach manuell oder automatisch auf andere Kabel umgeleitet wurde /WIR22w02/. /BSI22i06/, /HEI22w18/, /WIR22w02/

Wer die Kabel zerstört hat ist nicht bekannt, die Angriffe sind jedoch koordiniert durchgeführt worden. Die Angreifer wussten offenbar an welchen Stellen sie an die Kabel gelangen können und auf welche Weise sie den größten Schaden erzielen. Die Kabel wurden jeweils an zwei Stellen durchtrennt und die Zwischenstücke wurden entfernt, um die Reparatur zu erschweren. Bereits unmittelbar nach den Angriffen hat die Pariser Staatsanwaltschaft Untersuchungen eingeleitet. Der hier beschriebene Angriff ist kein Einzelfall. Bereits im Mai 2020 sind in Frankreich mehrere Netzwerkkabel unterbrochen worden. Die Zerstörung der Glasfaserkabel am 27.04.2022 wurde jedoch deutlich professioneller und koordinierter durchgeführt. /BSI22i06/, /CYB22w03/, /WIR22w02/

Kerntechnischer Bezug

Bislang liegen noch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.24 Cyberangriff auf ein Unterseekabel

Übersicht

Anfang April 2022 versuchten international agierende Angreifer einen Cyberangriff auf ein Unterseekabel bei Hawaii durchzuführen. Der Angriff konnte rechtzeitig erkannt und gestoppt werden. Es kam zu keinen Schäden.

Beschreibung

Ein Unterseekabel bei Oahu, welches der Anbindung von Internet, Festnetz und dem Mobiltelefonnetz von Hawaii mit der pazifischen Region dient, wurde Anfang April 2022 zum Ziel eines Cyberangriffs /CYB22w04/, /STA22w01/. International agierende IT-Angreifer hatten zuvor Zugangsdaten von einem privaten Telekommunikationsunternehmen auf dem US-amerikanischen Festland gestohlen, das mit dem Unterseekabel in Verbindung steht und sich damit Zugriff auf die Server des Unternehmens verschafft /CYB22w04/, /THR22w01/. Durch einen Hinweis ihrer Kollegen vom Festland der USA, konnte der Angriff durch die Homeland Security Investigation (HSI) Hawaiis abgewehrt werden /HTE22w01/. Es kam zu keinen Schäden. Im Anschluss wurden Verhaftungen vorgenommen. Wer den Angriff durchgeführt hat und welches Telekommunikationsunternehmen betroffen war, wurde vom HSI allerdings nicht bekannt gegeben, um die Strafverfolgung nicht zu gefährden. /BSI22i07/, /HNN22w01/

Um welche Art von Cyberangriff es sich gehandelt hat ist ebenfalls unklar. Nach Meinung von Experten hätten Kommunikationsverbindungen abgeschaltet oder auch individuelle Ziele angegriffen werden können. Da Unterseekabel 95 % des internationalen Internet-Datenverkehrs führen, werden sie in wachsendem Maß zum Ziel autoritärer Regierungen. Diese versuchen den Internetzugriff zu kontrollieren oder den Datenverkehr zu überwachen, um sensible Informationen zu stehlen. Parallel setzen die Betreiber-Unternehmen zunehmend Remote-Management-Systeme für ihre Kabelnetzwerke ein, von denen viele über mangelhafte Sicherheitsfunktionen verfügen.

Dies versetzt IT-Angreifer in die Lage an beliebigen Orten auf der Welt über das Internet Zugriff auf diese Systeme zu erhalten und die Kabelsignale physisch zu manipulieren und zu kontrollieren. /CYB22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.25 Strahlenschutz Spanien

Übersicht

Zwischen März und Juni 2021 kam es zu einem Cyberangriff auf das Radioaktivitäts-überwachungs- und -warnsystem Spaniens (Red de Alerta a la Radiactividad (RAR)). Das RAR-System dient zur Überwachung der Gammastrahlungswerte in ganz Spanien und wird von der Generaldirektion für Katastrophenschutz und Notfälle (DGPCE) und dem Ministerium für innere Angelegenheiten verwaltet, betrieben und gewartet. Aufgrund des Angriffs konnten hunderte Detektoren des RAR-Systems, welches zur kritischen Infrastruktur gehört, zur Erkennung von Gammastrahlung temporär nicht genutzt werden/HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Beschreibung

Das RAR-System Spaniens, welches zur Überwachung der Gammastrahlungswerte in ganz Spanien dient, wurde zwischen März und Juni 2021 Opfer eines Cyberangriffs. Das RAR-System umfasst ca. 800 Detektoren für Gammastrahlung, die landesweit in Spanien verteilt sind, und dient als Warnsystem für den Fall, dass die Gammastrahlungswerte ansteigen. Jeder der Detektoren ist mit einem zentralen Knotenpunkt verbunden, welcher sich im Kontrollzentrum der spanischen Zivilschutzbehörde Dirección General de Protección Civil y Emergencias (DGPCE) in Madrid befindet, welches sowohl Informationen sammeln als auch Befehle senden kann. Des Weiteren gibt es zehn regionale und sieben assoziierte Knotenpunkte, die einen alternativen Zugang zum RAR-System ermöglichen und über begrenzte Verwaltungsfunktionen verfügen. Durch den Angriff kam es zum Ausfall mehrerer hundert der über 800 Detektoren des RAR-Systems zur Erkennung erhöhter Gammastrahlungswerte. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Der Angriff erfolgte dabei in zwei Schritten. Zunächst verschafften sich die Angreifer unrechtmäßig Kontrolle über das Computersystem der DGPCE mit dem Ziel, eine Webanwendung aus dem Kontrollzentrum zu löschen, über welche das RAR-System verwaltet werden kann. In der zweiten Phase wurden im Laufe mehrerer Monate mehr als 300 der Gammastrahlungsdetektoren direkt angegriffen, um die Kommunikation zwischen diesen Detektoren und den Kontrollzentren zu unterbrechen. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Im Juli 2022 wurden zwei Verdächtige verhaftet, die angeblich für die Angriffe verantwortlich sind. Bei diesen handelt es sich um zwei ehemalige Mitarbeiter eines Drittanbieters, welcher im Auftrag der DGPCE mit der Wartung des RAR-Systems beauftragt war. Die beiden Verdächtigen waren dabei für die Wartung der Software zuständig, die sie bei dem Angriff löschen wollten. Es handelt sich also bei den Verdächtigen um Innentäter, durch deren fundierte Kenntnisse des Systems die Ausführung der Angriffe erleichtert wurde. Außerdem halfen die Kenntnisse dabei, die Urheberschaft der Angriffe zu verschleiern und damit die Ermittlungen zu erschweren. Das Motiv für den Angriff ist bisher unklar. Ausgangspunkt der Angriffe war ein öffentlich verfügbarer Internetzugang in einem Madrider Beherbergungsbetrieb. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Kerntechnischer Bezug

Ziel des Angriffs war das Radioaktivitätsüberwachungs- und warnsystem Spaniens, welches zur Überwachung der Gammastrahlungsaktivität in Spanien dient.

B.14.26 ZuoRAT

Übersicht

Im Mai 2022 wurde von den Sicherheitsforschern von Black Lotus Labs eine neue umfassende Kampagne zur Verbreitung eines auf Router zugeschnitten Remote Access Trojaners (RAT) publiziert. Der als ZuoRAT benannte Trojaner wurde spezifisch für Heimanwenderrouter und Router kleinerer Büros (Small Office/Homeoffice, SOHO) entwickelt und über einen Zeitraum von mindestens zwei Jahren gegen entsprechende Ziele eingesetzt.

Der ZuoRAT zeichnete sich dabei durch seine umfassenden Fähigkeiten aus, was den Angriff auf verschiedenste SOHO Router und seine Angriffswerkezuge betrifft. /MAL22r01/

Beschreibung

Mit der COVID-19 Pandemie kam es ab März 2020 zu einer deutlichen Verlagerung von Büroarbeitsplätzen in die als gesundheitlich sicherer eingeschätzten Heimarbeitsplätze. Infolgedessen wurden vermehrt Daten über Heimnetzwerke und damit SOHO Router geteilt, welche früher ausschließlich in Firmennetzwerken genutzt wurden. IT-Angreifer haben sich daher seit 2020 vermehrt auf Cyberangriffe auf Router, VPN-Verbindungen und andere für das Arbeiten im Homeoffice notwendige Infrastruktur konzentriert (siehe Abschnitt B.14.12 Pulse Connect Secure). Angriffe auf SOHO Router sind keine neue Erscheinung. So kam es 2016 zum gescheiterten Cyberangriff auf mehr als eine Million Telekom Router der Marke Speedport und 2016 wurde das Mirai Botnet bekannt, welches zum Teil auf übernommenen Realtek Routern basierte. Der ZuoRAT Trojaner zeichnete sich nicht nur dadurch aus, dass Teile der Mirai Schadsoftware massiv modifiziert in den Trojaner einflossen, sondern auch dass dieser Trojaner eine Vielzahl verschiedener Router angreifen kann und für anschließende Folgeangriffe im Netzwerk umfassend gerüstet ist. /BLL22r01/

Remote Access Trojaner dienen grundsätzlich IT-Angreifern zur Etablierung einer Backdoor, sodass sie einen temporären oder permanenten Einfallspunkt für die Angreifer etablieren. Der ZuoRAT Trojaner führt diesen ersten Angriffsschritt als erste Stufe einer Cyberangriffsserie aus, besitzt jedoch die Fähigkeit zur weiteren Verbreitung und für weitere Angriffe im betroffenen Netzwerk. Obwohl verfügbare Daten zeigen, dass unter anderem Router von ASUS, Cisco, DrayTek und NETGEAR betroffen sind, wurde bisher ausschließlich das vollständige Angriffsscript für Router des Typs JCG-Q20 bei erkannten ZuoRAT Trojanern erkannt. Zur erstmaligen Infektion der ausschließlich in China eingesetzten Router wurde ein Proof of Concept für ältere Schwachstellen (CVE-2020-26878 und CVE-2020-26879) durch die Angreifer verpackt in einer Windows Portable Executable genutzt. Mittels dieses Angriffswerkzeugs erlangt ZuoRAT zuerst Zugang zu Passwörtern des betroffenen Routers, dann Zugang zum Router selbst und anschließend wird weiterer Schadcode nachgeladen. Dieser Schadcode ermöglicht das umfassende Ausspionieren des auf dem Router verarbeiteten Datenverkehrs und die Übernahme des Datenverkehrs.

Im Rahmen der Ausspionierung können z. B. Accountdaten, verbundene IP-Adressen und Ziele der Datenströme ausgelesen werden.

Um zu erkennen, ob die Schadsoftware auf einem echten Router oder einer Testumgebung läuft, steuerte ZuoRAT per Kommando spezifische Webseiten mit IP-Erkennung an. Konnte keine IP ermittelt werden, löschte sich ZuoRAT selbst. /BLL22r01/

Die nächste Stufe der ZuoRAT Schadsoftware wird auf Kommando durch die Angreifer eingeleitet und dient dem Einwirken in verbundene Netzwerksysteme. Bis zu 2.500 verschiedene Funktionen wurden dafür in die Schadsoftware integriert. Hierzu zählt die vertiefte Auswertung des angeschlossenen LANs, das Auslesen von DNS-Verbindungen, die Speicherung von SSID Informationen und MAC-Adressen der angebundenen Geräte. Darauf aufbauend wurden DNS-Anfragen, also Domain Naming System Anfragen, welche IP-Adressen und ausgeschriebene Webadressen miteinander verbinden, von der Schadsoftware manipuliert. Hierdurch wurden legitime Webseitenaufrufe und Datenübertragungen auf von den Angreifern festgelegte IP-Adressen umgeleitet. Dies können Phishing-Webseiten sein oder Webseiten zur Verbreitung weiteren Schadcodes. Weitere Funktionen dienten dem Neuladen der Schadsoftware, dem Nachladen von Code oder der Abschaltung der Schadsoftware. /BLL22r01/

Der letzte Schritt der ZuoRAT Schadsoftware war der direkte Übergang vom Router auf angebundene Windows-Systeme. Hierzu wurde ein Loader für einen Windows-RAT an die angebundenen Systeme verteilt. Um die Infektionschancen zu erhöhen und die Entdeckungschancen zu minimieren, nutzte dieser Loader ein legitimes Zertifikat des chinesischen Technologiekonzerns Tencent. Über Shellcode wurde anschließend die Schadsoftware RAT CBeacon auf den Windows-Systemen installiert. Andere Systeme wie Linux, Mac oder Android wurden mit der Schadsoftware GoBeacon RAT angegriffen. Zusätzlich wurde auf die Schadsoftware Cobalt Strike zurückgegriffen. /BLL22r01/

Die ZuoRAT Schadsoftware wurde insbesondere auf Routern in den USA und Europa aufgefunden, jedoch auch in Hongkong und Taiwan. Sie verschleiert sich effektiv durch die Nutzung von bereits infizierten Routern als Systeme zur Kommunikation und zum Nachladen von Schadsoftware und nutzt insbesondere chinesische Services für Datenspeicherung, um eine direkte Erkennung zu vermeiden. Aufgrund vieler chinesischer Bezüge im Quellcode, dem Umfang und der Detailarbeit der ZuoRAT Schadsoftware wurde die Angriffsserie chinesischen staatlichen Stellen attribuiert.

„Zuo“ ist chinesisch für Links und leitet sich vom Dateinamen der Schadsoftware asdf, den linken vier Buchstaben der mittleren Tastaturreihe ab. /BLL22r01/

Um Cyberangriffe mit ZuoRAT oder ähnlicher Schadsoftware zu vermeiden, empfehlen die Forscher von Black Lotus Labs die folgenden Schritte: /BLL22r01/

- Nutzung der auf GitHub veröffentlichten Indicator of Compromise (IoC) für die genannten Loader und Schadsoftwares bei der Beobachtung und Sicherung von Netzwerken /GIT22w01/
- Sicherung von SOHO Routern durch regelmäßige Updates und dem Folgen der Best Practices bei der Einstellung der Sicherheitsmaßnahmen
- Einsatz von automatisierten Überwachungssystemen wie Secure Access Service Edge (SASE) im Geschäftsbereich.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.27 Cyberangriff auf Nexeya

Übersicht

Am 18.08.2022 wurde veröffentlicht, dass es zu einem Cyberangriff auf das französische Tochterunternehmen Nexeya des Rüstungsunternehmens Hensoldt gekommen ist. Hensoldt ist ein Rüstungsunternehmen mit Hauptsitz in Deutschland, welches auf Radarsysteme, optoelektronische Systeme, elektronische Kampfführung sowie Avionik spezialisiert ist. Nexeya ist auf den Entwurf und die Entwicklung von elektronischen Geräten für die Luftfahrt-, Verteidigungs-, Energie-, Bahn- und Raumfahrtbranche spezialisiert. Zu den Kunden von Hensoldt und Nexeya zählen somit auch Betreiber kritischer Infrastrukturen. Durch den Cyberangriff kam es zu Einschränkungen des Betriebs bei Nexeya. /HEI22w21, FAZ22w01, CSO22w02, HAN22w02/

Beschreibung

Nexeya wurde Ziel eines Cyberangriffs mit Ransomware, die der Ransomware-Gruppierung REvil zugeschrieben wird und am 12.08.2022 begonnen hat. Unmittelbar nach

Entdeckung des Angriffs wurden Maßnahmen zur Eindämmung und Bewertung eingeleitet. Es wurden Untersuchungen zu dem Angriff eingeleitet, wobei sowohl interne als auch externe Experten hinzugezogen wurden. Die nationalen Cybersicherheitsbehörden wurden über den Angriff informiert. Durch den Ransomware-Angriff, von dem beide Nexeya Datencenter in Frankreich betroffen waren, kam es zu einer Beeinträchtigung des laufenden operativen Geschäftsbetriebs, zudem war die Webseite des Unter-nehmens nicht erreichbar. Daher wurden auch Maßnahmen ergriffen, um den Betrieb wiederherzustellen. Es gibt keine Hinweise darauf, dass Daten oder die IT-Infrastruktur anderer Gesellschaften der Hensoldt-Gruppe oder Kunden des Unternehmens von dem Angriff betroffen sind. /HEI22w21, FAZ22w01, CSO22w02, HAN22w02/

Bei dem Ransomware-Angriff kam es zum Zugriff unbefugter Dritter auf bestimmte Systeme von Nexeya. Über den genauen Hergang des Angriffs liegen der GRS keine Informationen vor. Bei dem Angriff wurden Daten in erheblichem Umfang extrahiert und anschließend auf den Systemen von Nexeya verschlüsselt. Informationen zum genauen Umfang der extrahierten Daten sowie zu deren Inhalt liegen der GRS nicht vor. /HEI22w21, FAZ22w01, CSO22w02, HAN22w02/

Bei REvil handelt es sich um eine der finanziell profitabelsten Ransomware- und Ransomware-as-a-Service Gruppierungen weltweilt mit jährlichen Umsätzen im Bereich von 100 Millionen US-Dollar, die seit dem Jahr 2019 agiert. Mutmaßlich handelt es sich um eine aus Russland heraus agierende Gruppierung, die sich nach dem Ende der Aktivitäten der APT-Gruppierung GandCrab und möglicherweise aus Mitgliedern dieser Gruppierung gebildet hat. In der Regel fordert REvil ein Lösegeld für die Entschlüsselung der Daten von Opfern ihrer Cyberangriffe, daher ist die Vorgehensweise von REvil in der Regel rein kriminell und finanziell motiviert. Im vorliegenden Fall gibt es keine Informationen bezüglich einer Lösegeldforderung an Hensoldt oder Nexeya. Daher ist es denkbar, dass der Angriff der mutmaßlich mit Russland in Verbindung stehenden Gruppierung REvil auf den Rüstungskonzern Hensoldt vor dem Hintergrund des Krieges in der Ukraine eine politische Motivation haben könnte. /HEI22w21, FAZ22w01, CSO22w02, HAN22w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.28 Cyberangriff auf Friedrich Vorwerk Gruppe

Übersicht

Am 20.11.2022 kam es zu einem Cyberangriff auf die Friedrich Vorwerk Gruppe, einem deutschen Unternehmen u. a. zum Bau von Gas-Pipelines und damit Betreiber einer kritischen Infrastruktur. Die Friedrich Vorwerk Gruppe baut u. a. Pipelines für die Gasversorgung im Rahmen des Baus von LNG-Terminals. Durch den Cyberangriff kam es zu einem Ausfall weiter Teile der IT-Infrastruktur des Unternehmens. /HEI23w08, EYE23w01/

Beschreibung

Die Friedrich Vorwerk Gruppe wurde Ziel eines Cyberangriffs mit Ransomware, der am 20.11.2022 begann. Unmittelbar nach Bemerken des Angriffs wurden Maßnahmen zu dessen Eindämmung, Untersuchung und Bewertung eingeleitet. Entsprechende Behörden wie Datenschutzbehörde und Strafverfolgungsbehörde wurden hinzugezogen. Durch den Ransomware-Angriff wurden weite Teile der IT-Infrastruktur der Friedrich Vorwerk Gruppe beeinträchtigt. Die Ransomware wirkte sich auf alle File- und Datenbankserver sowie auf einige Arbeitsplatzrechner aus. Nach Informationen der Friedrich Vorwerk Gruppe wirkte sich der Angriff nicht nur auf die IT und die Mitarbeiter, sondern auch auf das Unternehmensergebnis aus. Durch den Angriff wurde die Profitabilität belastet und die Visibilität eingeschränkt. /HEI23w08, EYE23w01/

Bei dem Ransomware-Angriff kam es zum Zugriff unbefugter Dritter auf die IT-Infrastruktur der Friedrich Vorwerk Gruppe. Über den genauen Hergang des Angriffs, der dabei genutzten Schadsoftware oder der für den Angriff verantwortlichen Ransomware-Gruppierung liegen der GRS keine Informationen vor. Aufgrund der Reaktion der IT-Abteilung der Friedrich Vorwerk Gruppe konnte ein Datenabfluss sowie größere Schäden angeblich verhindert werden. Trotz der Begrenzung des Schadens dauerte es etwa vier Wochen, bis die IT-Infrastruktur wieder instandgesetzt war. In dieser Zeit waren weite Teile der IT-Infrastruktur nicht verfügbar. Nach Angaben der Friedrich Vorwerk Gruppe kam es zur Forderung einer Lösegeldzahlung, diese wurde aber verweigert. /HEI23w08, EYE23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.29 Cyberangriff auf Gasnetzbetreiber Desfa (Griechenland)

Übersicht

Am 19.08.2022 kam es zu einem Cyberangriff auf Desfa, einen griechischen Gasnetzbetreiber. Desfa ist die Betreiberfirma des griechischen Erdgasnetzes (Erdgasfernleitungsnetz und Gasverteilung Griechenlands) und dabei verantwortlich für den Betrieb, das Management, die Nutzung sowie die Entwicklung des Erdgassystems und seiner Verbindungsleitungen. Damit ist Desfa ein Betreiber einer kritischen Infrastruktur. Aufgrund des Angriffs wurden vorsorglich die meisten IT-Services deaktiviert, um Kunden von Desfa zu schützen. /HEI22w22, CSO22w03, SEC22w14, SEC22w15/

Beschreibung

Desfa wurde Ziel eines Cyberangriffs mit Ransomware, der der Ransomware-Gruppierung Ragnar Locker zugeschrieben wird. Nach der Entdeckung des Angriffs wurden umgehend Maßnahmen zur Eindämmung eingeleitet, wodurch laut Desfa verhindert werden konnte, dass der Angriff noch größere Auswirkungen hatte. Es wurden diverse IT-Systeme heruntergefahren sowie Untersuchungen zu dem Angriff eingeleitet, wobei auch externe Experten beauftragt und die entsprechenden Behörden eingeschaltet wurden. Außerdem wurden Arbeiten begonnen, um alle Systeme schnellstmöglich wieder verfügbar zu machen. Durch den Cyberangriff kam es zu einem Zugriff auf Teile der IT-Infrastruktur von Desfa, was auch einen Einfluss auf die Verfügbarkeit von Systemen hatte. Laut Desfa war die Gasversorgung aber zu jedem Zeitpunkt gesichert, da auf die dafür relevanten Systeme bei dem Angriff kein Zugriff erfolgte. /BLE22w07, CSO22w03, INS22w01, HEI22w22/

Bei dem Cyberangriff kam es zum Zugriff unbefugter Dritter auf bestimmte IT-Systeme von Desfa, wobei eine Ransomware eingesetzt wurde. Es kam zur Extraktion einer unbekannten Menge an Daten, wobei auch sensible Mitarbeiter- und Kundendaten gestohlen worden sein sollen. Die Ransomware-Gruppierung Ragnar Locker, die sich zu dem An-griff bekannt hat, ist mit einer Lösegeldforderung in unbekannter Höhe an Desfa heran-getreten. Desfa hat allerdings klargestellt, dass ein Lösegeld nicht bezahlt wird.

Darauf-hin hat Ragnar Locker mehr als 360 GB gestohlene Daten veröffentlicht. Der genaue Ablauf des Angriffs von Ragnar Locker auf Desfa ist nicht bekannt. /BLE22w07, CSO22w03, HEI22w22, INS22w01, SEC22w14, SEC22w15/

Ragnar Locker ist eine Ransomware-Gruppierung, die erstmals im Dezember 2019 aufgetreten ist. Es kam weltweit zu Angriffen auf staatliche Infrastrukturen, Dienste, Regierungssysteme und große Unternehmen aus den Bereichen Fertigung, Energie, Finanzdienstleistungen sowie Informationstechnologie. Allein in den USA waren im Jahr 2022 mindestens 52 Unternehmen und Betreiber kritischer Infrastrukturen von einem Angriff durch Ragnar Locker betroffen. Die Vorgehensweise von Ragnar Locker ist dabei identische zu der Vorgehensweise anderer Ransomware-Gruppierungen. Zuerst wird das Opfernetzwerk ausspioniert, dann werden nach Erlangung eines Zugriffs auf das Netzwerk Daten und sensitive Informationen exfiltriert, Daten auf IT-Systemen des Opfernetzwerks verschlüsselt und eine Lösegeldforderung, in der Regel in der Höhe mehrerer Millionen US-Dollar, gestellt. Die Ragnar Locker-Gruppierung nutzt bei ihren Angriffen zur Kompromittierung des Opfernetzwerks oftmals einen Zugriff über das Remote Desktop Protokoll. Dabei werden Brute Force Attacken ausgeführt, um schwache Passwörter zu er-halten oder es wird mit gestohlenen Zugangsdaten gearbeitet. Des Weiteren verwendet Ragnar Locker Techniken, um nach der Kompromittierung eines Netzwerks nicht entdeckt zu werden. Die eingesetzte Ransomware ist in der Programmiersprache C/C++ geschrieben. Die Ransomware beinhaltet Programmcode, der verhindert, dass bestimmte Länder wie beispielsweise Russland angegriffen werden. Außerdem gibt es Hinweise darauf, dass die Gruppierung aus Russland operiert. /SEC22w14, TRE22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.30 Zeppelin-Ransomware

Übersicht

Am 21.06.2022 wurde vom Federal Bureau of Investigation (FBI) und der US-Behörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) festgestellt, dass mehrere große Organisationen in den USA und Europa mit der Zeppelin-Ransomware angegriffen wurden. Dazu haben FBI und CISA Details in einem gemeinsamen Bericht veröffentlicht. /THR22w02, CIS22w01/

Beschreibung

Die Zeppelin-Ransomware ist eine Variante einer Delphi-basierten Ransomware, die ursprünglich als Vega oder VegaLocker bekannt war, Anfang 2019 erstmals auftauchte und als Ransomware as a Service (RaaS) funktioniert. In den Jahren 2019 bis mindestens Juni 2022 wurden mittels dieser Ransomware eine Reihe von Unternehmen und Betreiber kritischer Infrastrukturen in Europa und den USA angegriffen, darunter Unternehmen im Bereich der Verteidigung, Bildungseinrichtungen, Industrieunternehmen, Technologieunternehmen sowie insbesondere Organisationen im Gesundheitswesen und in der Medizin. Details zu den angegriffenen Unternehmen sind nicht bekannt. Bei den Angriffen wurden Lösegeldzahlungen in Form von Bitcoin gefordert, wobei die Höhe der geforderten Zahlungen im Bereich einiger tausend US-Dollar bis zu über einer Million US-Dollar reichten. /THR22w02, CIS22w01/

Bei den Angriffen mit der Zeppelin-Ransomware verschaffen sich die Angreifer den Zugang zu den Opfernetzwerken unter Ausnutzung von Schwachstellen im Remote Desktop Protokoll (RPD), SonicWall-Firewall-Schwachstellen und Phishing-Kampagnen. Nach erfolgreicher Infiltration des Opfernetzwerks verbringen die Akteure ein bis zwei Wochen damit, das Netzwerk des Opfers zu kartieren, um Datenenklaven zu identifizieren, wobei auch Cloud-Speicher und Netzwerk-Backups einbezogen werden. Anschließend wird die Zeppelin-Ransomware als .dll- oder .exe-Datei oder als Bestandteil eines PowerShell-Loaders bereitgestellt. Sobald die Zeppelin-Ransomware in das Opfernetzwerk eingedrungen ist, installiert sie sich in einem temporären Ordner namens -zeppelin und verbreitet sich auf dem infizierten Gerät. Vor der Verschlüsselung von Dateien werden diese exfiltriert, um die gängige Taktik der doppelten Erpressung anzuwenden, bei der die exfiltrierten Dateien verkauft oder veröffentlicht werden, wenn kein Lösegeld gezahlt werden sollte. /THR22w02, CIS22w01/

Sobald die Zeppelin-Ransomware ausgeführt wird, wird an jede verschlüsselte Datei eine zufällig erzeugte, neunstellige Hexadezimalzahl als Dateierweiterung angehängt, z. B. file.txt.txt.C59-E0C-929. Eine Textdatei mit einer Lösegeldforderung wird auf den kompromittierten Systemen hinterlassen, zumeist auf dem Desktop. Die jüngsten Angriffe mit der Zeppelin-Ransomware zeigen, dass auch eine Mehrfachverschlüsselungstaktik angewendet wird, bei der die Malware mehr als einmal in dem Opfernetzwerk ausgeführt wird, wobei für jeden Angriff unterschiedliche IDs und Dateierweiterungen erstellt wurden. Dies bedeutet, dass die Opfer mehrere Schlüssel benötigen, um die Dateien vollständig entschlüsseln zu können. /THR22w02, CIS22w01/

Laut /GOL22w02/ ist es der Cybersicherheitsfirma Unit 221B gelungen, den Schlüssel der Zeppelin-Ransomware zu knacken. Dadurch konnte mehreren Organisationen geholfen werden, ihre Daten zu entschlüsseln. Dazu wurde die Zeppelin-Ransomware analysiert und es wurde festgestellt, dass eine der Komponenten der Verschlüsselung aus einem 512-Bit-RSA-Schlüssel besteht, der auf jedem betroffenen System zufällig generiert wird. Dieser öffentliche Schlüssel war aus der Registry wiederherstellbar, indem eine Live-CD erstellt wurde, mit der auf einem infizierten System ein Linux-Betriebssystem gestartet werden konnte, welches diesen Schlüssel auslesen konnte. Dieser öffentliche Schlüssel kann geknackt werden, womit dann der 256-Bit-AES-Schlüssel erhalten wer-den kann, mit denen die Dateien verschlüsselt sind.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.31 Hive-Ransomware

Übersicht

Am 25.11.2022 wurde vom Federal Bureau of Investigation (FBI), der US-Behörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) und dem US-Department of Health and Human Services (HHS) ein gemeinsamer Bericht veröffentlicht, um vor der Ransomware-Gruppierung Hive zu warnen, die weltweit mehrere Organisationen mit Ransomware angegriffen hat. /CIS22w02/

Beschreibung

Die Ransomware-Gruppierung Hive ist im Juni 2021 erstmals aufgetreten und hat bis November 2022 nach Angaben des FBI weltweit über 1300 Unternehmen angegriffen und dabei rund 100 Millionen US-Dollar an Lösegeldzahlungen erhalten. Der durch die Angriffe entstandene Schaden geht Schätzungen zufolge in die Milliarden. Die Gruppierung Hive bietet ihre Dienste als Ransomware as a Service (RaaS) an, wobei ein Fünftel des erpressten Lösegeldes an die Entwickler der Ransomware und 80 Prozent der Lösegeldeinnahmen an die Angreifer geht. Mittels Hive-Ransomware wurde ein breites Spektrum an Unternehmen in über 80 Ländern angegriffen, darunter Regierungseinrichtungen, Kommunikationseinrichtungen, Produktionsanlagen, Informationstechnologie und insbesondere Einrichtungen im Gesundheits- und Sozialwesen, also auch kritische Infrastrukturen. Bei den Angriffen wurden Lösegeldzahlungen in Form von Bitcoin gefordert, wobei die Höhe der geforderten Zahlungen im Bereich einiger tausend US-Dollar bis zu über einer Million US-Dollar reichten. /CIS22w02, HEI23w09/

Bei den Angriffen mittels Hive-Ransomware wurde der Erstzugriff zum Opfernetzwerk mittels unterschiedlicher Methoden hergestellt, wie z. B. über einfache Logins mittels dem Remote Desktop Protokoll (RDP), Angriffen über VPN oder andere Remote-Netzwerkverbindungsprotokolle, über die Umgehung von Multifaktor-Authentifizierungen unter Ausnutzung einer Schwachstelle zum Zugriff auf FortiOS-Server, über Phishing-E-Mails mit maliziösen Anhängen oder über das Ausnutzen von Sicherheitslücken in Microsoft Exchange Servern. Nach erfolgreicher Infiltration des Opfernetzwerks wurden von der Hive-Ransomware mehrere Prozesse ausgeführt, um einer Entdeckung zu entgehen, wie z. B. die Identifizierung und das Beenden von Prozessen, die mit Backups und Antivirus-Programmen zusammenhängen, das Beenden von Volume Shadow Copy-Diensten und das Entfernen aller vorhandenen Schattenkopien, das Löschen von Windows-Ereignisprotokollen sowie das Entfernen von Virendefinitionen und die Deaktivierung von Windows-Defender und anderen gängigen Antivirenprogrammen. Anschließend werden von der Hive-Ransomware Daten extrahiert, wahrscheinlich mit Hilfe einer Kombination aus Rclone und dem Cloud-Speicherdienst Mega.nz. Nach der Extraktion von Daten erfolgt der Verschlüsselungsvorgang auf dem Opfernetzwerk, wobei im Stammverzeichnis eine Datei namens *.key erstellt wird, die für die Entschlüsselung benötigt wird. Die Lösegeldforderung wird mittels Textdatei in jedem betroffenen Verzeichnis abgelegt. In der Lösegeldforderung wird den Opfern gedroht, die exfiltrierten Daten zu veröffentlichen, wenn das Lösegeld nicht gezahlt werden sollte.

Außerdem ist bekannt, dass die Ransomware-Gruppierung Hive Netzwerke von angegriffenen Organisationen, die ihre Netzwerke ohne die Zahlung von Lösegeld wiederhergestellt haben, erneut angreift. /CIS22w02, HEI23w09/

Am 26.01.2023 konnte die Ransomware-Gruppierung Hive durch eine gemeinsame Aktion von Ermittlungsbehörden diverser Länder ausgeschaltet werden. An der Operation „Dawnbreaker“ waren Ermittlungsbehörden aus Deutschland, USA, Niederlande, Kanada, Frankreich, Irland, Litauen, Norwegen, Portugal, Rumänien, Spanien, Schweden und UK beteiligt. Bei der Operation wurde eine Vielzahl von Servern, Daten und Accounts des Hive-Netzwerks sowie seiner Nutzer sichergestellt. Ausgangspunkt hierfür war ein Angriff auf ein Unternehmen im Raum Esslingen. Im Zuge der Ermittlungen zu diesem Angriff konnte in die IT-Infrastruktur der Ransomware-Gruppierung Hive eingedrungen werden. Laut den Ermittlern hatten US-Behörden bereits seit Juli 2022 Zugang zu dem Netzwerk der Gruppierung Hive, was genutzt wurde, um mehreren von Angriffen betroffenen Unternehmen bei der Entschlüsselung von Daten zu helfen. /HEI23w09, TDR23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.32 Cuba-Ransomware

Übersicht

Am 05.01.2023 wurde vom Federal Bureau of Investigation (FBI) und der US-Behörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) ein gemeinsamer Bericht veröffentlicht, um vor der Ransomware-Gruppierung Cuba zu warnen, die weltweit mehrere Organisationen mit Ransomware angegriffen hat. /CIS23w02/

Beschreibung

Die Ransomware-Gruppierung Cuba wurde erstmals im Dezember 2019 beobachtet, aber erste Berichte des FBI wurden erst im November 2021 veröffentlicht. Bis August 2022 wurden weltweit mehr als 100 Organisationen kompromittiert, wobei über 140 Millionen US-Dollar Lösegeld gefordert und letztendlich über 60 Millionen US-Dollar

Lösegeld gezahlt wurden. Dabei wurden auch Betreiber kritischer Infrastrukturen angegriffen, wie z. B. Unternehmen im Finanzsektor, Regierungseinrichtungen, Unternehmen im Gesundheitswesen, Produktionsanlagen und Informationstechnologie. Trotz des Namens Cuba-Ransomware gibt es keinen Hinweis darauf, dass die Akteure dieser Gruppierung in irgendeiner Weise mit der Republik Kuba in Verbindung stehen. Die Motivation der Gruppierung ist eindeutig finanzieller Natur und es wird die Technik der doppelten Erpressung angewendet (Diebstahl und Verschlüsselung von Daten), um ein Lösegeld zu erpressen. Es gibt Hinweise darauf, dass die Akteure aus Russland stammen, da die Angriffe auf westliche Ziele ausgerichtet sind und die Ransomware sich selbst beendet und löscht, wenn russische Sprache auf dem angegriffenen System erkannt wird. /CIS23w02, HEI22w23, TRE22w02/

Bei den Angriffen mittels Cuba-Ransomware wurde der Erstzugriff zum Opfernetzwerk mittels verschiedener Techniken hergestellt, wie z. B. Ausnutzung bekannter Sicherheitslücken in kommerzieller Software, Phishing-Kampagnen, Kompromittierung von Zugangsdaten oder Nutzung legitimer Tools für das Remote Desktop Protokoll (RDP). Außerdem nutzt die Cuba-Ransomware eine Schwachstelle in Veeam Backup & Replication (VBR) Produkten, um Anmeldedaten aus Konfigurationsdateien zu stehlen. Nach dem Erstzugriff wird die Cuba-Ransomware mittels Hancitor, einem Loader, der dafür bekannt ist, Stealer wie Remote Access Trojaner und andere Arten von Ransomware auszuführen, verteilt. Zur Erweiterung der Berechtigungen auf kompromittierten Systemen und Erlangung eines möglichst weit reichenden Zugangs werden von der Ransom-ware-Gruppierung Cuba bekannte Sicherheitslücken und Schwachstellen ausgenutzt und Tools verwendet, wie z. B. Ausnutzung von Schwachstellen im Windows Common Log File System, Verwendung eines PowerShell-Skriptes zur Identifizierung von Dienst-konten für das zugehörige Active Directory Kerberos Tickets, Verwendung eines Tools namens KerberCache um zwischengespeicherte Kerberos-Tickets zu extrahieren oder Verwendung eines Tools zur Ausnutzung der Schwachstelle ZeroLogon um Domänenverwaltungsrechte zu erlangen. /BLE23w04, CIS23w02, HEI22w23, TRE22w02/

Um einer Entdeckung zu entgehen und Verteidigungsmaßnahmen zu umgehen, werden von der Cuba-Ransomware ebenfalls eine Reihe von Taktiken eingesetzt. Dies sind z. B. die Nutzung eines Droppers, der einen Kernel-Treiber namens ApcHelper.sys in das Dateisystem installiert, um gezielt Sicherheitsprodukte zu beenden, die Verwendung von Komponenten zur Beendigung von Prozessen von Antivirensoftware, die Verwendung

eines KillAV-Tools welches ebenfalls Prozesse von Antivirenprogrammen beendet oder die Ausnutzung einer Schwachstelle im Avast-Treiber, um Dienste zu beenden. Zur Bewegung im Opfernetzwerk werden ebenfalls eine Reihe von Tools, wie z. B. RDP (Remote Desktop Protokoll), SMB (Server Message Block) und PsExec (Tool zum Aus-führen von Prozessen auf anderen Systemen) verwendet. Außerdem wird häufig das Tool Cobeacon verwendet, um die Bewegung innerhalb des Opfernetzwerks zu erleichtern. Durch die Verwendung verschiedener Backdoors wie z. B. NetSupport RAT, Beacon oder Bughatch wird der Zugriff auf das Opfernetzwerk erhalten. Die Ransomware-Gruppierung Cuba verwendet neben einem eigenen Cobalt Strike-Netzwerk zur Kommunikation mit ihrem Command and Control Server auch PROXYTHA zur Kommunikation und zum Herunterladen weiterer Komponenten. Mittels der Cuba-Ransomware können sowohl lokale als auch im Netzwerk freigegebene Daten verschlüsselt werden. Die Verschlüsselung der Daten erfolgt mittels einer Kombination aus dem ChaCha20-Verschlüsselungsalgorithmus und RSA-Verschlüsselung. Die Daten werden mit dem ChaCha20-Algorithmus für symmetrische Verschlüsselung verschlüsselt und die RSA-Verschlüsselung wird verwendet, um den ChaCha20-Schlüssel zu verschlüsseln und somit die Entschlüsselung der verschlüsselten Daten zu verhindern. Nach der Verschlüsselung wird die Datei umbenannt und die Erweiterung .cuba angehängt. /CIS23w02, ELA23w01, HEI22w23, TRE22w02/

Seit dem Frühjahr 2022 wurden Verbindungen zwischen der Ransomware-Gruppierung Cuba und RomRom RAT-Akteuren ausgemacht. RomRom ist ein individuell angepasster Remote Access Trojaner, der als Command and Control Schnittstelle genutzt wird. Außerdem nutzt die Ransomware-Gruppierung Cuba möglicherweise auch Industrial Spy Ransomware. /CIS23w02, HEI22w23,

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.33 Diebstahl von FBI-Daten hochrangiger Verantwortlicher für kritische Infrastrukturen

Übersicht

IT-Angreifer haben sich im InfraGard-Programm des FBIs zum Schutz kritischer Infrastrukturen angemeldet und konnten die Datenbank wichtiger Schlüsselpersonen aus dem Bereich kritischer Infrastrukturen kopieren. Die Datenbank dient dazu die Schlüsselpersonen zu vernetzen. Offenbar betrifft der Datendiebstahl die Informationen von mehreren zehntausend Menschen. Die Angreifer haben die abgegriffenen Daten in einem Darknet-Forum zum Verkauf angeboten. Sie betreffen Trinkwasser- und Energieversorger, Finanzdienstleister, Transportunternehmen, die Rüstungsindustrie, Organisationen des Gesundheitswesens sowie Kernenergieunternehmen.

Beschreibung

Um den Schutz kritischer Infrastrukturen in den USA zu verbessern, hat das FBI im Jahr 1996 das InfraGard-Programm ins Leben gerufen /RHP22w01/. In diesem werden über eine Datenbank Schlüsselpersonen der beteiligten Unternehmen und Organisationen aus dem Bereich der kritischen Infrastrukturen miteinander und mit dem FBI vernetzt. Zu diesen Personen gehören Führungspersonal, Manager, IT-Verantwortliche, Militärangehörige, Beamte von Strafverfolgungsbehörden und Regierungsvertreter /RHP22w01/. Darüber hinaus stellt das Programm Informationen und Schulungen zu Sicherheitsbedrohungen und -risiken bereit, die sowohl die physische Sicherheit als auch die IT-Sicherheit betreffen. Teilnehmer am InfraGard-Programm sind Trinkwasser- und Energieversorger, Finanzdienstleister, Transportunternehmen, die Rüstungsindustrie, Organisationen des Gesundheitswesens sowie Kernenergieunternehmen /RHP22w01/. IT-Angreifern, die sich selbst als „USDoD“ bezeichnen und das Siegel des U.S. Department of Defense verwenden, ist es gelungen sich im InfraGard-Programm anzumelden und die Datenbank mit den Informationen zu mehreren zehntausend Schlüsselpersonen zu kopieren. Die Angreifer bieten die Datenbank seit dem 10.12.2022 im englischsprachigen Darknet-Forum Breached für 50.000-US-Dollar als Verhandlungsbasis zum Verkauf an /CYN22w01/. Der Administrator des Forums ist unter dem Namen „Pompompurin“ einschlägig bekannt. Die Angreifer geben zu, dass die meisten Felder der Datenbank wie Sozialversicherungsnummer und Geburtsdatum leer seien. Zu etwa nur der Hälfte der Konten liege eine E-Mail-Adresse vor. Sie führen dies darauf zurück, dass es sich um die Daten sicherheitssensibilisierter Personen handelt. /HEI22w20, KRS22w01/

Das FBI will zum aktuellen Zeitpunkt keine Auskunft geben und verweist darauf, dass der Vorfall noch nicht abgeschlossen sei. Dem gegenüber waren die IT-Angreifer bereit ausführlich über ihr Vorgehen zu berichten. Sie gaben an, dass sie Zugriff zum InfraGard-Programm erhalten haben, indem sie sich im November 2022 für ein neues Konto beworben hatten. Dazu hatten sie zuvor einen Identitätsdiebstahl begangen und die personenbezogenen Daten wie Sozialversicherungsnummer, Geburtsdatum und andere Informationen des Geschäftsführers eines hochrangigen US-Finanzunternehmens abgegriffen, das direkten Einfluss auf die Kreditwürdigkeit der meisten US-Amerikaner hat. Die Angreifer gingen davon aus, dass der Geschäftsführer des Unternehmens mit hoher Wahrscheinlichkeit eine InfraGard-Mitgliedschaft erhalten würde. Bei der Bewerbung gaben die Angreifer die Mobiltelefonnummer des Geschäftsführers an sowie eine eigene E-Mail-Adresse. Über die bald darauf Anfang Dezember 2022 erhaltene Zugangsbestätigung wurden sie zur Einrichtung einer Mehr-Faktor-Authentifizierung aufgefordert, wobei diese über die Angabe einer Mobiltelefonnummer oder E-Mail-Adresse erfolgen konnte. Bei Angabe der Mobiltelefonnummer wird an diese eine SMS mit einem einmal-gültigen Freischaltcode gesendet. Andernfalls wird der Freischaltcode an die angegebene E-Mail-Adresse gesendet. Die Angreifer verwendeten die bei ihrer Bewerbung angegebene E-Mail-Adresse zur Freischaltung. Wäre eine Registrierung nur über die Mobiltelefonnummer möglich gewesen, hätten sich die Angreifer nicht anmelden können, da sie dafür zusätzlich Zugriff auf das Mobiltelefon des Geschäftsführers benötigt hätten. Zudem wäre der Identitätsdiebstahl aufgefallen. Der Geschäftsführer gab an, dass er vom FBI nicht kontaktiert wurde. Das bedeutet, dass seitens des FBIs kein Versuch unternommen wurde die Identität des Bewerbers zu überprüfen. /HEI22w20, KRS22w01/

Nach der erfolgreichen Anmeldung hatten die Angreifer ungehinderten Zugang auf die Daten von InfraGard. Bei dem InfraGard-Programm handelt es sich um ein soziales Netzwerk inklusive eines Diskussionsforums. Eine Programmierschnittstelle (Application Programming Interface API) verbindet die einzelnen Komponenten des Systems und erlaubt ungeschützten Zugriff auf die Benutzerdaten. Um diese abzurufen, nutzten die Angreifer ein von ihnen programmiertes Python-Skript, das die einzelnen Konten der Datenbank automatisch abarbeitete. Dieses Vorgehen wird als „Scraping“ bezeichnet. Die Angreifer konnten die Echtheit der gestohlenen Daten beweisen, in dem sie diese nutzten, um einen Geschäftsführer eines anderen Unternehmens zu kontaktieren, welcher die Kontaktaufnahme bestätigte. /HEI22w20, KRS22w01/

Kerntechnischer Bezug

Von dem Diebstahl personenbezogener Daten aus der InfraGard-Datenbank sind auch Schlüsselpersonen aus dem Energiesektor und von Kernenergieunternehmen der USA betroffen. Wenn es den IT-Angreifern gelingen sollte die Daten im Darknet zu verkaufen, dann könnten die darin enthaltenen Informationen bei zukünftigen Cyberangriffen eingesetzt werden.

B.14.34 Informationsdiebstahl im DIB-Sektor

Übersicht

Es sind APT-Aktivitäten im Zusammenhang mit dem DIB-Sektor (Defense Industrial Base Sector) bekannt geworden, bei denen unter anderem die frei verfügbaren Python-Klassen Impacket zum Einsatz kamen, die den Zugriff auf Netzwerkpakete ermöglichen. Es erfolgte eine Exfiltration von Daten mithilfe der Schadsoftware CovalentStealer.

Beschreibung

Am 04.10.2022 veröffentlichten die U.S. Cybersecurity and Infrastructure Agency (CISA), das Federal Bureau of Investigation (FBI) und die National Security Agency (NSA) einen gemeinsamen Bericht /CFN22i01/ über die Kompromittierung einer U.S.-Organisation im Bereich des DIB-Sektors durch staatlich gesponserte IT-Angreifer. Beim Defense Industrial Base Sector (kurz DIB-Sektor) handelt es sich um einen weltweiten industriellen Komplex, der die Forschung und Entwicklung von militärischen Waffensystemen, Subsystemen und Komponenten oder Teilen ermöglicht. Die Angreifer nutzten die Schadsoftware CovalentStealer und die frei verfügbaren Python-Klassen Impacket, um sensible Daten zu stehlen. Impacket ist eine Sammlung von Python-Klassen, die die Arbeit mit Netzwerkprotokollen und den Zugriff auf Netzwerkpakete ermöglicht /FOR23w02/. Der Angriff erstreckte sich über einen Zeitraum von zehn Monaten und es wird vermutet, dass mehrere APT-Gruppierungen daran beteiligt waren. Einige dieser Gruppierungen scheinen sich bereits im Januar 2021 initialen Zugriff auf das IT-Netzwerk der Organisation über deren Microsoft Exchange Server verschafft zu haben. Später nutzten sie Schwachstellen in Microsoft Exchange aus, die unter dem Namen ProxyLogon (siehe Abschnitt A.4.1) bekannt sind, um den Netzwerkzugriff auszuweiten.

Die Ausnutzung der Schwachstellen erfolgte etwa zur gleichen Zeit, als Microsoft ein Sicherheitsupdate zur Schließung der Schwachstellen veröffentlichte. In ihrem gemeinsamen Bericht /CFN22i01/ gehen die CISA, das FBI und die NSA auf die technischen Details des Angriffs ein, die zwischen November 2021 und Januar 2022 gesammelt wurden. Von den Angreifern wurden bei ihrem Vorgehen die Schadsoftware CovalentStealer, die frei verfügbaren Python-Klassen Impacket, der Remote Access Trojaner (RAT) HyperBro (siehe Abschnitt B.14.21) und über ein Duzend China Chopper Web Shell-Varianten (siehe Abschnitt B.11.4) kombiniert. /BLC22w01, CFN22i01, SEB22w01/

Innerhalb von vier Stunden nachdem sich die Angreifer initialen Zugriff auf den Microsoft Exchange Server der Organisation verschafft hatten, führten sie eine Mailbox-Suche durch und sie nutzten das Administratorkonto eines früheren Angestellten, um Zugang zur Exchange Web Service (EWS) API zu erhalten. Diese Schnittstelle wird zum Senden und Empfangen von Webservice-Nachrichten verwendet. Im frühen Februar 2021 verschafften sich die Angreifer erneut Zugriff auf das IT-Netzwerk, indem sie die Zugangsdaten des gleichen Administratorkontos nutzten, um eine VPN-Verbindung herzustellen. Vier Tage später durchsuchten sie das Netzwerk mithilfe einer Command-Shell. Auf diese Weise kundschafteten sie das Netzwerk aus und es gelang ihnen manuell sensible Daten zu archivieren und für die Exfiltration vorzubereiten. Zu diesen Daten gehören z. B. Vertragsinformationen. /BLC22w01, SEB22w01/

Anfang März 2021 nutzten die Angreifer die ProxyLogon-Schwachstellen in Microsoft Exchange aus, um 17 Varianten der China Chopper Web Shell auf dem Microsoft Exchange Server der Organisation zu installieren. Ein Bericht des IT-Sicherheitsunternehmens FireEye /FIR14r02/ behandelt die technischen Eigenschaften und die Funktionalitäten der Web Shell China Chopper. Darin wird beschrieben, dass die Web Shell nur einen Speicherplatz von vier Kilobyte benötigt und Möglichkeiten zur Datei- und Datenbankverwaltung sowie zur Programmcode-Verschleierung bereitstellt. Darüber hinaus können mit der Web Shell Passwörter nach dem Brute-Force-Verfahren erraten werden. Im April 2021 richteten die Angreifer eine persistente Verbindung zum Netzwerk ein. Die Python-Klassen Impacket ermöglichten ihnen dann die laterale Bewegung innerhalb des Netzwerks, da in den Klassen die Arbeit mit Netzwerkprotokollen realisiert ist. Zusätzlich nutzten die Angreifer die Impacket-Klassen in Verbindung mit den bereits erwähnten Zugangsdaten des kompromittierten Administratorkontos, um ein Servicekonto mit höheren Privilegien im Microsoft Exchange Server einzurichten.

Dieses Konto ermöglichte dann über Outlook Web Access (OWA) den Fernzugriff über mehrere externe IP-Adressen auf den Exchange Server. /BLC22w01, FIR14r02, SEB22w01/

Zwischen dem späten Juni und Mitte Oktober 2022 verwendeten die Angreifer ihren erweiterten Netzwerkzugriff, um mit der Schadsoftware CovalentStealer zusätzlich sensible Daten zu stehlen und auf Microsoft OneDrive hochzuladen. In einem weiteren Bericht der CISA /CIS22i06/ werden die technischen Details der Schadsoftware CovalentStealer beschrieben. Die Schadsoftware basiert auf zwei frei verfügbaren Softwarewerkzeugen ClientUploader und dem PowerShell-Skript Export-MFT, welche das Hochladen komprimierter Dateien und die Extrahierung der Master File Table (MFT) eines Speicherlaufwerks ermöglichen. Darüber hinaus enthält die Schadsoftware CovalentStealer Möglichkeiten der Verschlüsselung und Entschlüsselung von Dateien, Möglichkeiten zur Absicherung der Kommunikation mit den Angreifern sowie Konfigurationsdateien. /BLC22w01, CIS22i06, SEB22w01/

Die CISA veröffentlichte auch Informationen zum RAT HyperBro /CIS22i07/. Dieser ermöglicht das Hochladen und Herunterladen von Dateien auf und von einem System, das Aufzeichnen von Tastatureingaben (Keylogging), die Ausführung von Befehlen und die Umgehung des Schutzes der Benutzerkontensteuerung. Letzteres bietet vollumfängliche Administrator-Privilegien. /BLC22w01, CIS22i07, SEB22w01/

Der gemeinsame Bericht der CISA, des FBI und der NSA /CFN22i01/ gibt YARA-Regeln an, mit denen sich Aktivitäten der Angreifer detektieren lassen. Zusätzlich enthält der Bericht Indicators of Compromise (IoC) bezüglich der Schadsoftware-Werkzeuge CovalentStealer, HyperBro und China Chopper. Darüber hinaus gibt der Bericht allgemeine Maßnahmen an, mit deren Hilfe sich die Wahrscheinlichkeit einer Kompromittierung durch die Angreifer minimieren lässt. Die beschriebenen Maßnahmen sind: Einrichtung einer Multi-Faktor-Authentifizierung (MFA) für alle Benutzerkonten, Umsetzung einer Netzwerksegmentierung in Abhängigkeit von Aufgaben und Funktionalität, Software- und Firmwareupdates, um mögliche Schwachstellen zu schließen, sowie die Durchführung von Audits bezüglich der Nutzung von Benutzerkonten. /BLC22w01, CFN22i01, SEB22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.35 Spionageangriffe durch ATP Lazarus unter Nutzung von Log4Shell

Übersicht

Ab Februar 2022 kam es unter Ausnutzung der Schwachstelle Log4Shell zu Cyberangriffen durch APT 38 Lazarus auf Energieunternehmen in den USA, Kanada und Japan. Durch die Log4Shell Schwachstelle in der Software VMWare Horizon erlangten die Angreifer Zugriff auf die Daten und Netzwerke der betroffenen Energieunternehmen und nutzten drei unterschiedliche Schadsoftwaren für den Aufbau eines langfristigen Zugriffs und das Auslesen von Zugangsdaten und weiteren für die Angreifer relevanten Datensätzen. Der Angriff wurde erstmalig im April 2022 erkannt und im September 2022 noch einmal ausführlich ausgewertet. /CSD22w01, CIS22r06/

Beschreibung

Lazarus ist eine bereits seit 2009 aktive APT-Gruppierung mit nordkoreanischem Hintergrund und einem umfassenden Tätigkeitsprofil. Energieunternehmen, wobei mit dem indischen Kernkraftwerk Kudankulam auch kerntechnische Anlagen zu den Zielen der Gruppierung gehören. Im Jahr 2022 nutzte die Gruppierung die kritische Schwachstelle Log4Shell in der VMWare Horizon Software um Energieunternehmen in den USA, Kanada und Japan anzugreifen. /CSD22w01, CIS22r06, SYM22r01/

Log4Shell ist eine kritische Schwachstelle, welche im Dezember 2021 in der umfassend genutzten Java Bibliothek Log4j entdeckt wurde und welche durch seit Januar 2022 verfügbare Updates auf aktualisierten IT-Systemen nicht mehr ausgenutzt werden kann. Da jedoch zum einen für jede Log4j nutzende Software individuelle Updates durch die Hersteller veröffentlicht werden müssen und zum anderen nicht jeder Betreiber von Log4j nutzender Software sofort entsprechende Updates auf seine Systeme aufspielt, waren im Februar 2022 weiterhin eine Vielzahl von betroffenen IT-Systemen verbreitet und sind es auch noch im Jahr 2023. /SYM22r01/

Die Cyberangriffe erfolgten immer über die bestehende Log4Shell Schwachstelle der VMWare Horizon Software auf mit dem Internet kommunizierenden Server. Die Schwachstelle benötigt weder eine Authentifizierung noch anderweitige aufwendigere Maßnahmen zur Ausnutzung, sodass die Angreifer direkten vollen Systemzugriff auf den betroffenen Server erlangen konnten.

Durch Nutzung der in VMWare Horizon vorliegenden ausführbaren Datei Node.exe erlangten die Angreifer den Zugriff auf eine Shell zur Ausführung beliebigen Codes. Anschließend erfolgte die Nutzung von Befehlen zur Netzwerkerkennung wie ipconfig/all und die Deaktivierung von möglicher Antivirensoftware wie Windows Defender. All diese Schritte konnten ohne eigentliche Schadsoftware erfolgen. /CSD22w01, CIS22r06/

Erst anschließend wurde die Schadsoftware durch die Angreifer auf das betroffene IT-System aufgespielt, wobei je nach Angriffsziel eine der drei Schadsoftwaren „VSingle“, „Yamabot“ oder „MagicRAT“ zum Einsatz kamen. Die Schadsoftwaren werden zuerst genutzt, um weitere Aufklärung über das Netzwerk und das betroffene IT-System zu betreiben und anschließend, um einen langfristig nutzbaren direkten Systemzugriff auf Administratorlevel zu erlangen, welcher auch nach Entfernung der Schadsoftware bestehen bleiben sollte. Neben diesem Administratorzugriff wurden auch auf Basis der Schadsoftware weitere langfristige Zugriffsmöglichkeiten für den Angreifer etabliert. Darüber hinaus ermöglicht die Schadsoftware das Nachladen von weiterem Schadcode über den Command and Controll (C2) Server der Angreifer. Zu den nachgeladenen Schadsoftwaren gehören bereits bekannte Schadsoftwaren wie MIMIKATZ und SOCKS PROXY, das langfristig Ziel erschien insbesondere das Auslesen von Zugriffsdaten, die Etablierung innerhalb des Netzwerks der angegriffenen Unternehmen und der allgemeine Abfluss von Daten gewesen zu sein. /CSD22w01, CIS22r06/

Es ist bislang nicht bekannt, welche Unternehmen des Energiesektor genau betroffen waren.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Da nicht benannte Unternehmen des Energiesektors betroffen waren, ist ein kerntechnischer Bezug nicht auszuschließen.

Weitere Bearbeitung

Die GRS verfolgt fortwährend die Aktivitäten der APT-Gruppierung Lazarus, da es sich bei dieser Gruppierung um eine der profiliertesten und aktivsten APT-Gruppierungen handelt und diese Gruppierung mindestens einmalig einen erfolgreichen Cyberangriff auf eine kerntechnische Anlage durchführte. Die Ergebnisse dieser Beobachtung fließen in die allgemeine Auswertung der Bedrohungslage ein, bei besonderen Ereignissen

werden die Handlungen der APT Lazarus gesondert von der GRS im Rahmen bestehender vorhaben ausgewertet.

B.14.36 Social-Engineering Angriffe durch iranische APT-Gruppierungen

Übersicht

Verschiedene Gruppierungen, welche der islamischen Republik Iran als zugehörig angesehen werden, verüben seit mehr als einem Jahrzehnt umfangreiche Cyberangriffe in einem weiten Umfeld aus politischen und ökonomischen Beweggründen. Zu den hierbei angewandten Vorgehensweisen gehören auch immer wieder umfassende und aufwendige Social Engineering Kampagnen, bei welchen die Opfer durch die Vorspiegelung falscher Tatsachen und das Ausnutzen menschlicher Verhaltensweisen zur Preisgabe von Zugangsrechten, Passwörtern und anderen wertvollen Details bewegt werden.

Beschreibung

2022 wurde in einer umfassenden Cyber Threat Analysis /INS22r01/ der Insikt Group die seit mehr als 10 Jahren bekannte Vorgehensweise verschiedener APT-Gruppierungen (APT 34, APT 35, Toroiseshell) aufgezeigt. Seit dem Jahr 2010 wurden von den islamischen Revolutionsgarden (IRGC) des Irans die Rolle des „Soft Wars“ und der Nutzung von psychologischen Operationen („PSYOPS“) zur Stärkung des eigenen Regimes und Schwächung wahrgenommener Feinde offiziell festgeschrieben. Im Verlauf der Entwicklung des Iranischen Cyberprogramms, zu welchem die genannten APT Gruppierungen sowie weitere Gruppierungen zählen, wurden daher verstärkt auf Social Engineering Maßnahmen gesetzt. Diese Angriffsmethoden beschreiben die Simulation bzw. Darstellung sozialer Interaktionen zur Manipulation der Angriffsziele und dienen schlussendlich dazu, dass die Angegriffen Handlungen im Sinne der Angreifer ausführen. Basis solcher Social Engineering Angriffe sind zumeist glaubwürdige Persönlichkeitsdarstellungen in den sozialen Medien. Mittels öffentlicher Fotos werden Profile in typischen sozialen Netzwerken wie Facebook, Twitter (jetzt X) oder auf Berufsvernetzungsplattformen wie LinkedIn erstellt, welche glaubwürdige Personen in für die Angreifer interessanten Sparten wie Nachrichten, Verteidigung, IT oder Finanzen darstellen sollen. Diese gefälschten Persönlichkeiten bauen anschließend Netzwerke auf um glaubwürdiger zu werden, zum Teil wieder mit gefälschten Profilen, um zum Teil über Jahre eine Glaubwürdigkeit zu entwickeln, die es ihnen erlaubt, mit ihren Zielen Kontakt

aufzunehmen, ohne als gefälschte Persönlichkeiten wahrgenommen zu werden. Anschließend werden z. B. Karrierechancen, romantische Avancen, gleiche Interessen oder ähnliche politische Ansichten genutzt, um in einen Austausch zu gelangen. Im Rahmen eines solchen Austausches werden dann unterschiedliche Ziele versucht zu erreichen:

- Diebstahl von Zugangsdaten, direkt durch Nutzung von Phishing durch Imitation populärer Webseiten
- Informationsgewinn für die weitere Nutzung, z. B. in Form von gefälschten Bewerbungsanträgen oder in allgemeinen Gesprächen
- Direkte Verteilung von Malware über Webseiten (drive by) und direkt getauschte Dateien wie MS-Word mit Macros.
- Langfristige Erzeugung von Verteilung von Falschnachrichten und Manipulation der Öffentlichkeit

Diese Arten von Social Engineering Kampagnen wurden in den letzten Jahren wiederholt aufgedeckt. So wurde eine Kampagne 2021 der Gruppierung PHOSPHORUS (auch bekannt als Mint Sandstorm) aufgedeckt, die über verschiedene Phasen erst „Small talk“ Unterhaltungen mit ihren Opfern führten, dann tiefergehende Diskussionen führten und anschließend gefälschte Einladungen zu Bewerbungsgesprächen, welche für die Übertragung von Schadsoftware genutzt wurden. Ziel der Kampagne waren unter anderem iranische Dissidenten. Ähnliche Kampagnen wurden 2020 und 2021 gegen Forscher verschiedener Universitäten, israelische Mediziner, Vertragsarbeiter des U.S. amerikanischen Verteidigungsministeriums, Journalisten und weiterer Gruppierungen. Weitere Kampagnen unter Nutzung verschiedener Googlefunktionen und Whatsapp wurden im Jahr 2022 berichtet und richteten sich gegen Gruppierungen wie Human Rights Watch und Amnesty International. Die Angriffe wurden der APT 42 zugeordnet. /INS22r01, MIC21w17, HRW22w01/

Social Engineering Angriffe im Kontext der Interessen der islamischen Republik Iran werden fortwährend geführt und dabei entsprechend der Zielsetzung angepasst. Neben Angriffen auf Menschenrechtsaktivisten, Dissidenten und militärische Gegenspieler, werden auch solche im wirtschaftlichen Kontext ins Ziel genommen, aus den Bereichen Finanzen, Medizin, Forschung und Entwicklung sowie IT.

Kerntechnischer Bezug

Die islamische Republik Iran führt ein eigenes ziviles nukleares Programm durch, bei welchem es Hinweise auf dessen militärische Bezuge sowie ein direktes militärisches Nuklearprogramm durch die IRGC gibt. Daher sind auch grundsätzlich Personen im nuklearen Kontext für die entsprechenden Kampagnen interessant. Als direkter Bezug wurde bisher bekannt, dass im Rahmen einer Social Engineering Kampagne iranischer Gruppierungen ein Report über die nuklearen Kapazitäten des Staates Israels als Aufmachung für die Kontaktanbahnung genutzt wurde.

Weitere Bearbeitung

Die GRS verfolgt fortwährend die Aktivitäten iranischer Gruppierungen im Rahmen ihrer kontinuierlichen Auswertung der Bedrohungslage für kerntechnische Anlagen und Einrichtungen in Deutschland.

B.15 2023

B.15.1 Cyberangriff auf ABB

Übersicht

Am 07.05.2023 wurde festgestellt, dass es zu einem Cyberangriff auf Asea Brown Boveri (ABB), einem international operierenden Unternehmen der Energie- und Automatisierungstechnik mit Hauptsitz in der Schweiz, gekommen ist.

ABB entwickelt u. a. industrielle Steuerungssysteme und SCADA-Systeme für Industrie- und Energieversorgungsunternehmen, zu den Kunden von ABB zählen somit auch Betreiber kritischer Infrastrukturen. Aufgrund des Angriffs wurden vorsorglich diverse IT-Systeme abgeschaltet und VPN-Verbindungen zu Kunden beendet, um eine weitere Ausbreitung zu verhindern. /BSI23l01, BLE23w01/

Beschreibung

ABB wurde Ziel eines Cyberangriffs mit Ransomware, welcher der Ransomware-Gruppierung Black Basta zugeschrieben wird.

Nach Entdeckung des Angriffs wurden umgehend Maßnahmen zur Eindämmung und Bewertung eingeleitet, wobei diverse IT-Systeme heruntergefahren und die Verbindungen zu Kunden getrennt wurden. Des Weiteren wurden Untersuchungen zu dem Angriff eingeleitet, wobei auch externe Experten beauftragt sowie -die Strafverfolgungs- und Datenschutzbehörden informiert wurden. Durch den Cyberangriff kam es zu einer Beeinträchtigung des Geschäftsbetriebs, wobei aber alle wichtigen Dienste und Systeme in Betrieb blieben und Kunden weiterhin bedient wurden. Allerdings waren Verzögerungen bei der Projektabwicklung sowie Störungen im Tagesgeschäft und in Produktionsprozessen die Folge. Diese blieben jedoch in Betrieb. Es gibt keine Hinweise darauf, dass Kunden von ABB direkt beeinträchtigt wurden. /BSI23l01, ABB23w01, BLE23w01, SCM23w01/

Trotz der sofort eingeleiteten Maßnahmen zur Eingrenzung der Auswirkungen und Wiederherstellung der Systeme, wurde laut /ABB23w01/ am 23.05.2023, also gut zwei Wochen nach dem Angriff, noch an der Wiederherstellung betroffener Dienste und Systeme gearbeitet.

Bei dem Cyberangriff kam es zum Zugriff unbefugter Dritter auf bestimmte Systeme von ABB, wobei eine Ransomware eingesetzt wurde, die sich nicht selbst verbreitet und bestimmte Daten exfiltriert. Es handelte sich um eine menschlich gesteuerte Ransomware, die das Eingreifen von Personen erfordert, um auf Zielsysteme übertragen zu werden. Eine Verbreitung über E-Mail-Adressen oder Anhänge fand nicht statt und es gab keine automatische Ausbreitung auf andere Systeme in dem Netzwerk. Das Eindringen in das Netzwerk von ABB gelang über bösartige Weblink-Techniken wie SEO-Poisioning und gefälschte Browser-Updates. Nach Erreichen des Erstzugriffs wurde der Trojaner Qakbot installiert. Der Angriff betraf den Windows Active-Directory-Dienst von ABB und hat Hunderte von Geräten in Mitleidenschaft gezogen. Über den Active-Directory-Dienst werden die Netzwerkstrukturen gegliedert und die Zugänge zu den Ressourcen administriert. Welche Daten bei dem Vorfall exfiltriert worden sind und wie hoch eine mögliche Lösegeldforderung war, ist aus den der GRS vorliegenden Unterlagen nicht bekannt. Es gibt aber Hinweise darauf, dass von ABB ein Lösegeld zur Eindämmung des Vorfalls gezahlt wurde und dass die exfiltrierten Daten nicht veröffentlicht wurden. Hierzu liegt kein Kommentar seitens ABB vor. /ABB23w01, BLE23w01, HEI23w06, SCM23w01/

Black Basta ist eine Ransomware-Gruppierung, die seit April 2022 bekannt ist. Es kam weltweit zu Angriffen von Black Basta auf Unternehmen aus diversen Branchen, wie beispielsweise Fertigungsindustrie, Baugewerbe, Transportwesen, Telekommunikationsunternehmen, pharmazeutische Industrie, Autohändler oder Unternehmen der Energietechnik. Black Basta nutzt dabei die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie, wobei die Daten vor deren Verschlüsselung extrahiert werden. Wird kein Lösegeld für das Entschlüsseln der Daten gezahlt, werden diese nicht entschlüsselt und außerdem veröffentlicht. Die Lösegeldforderungen variieren von Opfer zu Opfer, liegen aber in der Regel im Bereich einiger Millionen US-Dollar. Es gibt Hinweise, die darauf hindeuten, dass es sich bei Black Basta um eine russische Gruppierung handelt. /BSI22r07, HAC22w02, SEC22w03/

Kerntechnischer Bezug

ABB ist Hersteller industrieller Steuerungssysteme, die auch in nationalen und internationalen kerntechnischen Anlagen eingesetzt werden. Die Einsatzgebiete variieren dabei von rein betrieblichen Systemen bis hin zu Systemen mit sicherheitstechnischer Relevanz. Bei dem vorliegenden Cyberangriff sind keine Auswirkungen auf Kunden von ABB bekannt geworden. Daher liegen bislang keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.2 Cyberangriff auf Rheinmetall

Übersicht

Am 14. April 2023 wurde entdeckt, dass es zu einem Cyberangriff auf Rheinmetall, einem international agierenden Konzern, der seinen Hauptsitz in Deutschland hat, gekommen ist. Rheinmetall ist ein Hersteller von Automobilen, Militärfahrzeugen, Rüstungsgütern, Luftverteidigungssystemen, Motoren und verschiedenen Stahlprodukten und Deutsch-lands größter Rüstungskonzern. Laut eigenen Angaben ist Rheinmetall in der westlichen Welt einer der drei größten Hersteller von Militärfahrzeugen und im Munitionsgeschäft und betreibt somit kritische Infrastrukturen. Von dem Angriff waren ausschließlich Tochtergesellschaften von Rheinmetall im privaten Sektor betroffen, die sich auf Industrie-kunden, vor allem aus der Automobilbranche, konzentrieren. Dort kam es Ausfall diverser Systeme und Einschränkungen im Geschäftsbetrieb. /BLE23w02, MAL23w01, MIN23w01, SEC23w02/

Beschreibung

Rheinmetall wurde Ziel eines Cyberangriffs mit Ransomware, zu dem sich am 20.05.2023 die Ransomware-Gruppierung Black Basta bekannt hat. Nach Entdeckung des Angriffs wurden umgehend Maßnahmen zu dessen Eindämmung eingeleitet. Außerdem wurden die zuständigen Behörden informiert und es wurde Strafanzeige erstattet. /MAL23w01, SEC23w02, BLE23w02/

Laut Rheinmetall waren von dem Ransomware-Angriff ausschließlich im zivilen Sektor arbeitende Tochtergesellschaften von Rheinmetall betroffen, bei denen IT-Systeme kompromittiert wurden. Das militärische Geschäft war laut Rheinmetall aufgrund einer strikt getrennten IT-Infrastruktur nicht beeinträchtigt. Die zivile Sparte von Rheinmetall produziert vor allem für Industriekunden und den Automobilsektor. Weltweit waren mehrere Tochterunternehmen betroffen, in Deutschland die Firma Kolbenschmidt in Neckarsulm, wo diverse Systeme ausgefallen waren, und die Firma Pierburg in Neuss, bei welcher der Geschäftsbetrieb vorübergehend eingestellt werden musste. Da die Gruppierung Black Basta in der Regel finanziell motiviert agiert, wird davon ausgegangen, dass es sich bei dem Angriff nicht um einen politisch motovierten Angriff auf die Rüstungsindustrie handelt. /MAL23w01, BLE23w02, MIN23w01/

Bei dem Cyberangriff kam es zur Extrahierung von Daten, wobei nicht bekannt ist, wie genau diese Daten aussehen und in welchem Umfang Daten extrahiert wurden. Am 20.05.2023 wurden Rheinmetall und Beispiele der gestohlenen Daten auf der Leak-Webseite von Black Basta gelistet. Bei den veröffentlichten Daten handelte es sich z. B. um Geheimhaltungsvereinbarungen, Vertraulichkeitserklärungen, technische Schemata, Ausweiskopien, Kaufaufträge und anderen Unternehmensdokumente. Die Veröffentlichung der Daten deutet darauf hin, dass Verhandlungen hinsichtlich einer möglichen Lösegeldzahlung gescheitert sind und Rheinmetall kein Lösegeld zahlen will. Es ist allerdings nicht bekannt, ob und in welcher Höhe Lösegeld gefordert wurde. /SEC23w02, BLE23w02/

Black Basta ist eine Ransomware-Gruppierung, die seit April 2022 bekannt ist. Es kam weltweit zu Angriffen von Black Basta auf Unternehmen aus diversen Branchen, wie beispielsweise Fertigungsindustrie, Baugewerbe, Transportwesen, Telekommunikationsunternehmen, pharmazeutische Industrie, Autohändler oder Unternehmen der Energietechnik. Black Basta nutzt dabei die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie, wobei die Daten vor deren

Verschlüsselung extrahiert werden. Wird kein Lösegeld für das Entschlüsseln der Daten gezahlt, werden diese nicht entschlüsselt und außerdem veröffentlicht. Die Lösegeldforderungen variieren von Opfer zu Opfer, liegen aber in der Regel im Bereich einiger Millionen US-Dollar. Es gibt Hinweise, die darauf hindeuten, dass es sich bei Black Basta um eine russische Gruppierung handelt. /BSI22r07, HAC22w02, SEC22w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.3 Cyberangriff auf Cloud Nordic

Übersicht

Am 18. August 2023 wurde entdeckt, dass es zu einem Cyberangriff auf CloudNordic und AzeroCloud, dänischen Cloud- und Hosting-Anbietern, gekommen ist. CloudNordic und AzeroCloud gehören zu demselben Unternehmen und sind führende skandinavische Anbieter von Cloud-Diensten (Bereitstellung externer Datenspeicher) sowie Hosting-Diensten (Bereitstellung und Betrieb von Webservern und deren Netzwerkanbindung sowie Bereitstellung von E-Mail-Diensten). Durch den Angriff kam es zur Abschaltung aller Systeme von CloudNordic und AzeroCloud. /BSI23r02, BLE23w03, CLO23w01, HEI23w07/

Beschreibung

CloudNordic und AzeroCloud wurden Ziel eines Angriffs mit Ransomware, der am 18.08.2023 entdeckt wurde. Durch welche Gruppierung der Angriff durchgeführt wurde, konnte anhand der der GRS vorliegenden Informationen nicht ermittelt werden. Nach dem Angriff wurden Untersuchungen zu dem Angriff eingeleitet, wobei auch externe Experten beauftragt wurden und die Strafverfolgungsbehörden eingeschaltet wurden. Durch den Cyberangriff kam es zur Verschlüsselung aller Kundendaten und zur Abschaltung aller Systeme (Webseiten, E-Mail-Systeme, Kundensysteme, Webseiten der Kunden, usw.). Somit gingen durch den Angriff alle Daten, Systeme, Server sowie die Kommunikation verloren. Zur Extrahierung von Daten kam es laut CloudNordic nicht. /BSI23r02, BLE23w03, CLO23w01, HEI23w07/

Der Ransomware-Angriff fand während der Migration von Servern in ein neues Rechenzentrum statt. Dabei wurden zuvor in getrennten Netzen aktive Server mit dem internen Netzwerk des Unternehmens verbunden, über welches alle Server des Unternehmens verwaltet werden. Einige dieser zuvor getrennten Server waren mit Ransomware infiziert, die trotz installierter Firewalls und Antivirenprogramme nicht detektiert wurde. Somit nutzten die Angreifer die laufende Umstellung auf ein neues Rechenzentrum und eine bereits bestehende, aber ruhende Infektion der Server. Die Verbindung der bereits infizierten Server mit dem internen Netzwerk schaffte für die Angreifer die Möglichkeit, auf die zentralen Verwaltungssysteme und die Backup-Systeme zuzugreifen. Dadurch konnten bei dem Angriff alle Serverfestplatten einschließlich Backups verschlüsselt werden. Da die Angreifer aber keinen Zugriff auf den Dateninhalt selbst hatten, geht CloudNordic davon aus, dass keine Daten extrahiert wurden. Von dem Angriff sind alle Datenspeicher, Steuer- und Sicherungssysteme, Replikations-Backup-Systeme und sekundäre Sicherungssysteme betroffen. Es kam somit durch den Angriff zu einer Verschlüsselung sowohl aller Server-Laufwerke als auch der primären und sekundären Backup-Systeme, wodurch alle Rechner abstürzten und der Zugriff auf die Daten verloren ging. /BSI23r02, BLE23w03, CLO23w01, HEI23w07/

Trotz des Hinzuziehens externer Berater nach dem Angriff hat es sich als unmöglich erwiesen, die Daten wiederherzustellen. Einer Lösegeldforderung in unbekannter Höhe will und kann CloudNordic laut eigenen Angaben nicht nachkommen. Daher sind alle Kundendaten unwiederbringlich verloren. Von CloudNordic konnten lediglich Systeme wie Nameserver, Webserver und Mailserver für Kunden neu aufgesetzt werden, allerdings ohne Dateninhalt. Somit können Kunden Domains und Server wieder einrichten, müssen zur Datenwiederherstellung aber auf eigene lokale Kopien oder Wayback-Maschinen (z. B. web.archive.org) zurückgreifen. Allerdings erwartet CloudNordic nicht, dass die Kunden davon Gebrauch machen und geht davon aus, dass die Kunden zu anderen Anbietern wechseln werden. /BSI23r02, BLE23w03, CLO23w01, HEI23w07/

Neben CloudNordic und AzeroCloud sind von dem Angriff somit alle Kunden dieser Firmen betroffen. Laut /BLE23w03/ sind von dem Angriff mehrere hundert dänische Unternehmen betroffen. Diese haben alle Daten verloren, die in der Cloud gespeichert waren (z. B. Webseiten, E-Mail-Postfächer, Dokumente, usw.), falls keine Kopien der Daten an anderen Stellen vorhanden waren. Somit ist dieser Cyberangriff sowohl für CloudNordic und AzeroCloud als auch für die betroffenen Kunden potenziell existenzbedrohend.

Ransomware-Angriffe auf Cloud- und Hosting-Anbieter sind in den letzten Jahren häufiger vorgekommen. Da es durch einen erfolgreichen Angriff in der Regel zu massiven Störungen kommt, von denen viele Opfer betroffen sind, erhöht sich somit der Druck auf die Anbieter, ein Lösegeld zu zahlen. In der Regel lassen sich die Daten aber nach einiger Zeit wiederherstellen, da vom Netz getrennte Backup-Systeme vorhanden sind. Dies war bei diesem Angriff allerdings nicht der Fall. /BSI23r02, BLE23w03, HEI23w07/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.4 Physische Auswirkungen von Angriffen (meist Ransomware)

Im Juni 2023 wurde ein Bericht veröffentlicht, in dem ausgesagt wird, dass Angriffe auf kritische Infrastrukturen mit großen Auswirkungen im Vergleich zur Situation vor dem Ausbruch der Corona-Pandemie um 140 % gestiegen sind /SEC23w03/. Dem Bericht zufolge waren im Jahr 2022 über 150 Industriebetriebe von Angriffen betroffen, die zu physischen Folgen bei Fertigungsprozessen sowie in kritischen Infrastrukturen geführt haben, während es vor der Corona-Pandemie keine Cyberangriffe auf Produktionsanlagen gegeben haben soll. Des Weiteren wurde ausgesagt, dass die Gesamtzahl der Cyberangriffe im Vergleich zum Vorjahr um das 2,4-fache gestiegen ist. Legt man diese Wachstumsrate zugrunde, könnten laut /SEC23w03/ im Jahr 2027 bis zu 15.000 Industriestandorte von Cyberangriffen mit physischen Auswirkungen betroffen sein.

Die meisten dieser Cyberangriffe erfolgen laut /SEC23w03/ in Form von Ransomware-Angriffen, also der Verschlüsselung wichtiger Computersysteme und Daten in IT-Netzwerken. Durch diese Angriffe, die in den meisten Fällen nur auf die Netzwerke der IT-Unternehmen abzielen, ergeben sich aber in vielen Fällen auch Auswirkungen auf OT-Netze, also die physischen Prozesse in den Unternehmen. Bei nahezu allen Ransomware-Angriffen kam es auch zu physischen Auswirkungen, weil beispielsweise die physischen Betriebsabläufe von den betroffenen IT-Systemen abhingen oder die Opfer der Ransomware-Angriffe vorsichtshalber den Betrieb nach dem Angriff heruntergefahren haben.

Cyberangriffe, die sich auf die physischen Prozesse auswirken, können laut /SEC23w03/ zu Konsequenzen führen, die über Verzögerungen bei der Produktion hinausgehen. Folgende Beispiele für Cyberangriffe werden in /SEC23w03/ genannt:

- Ausfälle bei weithin bekannten Unternehmen, darunter 14 Werke eines führenden Automobilherstellers, 23 Werke eines bekannten Reifenherstellers sowie Ausfälle bei großen Lebensmittelunternehmen und einem Verlag
- Flugverspätungen für Zehntausende von Flugreisenden bei vier verschiedenen Cyberangriffen
- Beeinträchtigung der physischen Abläufe bei vier Cyberangriffen auf die Metallindustrie und den Bergbau; bei einem dieser Cyberangriffe kam es zu einem Brand und einer Beschädigung von materieller Ausrüstung
- Störungen beim Be- und Entladen von Frachtcontainern, Treibstoff und Öl in einem halben Dutzend Seehäfen auf drei Kontinenten
- Cyberangriffe führten zum Konkurs von zwei angegriffenen Unternehmen

Laut /SEC23w03/ kam es seit dem Jahr 2020 jährlich zu einer Verdoppelung von öffentlich zugänglichen Berichten über Cyberangriffe mit physischen Auswirkungen. Momentan steigt die Zahl der Cyberangriffe und betroffenen Standorte alle 2,5 Jahre um das Zehnfache. Bei einem Anhalten dieses Trends könnte sich die Zahl der Cyberangriffe und betroffenen Standorte zwischen den Jahren 2022 und 2027 laut /SEC23w03/ um das 100 fache erhöhen.

Die Mehrheit der Cyberangriffe im Jahr 2022 waren laut /SEC23w03/ eindeutig finanziell motivierte Ransomware-Angriffe mit einem Anteil von 74 %. Im Jahr 2022 führten 42 Ransomware-Angriffe zu physischen Auswirkungen, was nahezu der Gesamtzahl der Angriffe in den Jahren 2010 bis 2021 entspricht. Von den Ransomware-Angriffen im Jahr 2022 wurden 40 % auf bekannte Gruppierungen wie BlackCat, Conti, Lockbit, Hive, Black Basta, Black Byte, RansomEXX und LV zurückgeführt. Angriffe auf den Industriesektor ziehen aber auch Hacktivisten an, die im Jahr 2022 einen Anteil von 9 % aller Cyberangriffe ausmachten. Keiner dieser Cyberangriffe von Hacktivisten beinhaltete eine Löse-geldforderung. Diese Angriffe waren stattdessen laut /SEC23w03/ politisch oder ideologisch motiviert, mit dem einzigen Ziel der Störung kritischer Infrastrukturen oder Dienste, wobei die meisten dieser Angriffe im Zusammenhang mit dem laufenden Konflikt zwischen Iran und Israel oder dem russisch-ukrainischen Konflikt standen. Die

insgesamt sechs Cyberangriffe von Hacktivisten richteten sich in vier Fällen gegen die Unterbrechung des Verkehrsbetriebs (Schienenverkehr, öffentliche Verkehrsmittel oder Taxidienste), in einem Fall gegen ein Stahlwerk und in einem Fall gegen eine Ladestation für Elektrofahrzeuge. Die restlichen 17 % der Cyberangriffe des Jahres 2022 hatten kein erkennbares Motiv.

Ein weiterer in /SEC23w03/ hervorgehobener Trend ist die zunehmende Raffinesse der Cyberangriffe auf den Industriesektor. Während in den vergangenen Jahren nur staatlich geförderte Akteure Zugang zu fortschrittlichen Angriffswerkzeugen hatten, stehen fortschrittliche Werkzeuge laut /SEC23w03/ mittlerweile mehr Angreifern als je zuvor zur Verfügung. Das liegt daran, dass diese Werkezeuge mittlerweile weithin zugänglich sind. Dadurch bilden auch Länder, die zuvor nicht in der Lage waren, Schaden durch Cyberangriffe anzurichten, mittlerweile eine wachsende Bedrohung.

Aufgrund der wachsenden Bedrohung ist es laut /SEC23w03/ erforderlich, sich in den Richtlinien zur Cybersicherheit mit IT/OT-Interdependenzen zu befassen. Dabei sollten sich die Richtlinien zunächst mit der Definition der Kritikalität von Netzwerken und Systemen im Hinblick auf die schlimmsten Folgen eines Cyberangriffs befassen. Anschließend werden dann laut /SEC23w03/ spezifische Maßnahmen an der IT/OT-Grenze gefordert. Dabei sind die schlimmsten Szenarien einer Kompromittierung von OT-Netzwerken in der Regel physischer Natur (z. B. Produktionsausfall, Beschädigung von Geräten, usw.). Bei der Kompromittierung von IT-Netzwerken sind die schlimmsten Folgen eher geschäftlich (z. B. Aufräumkosten, Diebstahl geschützter Daten, Gerichtsverfahren im Zusammenhang mit personenbezogenen Daten, usw.). An der Schnittstelle zwischen IT und OT werden laut /SEC23w03/ sehr spezifische Sicherheitsmaßnahmen verlangt, die folgendes umfassen:

- OT-Netzwerke müssen mit der erforderlichen Kapazität weiterarbeiten, auch wenn IT-Netzwerke gefährdet sind
- Eigentümer und Betreiber müssen alle OT-Abhängigkeiten von IT-Diensten beseitigen. Ist dies nicht möglich, sind verbleibende Abhängigkeiten und Ausgleichsmaßnahmen zu dokumentieren
- Eigentümer und Betreiber müssen alle OT-zu-IT-Domain-Vertrauensverhältnisse beseitigen. Ist dies nicht möglich, sind Richtlinien zu entwickeln, um die Risiken auf-grund dieser Vertrauensverhältnisse zu verwalten

- OT-Netzwerke müssen so konzipiert sein, dass sie bei der Reaktion auf Cyberangriffe von IT-Netzwerken isoliert werden können

Aufgrund der exponentiellen Zunahme von Cyberangriffen auf die Fertigung und kritische Infrastrukturen ist es laut /SEC23w03/ unabdingbar, eine Strategie zum Umgang mit OT-Netzwerken, eine Schwachstellenbewertung sowie den Aufbau und die Optimierung eines OT-SOC (Security Operations Center, zentrale Stelle im Unternehmen, die sich ganzheitlich und dynamisch der Sicherheit aller OT-Komponenten und OT-Infrastruktur widmet) voranzutreiben.

B.15.5 Cyberangriff auf Zaun (UK)

Übersicht

Am 01.09.2023 wurde bekannt, dass es zu einem Cyberangriff auf Zaun Ltd., einem in Wolverhampton (West Midlands, England) ansässigen Hersteller von Umzäunungen, Sicherheitstoren, Pollern und anderen Sicherheitsbarrieren für kritische Infrastrukturen, gekommen ist. Zaun Ltd. ist laut eigenen Aussagen ein Spezialist für Hochsicherheitsumzäunungen und hat beispielsweise Gefängnisse, Militärbasen und Versorgungsunternehmen mit Zäunen ausgestattet. Bei dem Angriff wurden Daten entwendet, es kam aber nicht zum Ausfall von IT-Systemen oder zur Beeinträchtigung der Arbeiten. /DAI23w01, DAI23w02, DAR23w01, ZAU23w01/

Beschreibung

Zaun Ltd. wurde am 05./06. August 2023 Ziel eines Cyberangriffs mit Ransomware, die der Ransomware-Gruppierung LockBit zugeschrieben wird. Laut Aussagen von Zaun Ltd. konnten die unternehmenseigenen Vorkehrungen gegen Cyberangriffe verhindern, dass Daten verschlüsselt wurden. Nach dem Angriff wurden Untersuchungen zu dem Angriff eingeleitet. Die nationalen Cybersicherheitsbehörden wurden über den Vorfall informiert und externe Berater wurden hinzugezogen. Der Angriff hatte keine Beeinträchtigung des Geschäftsbetriebs zur Folge, es kam aber zur Extraktion von Daten aus dem betroffenen IT-Netzwerk. /DAI23w01, DAI23w02, DAR23w01, ZAU23w01/

Bei dem Cyberangriff kam es zum Zugriff der LockBit-Gruppierung mittels einer Ransomware. Der Zugriff erfolgte über einen Windows-7-PC, auf welchem die Steuerungssoftware für eine der Produktionsmaschinen lief.

Details zur Sicherheitslücke, die bei dem Angriff ausgenutzt wurde, liegen nicht vor, es ist aber anzumerken, dass Windows 7 erstmals im Jahr 2009 veröffentlicht wurde und dass die Unterstützung für das Betriebssystem bereits im Jahr 2020 ausgelaufen ist und erweiterte Sicherheitsupdates seit Januar 2023 nicht mehr bereitgestellt werden. Nach dem Cyberangriff wurde der betroffene Rechner entfernt und die Sicherheitslücke laut Zaun Ltd. somit geschlossen. /DAR23w01, ZAU23w01/

Bei dem Cyberangriff wurden keine Daten auf dem betroffenen IT-Netzwerk verschlüsselt, es kam aber zur Extraktion von Daten in einer Größenordnung von 10 GB. Es ist nicht klar, ob diese auf den betroffenen PC beschränkt waren oder ob auch auf interne Server zugegriffen werden konnte. Laut Zaun Ltd. handelt es sich bei den gestohlenen Daten um historische E-Mails, Bestellungen, Zeichnungen und Projektdaten, geheime Informationen wurden nicht extrahiert. Zaun Ltd. ist laut eigenen Aussagen kein von der Regierung zugelassener Sicherheitsdienstleister und alle Einzelheiten zu Produkten seien auf der Unternehmenswebseite verfügbar und frei einsehbar. Aus den extrahierten Daten könne laut Zaun Ltd. kein zusätzlicher Nutzen gezogen werden, der über das hinausgeht, was aus der Einsichtnahme in die öffentlich zugänglichen Webseiten erhältlich wäre. Diese Aussage steht im Widerspruch zu den Aussagen britischer Tageszeitungen. In diesen wird berichtet, dass sensible Informationen über die Geschäfte von Zaun Ltd. mit Einrichtungen des britischen Verteidigungsministeriums ins Darknet gestellt wurden. Laut britischen Tageszeitungen wurden Einzelheiten über Sicherheitsausrüstungen einer Atom-U-Boot-Basis, eines Chemiewaffenlabors, einer Station der Royal Air Force, einer militärischen Forschungseinrichtung, einer Kaserne der britischen Armee sowie Informationen über eine Reihe britischer Hochsicherheitsgefängnisse und Bestellungen von Militär- und Geheimdiensten veröffentlicht. Inwiefern die Aussage der britischen Tageszeitungen hinsichtlich der Veröffentlichung sensibler, streng geheimer Informationen oder die Aussagen von Zaun Ltd., dass die gestohlenen Daten über die Unternehmenswebseiten in vollem Umfang bezogen werden können, stimmen, lässt sich anhand der vor-liegenden Unterlagen nicht ermitteln. /DAI23w01, DAI23w02, DAR23w01, ZAU23w01/

Laut /FBI22r01, KAS22w02/ ist LockBit eine Ransomware-Gruppierung, deren erste Angriffe im September 2019 bekannt geworden sind. Zu diesem Zeitpunkt wurde die Gruppierung noch ABCD genannt, da diese Dateierweiterung bei verschlüsselten Daten verwendet wurde. Bei LockBit handelt es sich um eine Ransomware-as-a-Service-Gruppierung, die laut /REC22w01/ eine der produktivsten aktiven Gruppierungen ist.

Im Jahr 2022 wurden laut /DAI23w02/ von LockBit mehr als 1400 Ransomware-Angriffe durchgeführt. Die Gruppierung führt zielgerichtete Angriffe auf Unternehmen und Regierungsorganisationen aus, Privatpersonen sind eher keine Angriffsziele. Es werden Unternehmen weltweit angegriffen, wobei bewusst Unternehmen mit Standort in Russland gemieden werden. Die Schadsoftware von LockBit ist dabei darauf ausgelegt, den Zugriff zum angegriffenen System zu sperren, Daten zu verschlüsseln und damit eine Lösegeldzahlung zu erzwingen. Laut /CSO23w01/ ist der hier beschriebene Angriff für die LockBit-Gruppierung eher ungewöhnlich, da es normalerweise vermieden wird, sensible Organisationen oder solche anzugreifen, die die Aufmerksamkeit der Strafverfolgungsbehörden nach sich ziehen und eine erhöhte Medienpräsenz der Gruppierung zur Folge haben.

Kerntechnischer Bezug

Zaun Ltd. ist Hersteller von Hochsicherheitsumzäunungen, die laut eigenen Aussagen auch in kerntechnischen Anlagen eingesetzt werden. Inwieweit bei dem Cyberangriff sensible, streng geheime Informationen entwendet wurden, kann aus den vorliegenden Unterlagen nicht eindeutig ermittelt werden. Laut Zaun Ltd. wurden ausschließlich Daten gestohlen, die über die Unternehmenswebseiten in vollem Umfang bezogen werden können. Daher liegen bislang keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.6 BianLian-Ransomware

Übersicht

Am 16.05.2023 wurde vom Federal Bureau of Investigation (FBI), der US-Behörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) und dem australischen Zentrum für Cybersicherheit (Australian Cyber Security Center, ACSC) ein gemeinsamer Bericht veröffentlicht, um vor der Ransomware-Gruppierung BianLian zu warnen, die vor allem in den USA und Australien mehrere Organisationen mit Ransomware angegriffen hat. /CIS23w03/

Beschreibung

Die Ransomware-Gruppierung BianLian ist im Juni 2022 erstmals aufgetreten und hat seitdem mehrere Unternehmen (auch Betreiber kritischer Infrastrukturen) angegriffen.

Dabei werden insbesondere Unternehmen angegriffen, die mit sensiblen Daten arbeiten, wie beispielsweise Finanzinstitute, Regierungsorganisationen, professionelle Dienstleistungsunternehmen, Fertigungsunternehmen, Unternehmen aus der Medienbranche, Unternehmen aus dem Gesundheitswesen sowie Bildungseinrichtungen. Dabei operiert die Ransomware-Gruppierung BianLian weltweit, wobei eine höhere Konzentration an An-griffen in den USA, Australien und Europa vorliegt. Bis Mitte 2023 wurden insgesamt 145 Organisationen Opfer der Gruppierung. Genaue Informationen zu den angegriffenen Unternehmen, den erpressten sowie den tatsächlich erhaltenen Lösegeldern liegen der GRS nicht vor.

Ursprünglich setze die Ransomware-Gruppierung BianLian bei ihren Angriffen das Modell der doppelten Erpressung ein, bei welchem Daten der Opfer gestohlen und anschließend im Opfernetzwerk verschlüsselt werden. Dann wird ein Lösegeld für die Entschlüsselung der Daten verlangt, wobei ein weiteres Druckmittel die zuvor gestohlenen Daten sind, mit deren Veröffentlichung gedroht wird. Nachdem im Januar 2023 von Avast ein Entschlüsselungsprogramm veröffentlicht wurde, welches die Verschlüsselung mit der BianLian-Ransomware aufheben konnte, hat die Gruppierung ihre Vorgehensweise geändert. Es wurde dazu übergegangen, hauptsächlich durch Exfiltration zu erpressen, also nur durch die Warnung vor der Veröffentlichung gestohlener, sensibler Daten. Die IT-Systeme der Opfer bleiben bei den Angriffen intakt, es findet keine Verschlüsselung von Daten statt. /CIS23w03, LOG23w01, SOC23w02, ZDN23w01/

Bei den Angriffen mittels BianLian-Ransomware wurde der Erstzugriff zum Opfernetzwerk meist durch Ausnutzung gültiger, kompromittierter Zugangsdaten für das Remote Desktop Protokoll (RDP) erlangt. Die Zugangsdaten wurden entweder gekauft oder per Phishing erhalten. Zum Aufbau einer Command and Control Struktur wurde für jedes Opfer eine spezifische, in der Programmiersprache Go programmierte Backdoor in das Opfernetzwerk implantiert sowie eine Software für die Fernverwaltung und den Fernzugriff installiert, wie z. B. TeamViewer, Atera Agent, Splash Top oder AnyDesk. Außerdem wurden lokale Administratorkonten erstellt oder aktiviert und die Passwörter dieser Konten geändert. Um einer Entdeckung nach der Infiltration der Opfernetzwerke zu umgehen, verwenden Akteure der Ransomware-Gruppierung BianLian PowerShell und Windows Command Shell, um Antivirenprogramme zu deaktivieren. Außerdem werden Änderungen an der Windows-Registry vorgenommen, um den Manipulationsschutz von Sophos-Diensten zu deaktivieren und damit die Möglichkeit zu schaffen, diese Dienste zu deaktivieren.

Anschließend werden von der Ransomware-Gruppierung BianLian mehrere Tools in das Opfernetzwerk geladen, um das Opfernetzwerk auszuspionieren. Verwendete Tools sind beispielsweise Advanced Port Scanner (Netzwerkscanner, der offene Ports auf Netzwerkcomputern finden soll und die Versionen von Programmen ab-rufen soll, die auf diesen Ports laufen), SoftPerfect Netzwerkscanner (Netzwerkscanner, der Computer anpingen, Ports scannen und freigegebene Ordner entdecken kann), SharpShares (Aufzählen der zugänglichen Netzwerkfreigaben in einer Domäne) sowie PingCastle (Aufzählen von Active Directory). Zum Auskundschaften der Opfernetzwerke nutzen Akteure der Ransomware-Gruppierung BianLian außerdem Windows-Tools und die Windows Command Shell. /CIS23w03, LOG23w01, ZDN23w01/

Anschließend wird von der Ransomware-Gruppierung BianLian mithilfe von PowerShell-Skripten nach sensiblen Daten gesucht, die dann zur Datenerpressung exfiltriert werden. Die Exfiltration erfolgt über das File Transfer Protokoll (FTP), Rclone (Tool zur Synchronisation von Dateien mit Cloud-Speichern) sowie den Dateifreigabedienst Mega. Bis zum Januar 2023 wurden die Daten im Opfernetzwerk nach der Exfiltration verschlüsselt, wobei zur Verschlüsselung ein AES-256-Schlüssel verwendet wurde. Der Verschlüsseler änderte alle verschlüsselten Dateien so, dass diese die Endung .bianlian er-hielten. Außerdem wurde in jedem betroffenen Verzeichnis eine Erpresser-Notiz erstellt. Nach Veröffentlichung eines Entschlüsselungsprogramms für mittels der BianLian-Ransomware verschlüsselten Dateien erfolgt von der Ransomware-Gruppierung BianLian keine Verschlüsselung der Daten mehr nach deren Exfiltration. Die Gruppierung hat sich ausschließlich auf den Diebstahl sensibler Daten spezialisiert und nutzt diese als Druckmittel, um die Opfer mit der Warnung der Veröffentlichung exfiltrierter Daten zu einer Lösegeldzahlung zu erpressen. Sollte eine Lösegeldzahlung verweigert werden, droht die Ransomware-Gruppierung BianLian damit, die exfiltrierten Daten auf einer Seite im Tor-Netzwerk zu veröffentlichen. /CIS23w03, LOG23w01, ZDN23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.7 Cyberangriff auf Albert Ziegler GmbH

Übersicht

Am 09.02.2023 kam es zu einem Cyberangriff auf die Albert Ziegler GmbH, einem deutschen Hersteller von Feuerwehrbedarf und Fahrzeugen mit Hauptsitz im schwäbischen Giengen. Die Albert Ziegler GmbH ist laut eigener Aussage ein international führender Anbieter von Lösungen für die Brandbekämpfung sowie das Notfall- und Einsatzmanagement, wobei das Produktportfolio alle Arten von Einsatzfahrzeugen, Feuerlöschsystemen, Steuerungs- und Betriebslösungen sowie Feuerwehrausrüstung umfasst und bei Feuerwehren (kritische Infrastruktur) in über 100 Ländern weltweit im Einsatz ist. Aufgrund des Angriffs wurden alle relevanten IT-Systeme umgehend abgeschaltet. /BSI23r06, ZIE23w01/

Beschreibung

Die Albert Ziegler GmbH wurde am 09. Februar 2023 Ziel eines Cyberangriffs mit Ransomware, die der Ransomware-Gruppierung ALPHV (BlackCat) zugeschrieben wird. Laut Aussagen der Albert Ziegler GmbH wurden aufgrund des Angriffs standortübergreifend sämtliche IT-Systeme sicherheitshalber abgeschaltet, wodurch die Arbeitsfähigkeit und die Erreichbarkeit stark eingeschränkt wurden. Nach dem Angriff wurden Untersuchungen zu dem Angriff eingeleitet, wobei sowohl die entsprechenden Behörden informiert wurden als auch externe Berater hinzugezogen wurden. Vermutlich kam es bei dem Cyberangriff sowohl zu einer Extraktion als auch zur Verschlüsselung von Daten. Trotz der Zusammenarbeit mit externen Beratern und Dienstleistern, um die IT-Systeme schnellstmöglich wieder in Betrieb zu nehmen, waren die Systeme am 20.02.2023 erst teilweise wiederhergestellt. Laut Aussage der Albert Ziegler GmbH mussten alle Systeme neu aufgesetzt werden. /BSI23r06, BTB23w01, ZIE23w01, ZIE23w02/

Bei dem Cyberangriff kam es zum Zugriff der Ransomware-Gruppierung ALPHV (BlackCat) mittels einer Ransomware. Über den genauen Ablauf des Angriffs, die Menge der verschlüsselten bzw. extrahierten Daten sowie deren Inhalt liegen der GRS keine Informationen vor. Über eine eventuelle Lösegeldforderung liegen der GRS ebenfalls keine In-formationen vor, es ist aber davon auszugehen, dass ein Lösegeld gefordert wurde. Am 21.04.2023 wurde auf der Leak-Seite der Ransomware-Gruppierung ALPHV (BlackCat) die Albert Ziegler GmbH als Opfer eines Cyberangriffs angegeben und es wurden

mehrere gestohlene Dokumente veröffentlicht, die angeblich dem Unternehmen gehören sollen. Dies deutet darauf hin, dass einer eventuellen Lösegeldforderung nicht nachgekommen wurde und kein Lösegeld gezahlt wurde. /BSI23r06, BTB23w01/

BlackCat ist eine bekannte Ransomware-Gruppierung, deren Angriffe erstmals im November des Jahres 2021 bekannt wurden und die seitdem bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. BlackCat ist dabei die erste Organisation, die ihre Ransomware in der Programmiersprache Rust geschrieben hat, wodurch die Ransomware relativ einfach auf mehrere Betriebssysteme und Prozessarchitekturen anzupassen ist und damit speziell auf ein ausgewähltes Ziel zugeschnitten werden kann. Wie üblich erfolgt bei einem Angriff eine Verschlüsselung der Daten und eine Erpressung von Lösegeld für deren Entschlüsselung. Für den Fall des Nichtbezahlens des Lösegeldes wird mit der Veröffentlichung der Daten gedroht.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.8 Angriff auf die polnische Bahn

Übersicht

Am 25.08.2023 kam es zu einem durch Einwirkung Dritter verursachten Halten einiger Züge im Nordwesten Polens, ausgelöst aufgrund eines vermutlich unbefugten Sendens eines Nothalt-Signals. Daraufhin kam es zu einer Reihe Verspätungen im polnischen Bahnverkehr /BSI23r08/. Am 29.08.2023 kam es zu weiteren 25 Nothalten im polnischen Bahnverkehr, diesmal waren südwestliche und nördliche Provinzen betroffen /BSI23r10/.

Beschreibung

Der polnische Bahnverkehr wurde am 25.08.2023 und am 29.08.2023 Opfer von Angriffen, durch die es zu Störungen des Bahnverkehrs (zum Anhalten von Zügen und daraufhin zu Verspätungen im Zugverkehr) gekommen ist. Betroffen waren nördliche, nordwestliche und südwestliche Provinzen in Polen /BSI23r10/. Zudem wurden die Störsignale mit Aufnahmen der russischen Nationalhymne und einer Ansprache von Wladimir Putin begleitet /WIN23w01, HEI23w01, WIR23w01/. Durch das unbefugte Senden eines Notsignals kam es zum Anhalten von Zügen, dieses Senden erfolgte im

ungesicherten 150-MHz-Band des analogen Funksystems der „Polnische Staatsbahnen AG“ /BSI23r10/. Zum Herbeiführen dieser Störung wird lediglich ein Radiosender benötigt, sowie die richtige Frequenz und der physische Zugang in ein Gebiet einige Kilometer um den gewünschten Haltepunkt herum /WIN23w01/. Es ist hierbei nicht klar, ob für diesen Angriff Radiosender in die betroffenen Gebiete eingebracht wurden oder ob bestehende Radiosender angegriffen und missbraucht wurden. Es handelt sich grundsätzlich um einen technisch einfach durchzuführenden Angriff, wobei eine seit langem bekannte Schwachstelle der technischen Infrastruktur ausgenutzt wurde /WIN23w01, HEI23w01/. Bis zum Nachmittag des 29.08.2023 kam es zum Auslösen von 25 Nothalten im polnischen Bahnverkehr /BSI23r10/. Vermutet wird, dass Angreifer aus Russland und Belarus diesen Vorfall verursacht haben /FOC23w01, BSI23r10/. Als Grund dieser Sabotage wird die aktive Unterstützung der ukrainischen Verteidigungsmaßnahmen gegen die russische Invasion durch Polen vermutet /WIN23w01/, insbesondere durch Waffenlieferungen und andere Hilfen an die Ukraine /HEI23w01, BSI23r10/. Zur Vermeidung von Angriffen auf das ungesicherte 150-MHz-Band soll bis 2025 der Zugverkehr digitalisiert werden; in Deutschland wurde der analoge Zugfunk bereits abgelöst. Die polnische Nachrichtenagentur (Polska Press Agency (PAP)) berichtet von Festnahmen in Bezug auf diesen Vorfall, so sollen Mitarbeiter eines Spionagerings im Laufe des Jahres vom polnischen Inlandsgeheimdienst festgenommen worden sein /BSI23r10/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.9 Cyberangriff auf das Bundesfinanzministerium (DDoSia-Projekt)

Übersicht

Am 16.08.2023 wurden mehrere deutsche Webseiten Opfer eines Cyberangriffs, der zu einer Nichterreichbarkeit der Webseiten führt. Unter den betroffenen Webseiten befanden sich deutsche Versicherungskonzerne und die Webseite des Bundesfinanzministeriums (BMF) /BSI23w07/.

Beschreibung

Mehrere Webseiten von deutschen Versicherungskonzernen und die des Bundesfinanzministeriums (BMF) wurden auf einer Zielliste des pro-russischen DDoS-Netzwerkes „DDoSia“ am 16.08.2023 aufgelistet und vermutlich aufgrund dieser Auflistung im Nachgang angegriffen. Bei den Cyberangriffen handelte es sich um DDoS-Angriffe. Diese sind nach Angaben des BSI vermutlich auf die pro-russische Angreifergruppierung NoName057(16) zurückzuführen. Die Cyberangriffe auf die gelisteten Webseiten waren zu Teilen erfolgreich, da die Webseiten des BMF und einiger Versicherungskonzerne nur sporadisch oder eingeschränkt erreichbar waren. Als Grund für die Angriffe wird von den Angreifergruppierungen im Allgemeinen die Unterstützung der Ukraine durch Deutschland angeführt, hier im Besonderen die finanzielle Unterstützung der Ukraine durch Deutschland /BSI23w07/.

Die Angreifergruppierung NoName057(16) startete bereits im Sommer 2022 ein DDoS-Projekt /GOL23w02/ mit dem Namen DDoSia. Bei DDoSia handelt es sich um ein von der genannten Angreifergruppierung entwickeltes DDoS-Angriffs-Toolkit. DDoSia wird eingesetzt, um Länder anzugreifen, die sich im Ukraine-Krieg gegen Russland positionieren /SAK23w01/. Freiwillige können sich diesem Projekt anschließen und Cyberangriffe gegen verschiedene Ziele durchführen. Die Organisation der DDoS-Angriffe läuft hauptsächlich über Telegram und die Teilnehmeranzahl des DDoSia-Projektes steigt weiterhin an. Zum Anlocken von mehr Teilnehmern an diesem Projekt werden die Teilnehmer mit Kryptowährungen bezahlt /GOL23w02, SAK23w01/. Im Fokus der Cyberangriffe im Rahmen dieses Projekts stehen hauptsächlich die Ukraine und NATO-Länder /GOL23w02, SAK23w01/.

Seit Beginn des DDoSia-Projektes der Gruppierung NoName057(16) sind bereits zahlreiche Länder Opfer von DDoS-Angriffen geworden. Seit 2022 werden primär Ziele in Europa angegriffen, aber auch Australien, Kanada und Japan waren schon von Cyberangriffen durch diese Angreifergruppierung betroffen /THN23w01/. Es ist zu erkennen, dass sich die Angreifergruppierung NoName057(16) primär auf die Ukraine und die NATO-Mitgliedsstaaten fokussiert, einschließlich der östlichen Staaten, wie Litauen, Polen, Tschechien und Lettland. Sekundär sind die westlichen NATO-Länder, wie Frankreich, Großbritannien, Italien, Kanada oder andere EU-Staaten Ziele von DDoSia-Angriffen, aufgrund der politischen, militärischen und ökonomischen Unterstützung der Länder für die Ukraine /SAK23w01/. Im Jahr 2023 wurden in den Monaten zwischen Mai und Juni zahlreiche Webseiten in Deutschland angegriffen.

Im Durchschnitt werden weltweit ungefähr 15 Ziele täglich angegriffen /GOL23w02, SAK23w01/.

Die Kommunikation zum DDoSia-Projekt läuft über den Telegram-Kanal der Gruppierung NoName057(16), es gibt einen russischen und englischen Kanal. Über einen Link können interessierte Hacker dem Projekt beitreten und erlangen dadurch Zutritt zu sieben verschiedenen Kanälen. Einer dieser Kanäle enthält die Anleitung zur Durchführung eines DDoS-Angriffs mit dem DDoSia-Toolkit. Es können über den Telegram-Kanal die benötigten Dateien für diesen Cyberangriff mit der entsprechenden Anleitung der einzelnen durchzuführenden Schritte, erzeugt werden. Durch die Registrierung über einen russischsprachigen Bot erhält der Benutzer am Ende eine Zip-Datei mit der notwendigen Schadsoftware. Beim Ausführen der Datei ist die Anzahl der Ziele und die ausgeführten Aktionen gegen das Ziel zu sehen /SAK23w01/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.10 Cyberangriffe auf osteuropäische Regierungen

Übersicht

Zwischen März und Mai 2023 wurden diplomatische Einrichtungen in ganz Osteuropa Opfer einer Phishing-Kampagne /BSI23r11/.

Beschreibung

Diplomatische Einrichtungen in ganz Osteuropa wurden zwischen März und Mai 2023 Ziel einer Spear-Phishing-Kampagne der russischen APT-Gruppierung APT29 (auch bekannt als BlueBravo, Nobelium, Cloaked Ursa und Midnight Blizzard) (siehe Abschnitt 2.10.2). Bei den Cyberangriffen im Rahmen dieser Angriffswelle wurde versucht, die Empfänger mit einer Backdoor namens GraphicalProton zu infizieren. Bereits im Januar waren Phishing Angriffe mit einer Backdoor namens GraphicalNeutrino erfolgt. Im Unterschied zu GraphicalNeutrino wird GraphicalProton jedoch als Loader verwendet. GraphicalProton wird über eine in einer Phishing-E-Mail enthaltenen ISO- oder ZIP-Datei auf betroffene Systeme eingebracht und nutzt Microsofts OneDrive oder Dropbox für die Command-and-Control-Kommunikation.

Es ist anzunehmen, dass die Angriffswelle auf das Interesse der russischen Regierung an strategischen Daten in Bezug auf den Ukraine-Krieg zurückzuführen ist /BSI23r11/.

Kerntechnische Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.11 Cyberangriff auf Eurocontrol

Übersicht

Am 20.04.2023 teilte die europäische Flugsicherungsbehörde Eurocontrol mit, dass sie am 19.04.2023 Opfer eines Cyberangriffs geworden war /BLI23w01, SEC23w04//. Die European Organization for the Safety of Air Navigation (EOSAN), auch bekannt als Eurocontrol, koordiniert den Flugverkehr in 41 Ländern /CPO23w01, SEC23w04/ und ist für die Sicherheit des Luftverkehrs in Europa zuständig, sowie für die Verwaltung des grenzüberschreitenden Luftverkehrs in den von den nationalen Luftverkehrsbehörden kontrollierten Lufträumen /BLI23w01/.

Beschreibung

Die europäische Luftsicherungsbehörde Eurocontrol wurde im April 2023 Opfer eines Cyberangriffs, zu dem sich die Angreifer-Gruppierung Killnet bekannt hat. Es handelte sich hier um einen erneuten DDoS-Angriff, der zu Unterbrechungen der Webseite und der Webverfügbarkeit der Behörde führte /CPO23w01, BLI23w01, SEC23w04, CSO23w02/. Nach Angaben eines Eurocontrol-Beamten wurde umgehend reagiert und sämtliche operativen Systeme abgeschottet. Die internen Systeme sowie die Sicherheit der Flugnavigation wurden nicht kompromittiert. Es kam zu keinerlei Verspätungen oder Störungen bei kommerziellen Flügen. Dennoch erschwerte der Cyberangriff den Flugsicherungsbetrieb. Einige Airlines waren gezwungen, kommerzielle Lösungen zur Koordinierung der Flüge zu verwenden und mindestens 2.000 Mitarbeiter hatten keinen Zugang zu den internen und externen Kommunikationstools /CPO23w01, BLI23w01, CSO23w02/ (die Kommunikation musste über eine andere Software erfolgen /WAT23w01, CSO23w02/). Zusätzlich kam der Hinweis an Fluggesellschaften, dass die Flugpläne über andere Kanäle eingereicht werden sollten. Somit kam es zu massiven Auswirkungen auf Eurocontrol.

Als Grund für den Cyberangriff wird die Unterstützung der Ukraine durch Eurocontrol vermutet, da diese mit der NATO verbunden ist /CSO23w02/.

Dieser Cyberangriff auf den Flugverkehr war bei weitem nicht der erste und einzige Angriff, der von Killnet durchgeführt wurde. Im Oktober 2022 griff die Angreifergruppierung bereits 14 US-Flughäfen mit DDoS-Angriffen an. Zudem wurden auch etwa zwei Dutzend Flughäfen in Europa von Killnet angegriffen /CPO23w01/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.12 Cyberangriff auf Webseiten von Krankenhäusern

Übersicht

Am 30.01.2023 wurden mehrere Systeme von Krankenhäusern in den USA Opfer eines Cyberangriffs /COM23w01/. Es wurden auch Webseiten von europäischen Krankenhäusern angegriffen, wie zum Beispiel das University Medical Center Groningen in den Niederlanden /BIT23w01/. Die Angreifergruppierung nannte als Opfer des Cyberangriffs noch Ziele in weiteren Staaten, darunter Großbritannien, Norwegen und Deutschland /BSI23r03/.

Beschreibung

Ende Januar 2023 wurden mehrere Webseiten von Krankenhäusern in den USA, sowie in einigen europäischen Ländern Opfer von Cyberangriffen. Die Cyberangriffe waren die Folge eines Aufrufs der Angreifergruppierung Killnet vom 28.01.2023, worin zu DDoS-Angriffen auf Webseiten von Krankenhäusern in unterschiedlichen westlichen Staaten aufgerufen wurde /COM23w01, MAL23w02, BSI23w03/. In den USA waren beispielsweise mehrere Webseiten der University of Michigan Health nicht erreichbar. Nach Angaben der Betroffenen erfolgte bei keinem der Cyberangriffe Zugriff auf Patienteninformationen /DFP23w01/. Nach Angaben von Killnet kam es aufgrund der Angriffswelle zu Nichterreichbarkeiten von Webseiten von angegriffenen Krankenhäusern. Dies lässt sich auch beispielsweise für Krankenhäuser in den USA und den Niederlanden bestätigen.

Bei den anderen aufgelisteten Ländern wurden nach Angaben des BSI zufolge keine Einschränkungen auf den Webseiten der Krankenhäuser gemeldet /BSI23w03/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.13 Cyberangriffe auf die deutsche Behörde und deutsche Unternehmen

Übersicht

Am 25.01.2023 wurden deutsche Behörden und Unternehmen Opfer von Cyberangriffen. Betroffen waren Webseiten von Flughäfen, der Bundes- und Landesverwaltung, sowie Webseiten im Finanzsektor /ZDF23w02/.

Beschreibung

Nach einer Ankündigung der Angreifergruppierung Killnet, Cyberangriffe auf deutsche Ziele durchzuführen, wurden eine Reihe von deutschen Behörden und Unternehmen Ende Januar 2023 Opfer von Cyberangriffen. Der von Killnet angegebene Grund für die angedrohten und durchgeführten Cyberangriffe war die Zusage der Lieferung von deutschen Leopard-Panzern an die Ukraine. Bei den Cyberangriffen handelt es sich, wie bei Killnet schon vielfach beobachtet, um DDoS-Angriffe, die zu einer Nichterreichbarkeit von einigen Webseiten führten. Betroffen waren dabei Webseiten von Flughäfen, der Bundes- und Landesverwaltung, sowie die baden-württembergische Polizei /ZDF23w02, HAN23w01, TAG23w01, CSO23w03/. Die Cyberangriffe bzw. angekündigten und versuchten Cyberangriffe sind Teil der von Killnet unterstützten Aktion #DeutschlandRIP /HAN23w01, TAG23w01, CSO23w03/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.14 Veröffentlichung von Daten im Bezug zur NATO

Übersicht

Am 20.04.2023 wurden über Telegram mehrere Dokumente mit Bezug zur NATO veröffentlicht, darunter Screenshots und eine CSV-Datei mit personenbezogenen Daten /BSI23r05/.

Beschreibung

Die Angreifergruppierung Killnet hat Ende April 2023 mehrere Dokumente mit personenbezogenen Daten von über 4.600 Personen veröffentlicht. Diese Daten sollen mit der NATO in Verbindung stehen. Die Angreifergruppierung Killnet ist vor allem für zahlreiche DDoS-Angriffe auf verschiedene Ziele bekannt. Es ist in diesem Fall nicht bekannt, wie Killnet an die betroffenen Daten gelangt ist und wie valide die veröffentlichten Informationen sind. Auch wenn es der Einschätzung des BSI zufolge bislang keine Weiterentwicklung der technischen Fähigkeiten von Killnet gibt, ist nicht auszuschließen, dass die Gruppierung Zugang zu einzelnen Portal-Accounts oder einer Datenbank erlangt hat /BSI23r05/. Ebenso nicht auszuschließen ist, dass die Angreifergruppierung an einer Erweiterung ihrer Fertigkeiten arbeitet.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.15 Cyberangriff auf World Congress Webseite

Übersicht

Im Juli 2023 warnte das CERT (Computer Emergency Response Team) der Ukraine „CERT-UA“ vor einer maliziösen Webseite, die einen Zusammenhang mit dem Ukraine World Congress vortäuschte /BSI23r12/.

Beschreibung

Die legitime Webseite des Ukraine World Congress "https://ukrainianworldcongress.org" wurde hierzu von den Angreifern kopiert und um maliziöse Inhalte erweitert.

Diese Phishing-Kampagne wird der prorussischen Gruppierung RomCom (auch bekannt als Storm-0978 und DEV-0978) zugerechnet und steht vermutlich im Zusammenhang mit dem NATO-Gipfel in Litauen, der am 11. Und 12.07.2023 stattfand. Die genannte Webseite enthielt mehrere Dokumente im Microsoft Word Format und nach dem Öffnen dieser Dokumente erfolgte ein Verbindungsaufbau mit der Infrastruktur der Angreifer über SMB und http. Auf diesem Weg wurden mehrere Dateien heruntergeladen und ausgeführt. Diese Phishing Kampagne nutzte eine bis dahin noch nicht bekannte Schwachstelle von Microsoft Office mit der Kennung CVE-2023-36884 aus. Diese Schwachstelle ermöglicht es einem Angreifer, beliebigen Code auszuführen, jedoch muss der Angreifer den Nutzer dazu verleiten ein manipuliertes Office-Dokument zu öffnen/BSI23r12/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.16 Cyberangriff auf Mailserver der Ukraine

Übersicht

Im Mai 2023 berichtete das CERT (Computer Emergency Response Team) der Ukraine „CERT-UA“ über eine laufende Phishing-Kampagne auf staatliche Regierungsbehörden in der Ukraine /BSI23r13, BSI23r14/. Mit einer weiteren Phishing-Kampagne im Juni 2023 wurden laut CERT-UA E-Mail-Server ukrainischer Behörden und Regierungsstellen kompromittiert /BSI23r15/.

Beschreibung

Im Mai 2023 berichtete das CERT-UA über eine Phishing-Kampagne, die der APT-Gruppierung APT28 (auch bekannt als BlueDelta, Fancy Bear, Sednit oder Sofacy) zugerechnet wird (siehe Abschnitt 2.10.1). Bei dieser Kampagne wurden Mails an staatliche Regierungsbehörden in der Ukraine geschickt, die Anweisungen für die Durchführung eines vorgeblichen Windows-Update geben, als Absender wird eine @outlook.com E-Mail-Adresse verwendet. Für das angebliche Windows-Update soll ein PowerShell-Skript heruntergeladen und ausgeführt werden.

Dabei wird im Hintergrund ein weiteres, maliziöses Power-Shell-Skript heruntergeladen, dass Informationen von den betroffenen Systemen sammelt und dies an eine Mocky API sendet /BSI23r13, BSI23r14/.

Auch der Angriff im Juni 2023 wird der APT-Gruppierung APT28 zugeschrieben. Von dieser Phishing-Kampagne betroffen waren u. a. ein regionales Büro der Staatsanwaltschaft, eine zentrale Regierungseinheit und verschiedene Regierungsstellen, sowie eine Organisation, die sich mit der Instandhaltung militärischer Infrastruktur beschäftigt. Bei der Phishing-Kampagne wurden verschiedene Schwachstellen der Webmail-Anwendung Roundcube ausgenutzt. So waren die Angreifer in der Lage ungepatchte E-Mail-Server zu übernehmen, E-Mails umzuleiten und Informationen, wie beispielsweise Adressbücher auszuleiten. Das Hauptziel dieser Kampagne war offenbar das Erlangen von militärischen Informationen /BSI23r15/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.17 Cyberangriff auf russischen Radiosender

Übersicht

Am 09.03.2023 wurden TV- und Radiosender in Moskau gehackt und ein fingierter Atomalarm gesendet /FRA23w01/. Am 05.06.2023 kam es erneut zu Hackerangriffen auf die Radiosender sowie vermutlich auch einige TV-Sender und es wurde in den an die Ukraine angrenzenden russischen Gebieten, eine gefälschte Rede von Präsident Putin gesendet /BSI23r16/.

Beschreibung

Im Jahr 2023 wurden im März und im Juni Cyberangriffe auf russische Radio- und TV-Sender ausgeübt. Bei diesen Cyberangriffen wurde im März ein fingierter Atomalarm in Moskau gesendet und im Juni eine gefälschte Rede von Präsident Putin. Bei dem Atomalarm wurde die Bevölkerung aufgefordert, Schutzräume aufzusuchen und Jodtabletten einzunehmen. Im Fernsehen wurde den Zuschauern eine Karte Russlands gezeigt in der diese sich langsam rotfärbte. Parallel wurde zum Tragen einer Gasmaske oder zum Bedecken des Mundes aufgefordert.

Das russische Katastrophenministerium erklärte im Anschluss, dass diese falschen Informationen von IT-Angreifern nach der Kompromittierung von Radio- und Fernsehsendern ausgestrahlt wurden. Bei diesem Cyberangriff war nicht nur Moskau betroffen, sondern auch andere Regionen, wie Swerdlowsk und Jekaterinburg. Bereits im Februar 2023 kam es zu vorgetäuschten Luftangriffsalarmen und Raketendrohungen in Russland. Bei der gefälschten Rede im Juni 2023 war von einer angeblichen ukrainischen Invasion die Rede und der Verhängung des Kriegsrechts in den Regionen Kursk, Belgorod und Brjansk /FRA23w01, BSI23r16/.

Kerntechnischer Bezug

Bei dem Cyberangriff im Mai 2023 wurden zwar fingierte Meldungen zu angeblichen nuklearen Angriffen auf russische Gebiete verbreitet, dies hatte allerdings keinen tatsächlichen Hintergrund mit kerntechnischem Bezug. Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.18 Cyberangriff auf russische Webseiten

Übersicht

Am 21.02.2023 wurden zwei russische Medien-Webseiten Opfer eines Cyberangriffes /BSI23r17/.

Beschreibung

Während der Rede von Wladimir Putin im Februar 2023 waren aufgrund eines Cyberangriffs zwei russische Medien-Webseiten nicht erreichbar, darunter die Webseite des staatlichen russischen Fernsehsenders Allrussische staatliche Fernseh- und Radiogesellschaft (WGTRK) und die Webseite der Streaming-Plattform Smotrim.ru. Im Nachgang bekannte sich eine pro-ukrainische Angreifergruppierung, die unter dem Namen IT-Army agiert, zu den DDoS-Angriffen, welche die Kanäle lahmlegten, auf denen die Rede von Wladimir Putin übertragen werden sollten. Durch diesen Cyberangriff fiel die staatliche Internetseite WGTRK aufgrund technischer Arbeiten für einige Zeit aus. Die Streaming-Plattform Smotrim.ru konnte aufgrund des Cyberangriffs nicht geladen werden. Die sich hier bekennende pro-ukrainische Angreifergruppierung besteht aus ukrainischen Technikspezialisten und Hacktivisten. Die Gruppierung hat sich zu Beginn des Ukraine-Krieges gegründet und ist nach eigenen Angaben bereits für

über 15.000 Cyberangriffe auf russische Webseiten verantwortlich, darunter Regierungsstellen, Banken und Privatunternehmen. Laut der russischen Nachrichtenagentur TASS wurde ein Ausfall der Webseiten bestätigt, aber eine Attribuierung wurde in diesem Zusammenhang nicht vorgenommen /BSI23r17/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.19 Cyberangriff auf Infotel

Übersicht

Am 08.06.2023 kam es aufgrund eines Cyberangriffs zu einem Komplettausfall des russischen Providers Infotel /BSI23r18/.

Beschreibung

Im Juni 2023 wurde Infotel, ein russischer Provider, der maßgeblich für die russische Zentralbank ist, Opfer eines Cyberangriffes. Aufgrund des Cyberangriffs kam es zu einem Komplettausfall der Dienste des Providers. Laut einer Meldung des ukrainischen Nachrichtenportals „Economichna Pravda“ und des amerikanischen Internet Outage Detection and Analysis Portals (IODA) der Georgia Tech, wird von einem erfolgreichen Cyberangriff auf den Provider Infotel berichtet. Die IODA bestätigt einen Komplettausfall der Dienste des Providers am 08.06.2023 /BSI23r18/. Laut der Telekommunikationsfirma Infotel wurde der Cyberangriff bestätigt. Die pro-ukrainische Angreifergruppierung Cyber Anarchy Squad hat sich zu diesem Cyberangriff bekannt.

Infotel ist ein Provider für die russische Zentralbank und die Verbindung zwischen den lokalen Banken, Finanzfirmen und Onlinehändlern. Durch den Cyberangriff kam es für die Kunden zu Problemen beim Zugang des Banksystems und der Durchführung von Zahlungen. Zusätzlich gibt Cyber Anarchy Squad an, Zugang zu sensiblen Informationen erlangt zu haben, wie Listen von Kunden und deren E-Mail-Verkehr /OOD23w01/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.20 Cyberangriff auf Dozor-Teleport

Übersicht

Am 29.06.2023 wurde ein Ausfall des Netzwerkes der Dienste des russischen Satelliten-Internetanbieters Dozor-Teleport registriert /BSI23r20/.

Beschreibung

Im Juni 2023 kam es zu einem Ausfall des Netzwerks des russischen Satelliten-Internetanbieters Dozor, dessen Dienste u. a. vom russischen Energieunternehmen Gazprom, sowie von Verteidigungs- und Sicherheitsdiensten genutzt werden. Die IT-Angreifer, die sich zu diesem Cyberangriff bekannt haben, behaupten, mit der russischen Privatarmee Wagner-Gruppe in Verbindung zu stehen. Zudem geben sie an, nicht nur einige Satellitenterminals zum Absturz gebracht zu haben, sondern auch vertrauliche Daten des Providers gestohlen und unbrauchbar gemacht zu haben. Unter den veröffentlichen Daten auf dem Telegram-Kanal der Gruppierung sind Netzwerkpläne, sowie ein Screenshot einer Active-Directory-Management-Konsole und es wurde eine ZIP-Datei mit einer Größe von 150 MB (674 Dateien) zum Download zur Verfügung gestellt /BSI23r20/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.21 WinRaR

Übersicht

Am 29.04.2023 wurde eine nicht näher genannte ukrainische Behörde mit Hilfe von WinRaR angegriffen, um Daten der Behörde durch auf Living-off-the-land-Techniken basierendes Löschen und Überschreiben zu zerstören /BSI23r14/.

Beschreibung

Im April 2023 wurde eine nicht näher genannte ukrainische Behörde Opfer eines Cyberangriffes. Dieser Cyberangriff wird der APT-Gruppierung Sandworm zugeschrieben. Die Angreifer erlangten durch kompromittierte, vermutlich nicht durch Multi-Faktor-Authentifizierung geschützte VPN-Zugänge Zugriff auf kritische Systeme. Danach gelang es ihnen, Daten sowohl auf Linux- als auch auf Windows-Rechnern zu löschen. Je nach Betriebssystem wurden dabei verschiedene Skripte zum Löschen der Dateien eingesetzt. Unter Windows soll eine Version des BAT-Scripts „RoarBat“ und unter Linux unter anderem das Dienstprogramm „dd“ genutzt worden sein. Dadurch wurden die betroffenen Daten gelöscht oder überschrieben und wurden so dauerhaft unbrauchbar gemacht. Aufgrund der eingesetzten Living-off-the-land-Techniken, d. h. der maliziösen Nutzung legitimer, vorhandener Programme, konnte vermutlich eine Erkennung durch vorhandene Sicherheitssoftware umgangen werden. Bereits im Januar 2023 wurde ein ähnlicher Vorfall auf die ukrainische Nachrichtenagentur Ukrinform beobachtet, der ebenfalls der APT-Gruppierung Sandworm zugeschrieben wird /BSI23r14/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.22 Suncor

Übersicht

Ein Cyberangriff auf den kanadischen Mineralölkonzern Suncor beeinträchtigte dessen Transaktionen mit Kunden und Lieferanten. Obwohl offenbar Daten abgegriffen wurden, gibt es derzeit keine Hinweise darauf, dass diese von den Angreifern missbraucht worden sind.

Beschreibung

Auf Kanadas führenden Mineralölkonzern Suncor Energy wurde ein Cyberangriff durchgeführt, wodurch die Transaktionen des Unternehmens mit seinen Kunden und Lieferanten beeinträchtigt wurden /NEW23w01/. Stattgefunden hat der Angriff etwa am 21. Juni 2023 /CYD23w01/. An manchen Tankstellen des Betreibers Petro-Canada,

welcher sich im Besitz von Suncor Energy befindet, waren ausschließlich Barzahlungen möglich bzw. Auto-Waschstraßen nicht nutzbar. Darüber hinaus war die Anmeldung in der Unternehmens-App und im Petro-Point-Programm von Suncor Energy gestört. Im Anschluss an den Angriff hat das Unternehmen seine operativen IT-Systeme und Backup-Datenbanken isoliert /CYD23w01/. Am 25. Juni 2023 hat Suncor Energy eine Pressemitteilung zu dem Cyberangriff veröffentlicht /CPO23w02/. Darin gab das Unternehmen an, es lägen keinerlei Hinweise über das Abgreifen von Kunden-, Lieferanten- oder Mitarbeiterdaten vor. Kurze Zeit später wurde jedoch von Beamten der Diebstahl von Kundenprämiendaten aus dem Petro-Points-Programm bestätigt. In weiterer Folge befindet sich Suncor Energy mit einigen Kunden im Rechtsstreit. Anzeichen, dass die Daten von den Angreifern missbraucht wurden, gibt es jedoch derzeit nicht. Nach eigenen Angaben hat das Unternehmen Gegenmaßnahmen ergriffen und arbeitet mit externen Experten sowohl an der Untersuchung des Vorfalls als auch an der Problemlösung. Suncor Energy hat keine Angaben gemacht, ob bei dem Cyberangriff Ransomware eingesetzt worden ist und gab keine weiteren Details bekannt. In den Tagen nach dem Cyberangriff ist es dem Unternehmen gelungen wieder eine sichere IT-Umgebung aufzubauen /CYD23w01/. Ab dem 29. Juni 2023 waren Kartenzahlungen wieder weitgehend möglich. Einige Sicherheitsexperten vermuten, dass der Cyberangriff von russischen Angreifern durchgeführt wurde, um die kanadische Unterstützung der Verteidigung der Ukraine gegen die russische Invasion zu schwächen. Es wird angenommen, dass der Vorfall Suncor Energy Millionen von Dollar kosten wird. Das Unternehmen tauschte im Anschluss an den Cyberangriff nach und nach alle PCs und Laptops seiner Mitarbeiter aus, um sicherzustellen, dass die Verwendung der Geräte keine Gefahr darstellt. Darüber hinaus riet das Unternehmen seinen Mitarbeitern keine sozialen Medien auf Firmengeräten zu nutzen oder fremde Personen im Aufzug hinter sich miteinsteigen zu lassen. /CBC23w01, CPO23w02, CYD23w01, HEI23w12, YAF23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.23 Angriff auf E-Mail Security Gateway (ESG)-Geräte des Herstellers Barracuda

Übersicht

Durch Ausnutzung einer Zero-Day-Schwachstelle, wurden E-Mail Security Gateway (ESG)-Geräte des Herstellers Barracuda mit Schadsoftware angegriffen. Die Schadsoftware liegt in drei verschiedenen Varianten vor.

Beschreibung

Am 19.05.2023 hat das Unternehmen Barracuda eine Schwachstelle CVE-2023-2868 in einem Modul seiner E-Mail Security Gateway (ESG)-Geräte entdeckt, das die Anhänge in eingehenden E-Mails überprüft. Daraufhin hat das Unternehmen am 20.05.2023 ein erstes weltweites Sicherheitsupdate für alle seine ESG-Geräte veröffentlicht und am 21.05.2023 ein weiteres Update. Am 23.05.2023 informierte Barracuda alle nach dem Kenntnisstand des Unternehmens betroffenen Kunden mithilfe der ESG-Benutzeroberfläche über die Schwachstelle und gab entsprechende Handlungsempfehlungen bekannt. Zusätzlich hat sich das Unternehmen auch direkt an seine Kunden gewendet. /BSI23i06/

Die Schwachstelle wird nachstehend detailliert beschrieben /NVD23i06/:

- **CVE-2023-2868:** Die Schwachstelle betrifft die Remote-Befehlseinschleusung in den Programmversionen 5.1.3.001 bis 9.2.0.006 der ESG-Geräte des Herstellers Barracuda. Sie besteht durch einen Fehler in der umfassenden Bereinigung der Verarbeitung von Dateien mit der Endung *.tar*, bei denen es sich um Bandarchive handelt. Dabei ist die Eingabevalidierung einer vom Benutzer bereitgestellten *.tar*-Datei unvollständig. Infolgedessen kann ein Angreifer aus der Ferne gezielt *.tar*-Dateien auf eine bestimmte Weise formatieren, wodurch er einen Systembefehl mit Berechtigungen des ESG-Geräts ausführen kann. Bedrohungsgrad: kritisch. CVSS:3.1-Score: 9.8.

Barracuda gab bekannt, dass einige seiner ESG-Geräte durch Ausnutzung der Schwachstelle bereits mit Schadsoftware kompromittiert worden sein. Das Unternehmen hat einen entsprechenden Bericht /BAR23w01/ auf seiner Webseite mit Analyseergebnissen und einer Chronik der Ereignisse veröffentlicht. Darin wird angegeben, dass die Ausnutzung der Schwachstelle bereits im Oktober 2022 begonnen hatte und dass drei

verschiedene Varianten der Schadsoftware die Schwachstelle verwenden würden, um den E-Mailverkehr zu überwachen. Einige der Schadsoftwarevarianten etablieren eine Backdoor auf den kompromittierten Geräten, um eine persistente Verbindung herzustellen. Die U.S. Cybersecurity and Infrastructure Security Agency (CISA) hat am 28.07.2023 einen Analysebericht /CIS23i05/ über die drei Schadsoftwarevarianten veröffentlicht. Demnach wird die Schadsoftware über den Anhang einer Phishing-E-Mail verteilt. Nach ihrer Installation auf dem ESG-Gerät nutzt die Schadsoftware die Schwachstelle CVE-2023-2868 aus, um eine Reverse-Shell-Backdoor auf das ESG-Gerät zu laden, die einen Kommunikationskanal mit dem Command-and-Control-Server (C&C) der Angreifer aufbaut. Von diesem wird dann eine zusätzliche Backdoor auf das ESG-Gerät geladen. Nach den Angaben im CISA-Analysebericht /CIS23i05/ existieren sechs verschiedene Backdoors, die als zusätzliche Backdoor eingesetzt werden können. Die Backdoors werden nachstehend beschrieben. /BAR23w01, BSI23i06, BSI23i08, CIS23i05/

- **SEASPY:** Es handelt sich um eine persistente, passive Backdoor, die sich als legitimer Barracuda-Dienst tarnt. Die Backdoor überwacht den Datenverkehr mit dem C&C-Server der Angreifer. Erfasst sie dabei die richtige Paketsequenz, richtet sie eine Transmission Control Protocol (TCP)-Reverse-Shell ein, die mit dem C&C-Server verbunden ist. Die Shell ermöglicht den Angreifern die Ausführung von beliebigen Befehlen auf dem ESG-Gerät.

- **SUBMARINE:** Dies ist eine persistente Backdoor, die sich in der SQL-Datenbank des Systems einnistet und den Angreifern die vollständige Systemkontrolle ermöglicht. Sie verschafft ihnen zusätzliche Privilegien sowie Möglichkeiten zur lateralen Bewegung im Netzwerk und zur Bereinigung.

- **WHIRLPOOL:** Die Backdoor etabliert eine Transmission Control Protocol (TCP)-Reverse-Shell, die eine Verbindung mit dem C&C-Server der Angreifer aufbaut.

- **SKIPJACK:** Es handelt sich um eine Backdoor, die Informationen zum Dateisystem auflistet.

- **SEASPRAY:** Diese Backdoor registriert einen Event-Handler für alle eingehenden E-Mail-Anhänge und startet die bereits oben beschriebene WHIRLPOOL-Backdoor.

- **SALTWATER:** Über die Backdoor wird mithilfe des TLS-Protokolls eine Netzwerkkommunikation aufgebaut und es können beliebige Benutzerschnittstellen-Befehle ausgeführt werden.

Das IT-Sicherheitsunternehmen Mandiant hat die Backdoor WHIRLPOOL im Juni 2023 entdeckt und ordnet sie der chinesischen APT-Gruppierung UNC4841 zu. Mandiant veröffentlichte am 29.08.2023 eine ausführliche Analyse /MAN23w02/ zu den Tätigkeiten von UNC4841 in Zusammenhang mit der Schwachstelle CVE-2023-2868, die den Zeitraum vom Oktober 2022 bis Juni 2023 umfasst. Dabei wird deutlich, dass die APT-Gruppierung ihre Angriffstaktik an die jeweiligen, durch das Unternehmen Barracuda veröffentlichten, Informationen anpasste. Von UNC4841 wurden weltweit ESG-Geräte kompromittiert. Jedoch richtet sich der Schwerpunkt der Angriffe gegen Organisationen in den USA und Kanada. Betroffen von den Angriffen sind nationale Regierungen, High-Tech- und Informationstechnologieunternehmen, lokale Regierungen, Telekommunikationsanbieter, Produktionsunternehmen sowie Hochschulen und Universitäten. /BSI23i09, BSI23i10, MAN23w02/

Barracuda rät seinen Kunden ihre Logdateien mithilfe der vom Unternehmen veröffentlichten Indicators of Compromise (IoC) auf eine mögliche Kompromittierung hin zu überprüfen. Jedoch weist das Unternehmen darauf hin, dass sich seine Untersuchungen nur auf seine ESG-Produkte beschränken. Betroffene Kunden sollten daher ihre spezifische Systemumgebung auf mögliche weitere Kompromittierungen überprüfen. Die CISA hat in ihrem Analysebericht /CIS23i05/ zusätzliche IoCs veröffentlicht, die sie am 09.08.2023 ergänzte /CIS23i06/. Am 06.06.2023 wurden die Handlungsempfehlungen von Barracuda aktualisiert. Demnach reicht die Installation der Sicherheitsupdates nicht aus, sodass alle betroffenen ESG-Geräte unverzüglich ersetzt werden müssen. Kunden, die ihre Geräte noch nicht ausgetauscht haben, sollen sich mit dem Hersteller in Verbindung setzen. /BAR23w01, BSI23i06, BSI23i07, BSI23i09/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.24 Cyberangriff mittels Social Engineering unter Verwendung von Videomaterial

Übersicht

Im Jahr 2023 wurde ein IT-Sicherheitsvorfall bekannt, bei dem Mitarbeiter eines deutscher KRITIS Betreiber über Social Engineering zur Freigabe von Finanzmitteln gebracht werden sollten. Das Besondere an diesem Social Engineering Angriff war die Verwendung von authentischem Videomaterial.

Beschreibung

Der Cyberangriff betraf lauf BSI /BSI23r07/ ein Unternehmen aus dem Sektor Energie. Das offensichtliche Ziel des Cyberangriffs bestand darin, entsprechend verantwortliche Mitarbeiter des betroffenen Unternehmens zu täuschen und zur Freigabe von nicht legitimen Zahlungen zu verleiten. Die Angreifer gingen bei diesem Social Engineering Angriff mehrschrittig vor. Zunächst einmal war den Angreifern offenbar bekannt, welche Mitarbeiter zur Freigabe von Zahlungen berechtigt sind, was auf entsprechende Angriffsschritte zur Informationsgewinnung schließen lässt. Wie genau diese allerersten Angriffsschritte aussahen ist derzeit nicht bekannt. Die ermittelten verantwortlichen Mitarbeiter wurden anschließend gezielt zu einer manipulierten Videokonferenz eingeladen. Während dieser Videokonferenz wurde den Mitarbeitern ein Video des Geschäftsführers gezeigt. Hierbei handelte es sich um legitimes, in einem anderen Zusammenhang erstelltes Videomaterial. Wie die Angreifer an dieses Videomaterial gelangten, ist derzeit nicht bekannt. Nach Abspielen des Videos wurden die Teilnehmer der Videokonferenz aufgrund angeblicher Soundprobleme dazu aufgefordert, einem WhatsApp-Chat beizutreten, um die Besprechung über eine anstehende Information fortzusetzen. An dieser Stelle wurden die Mitarbeiter nach Informationen des BSI misstrauisch und brachen den Kontakt ab.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.25 Cyberangriffe auf japanische Verteidigungsnetzwerke und auf die japanische Cybersicherheitsbehörde

Übersicht

Im August 2023 wurden Informationen aus dem Jahr 2020 über einen mutmaßlich chinesischen Cyberangriff auf japanische Verteidigungsnetzwerke bekannt /BSI, WP etc./. Wenige Tage zuvor hatte die japanische Cybersicherheitsbehörde NISC (National Center of Incident Readiness and Strategy for Cybersecurity) einen Datenabfluss aus den eigenen Netzwerken bekannt gegeben /NISC; BSI; FT/.

Beschreibung

Den vorliegenden Informationen zufolge wurde die NSA im Herbst 2020 auf einen Cyberangriff aufmerksam, der auf das Ausspionieren höchst sensitiver Informationen des japanischen Verteidigungsapparates ausgerichtet war. Dem in der Washington Post am 7.8.2023 veröffentlichten Bericht zufolge, hatten die Angreifer weitreichenden und persistenten Zugang zu militärischen Informationen wie Plänen, Fähigkeiten und Bewertungen von Unzulänglichkeiten und Schwachstellen. Der Angriff wird staatlich gesponsorten chinesischen Angreifern zugeschrieben. Unklar bleibt jedoch, ob und wann der Zugriff der chinesischen Angreifer auf die japanischen Verteidigungsnetzwerke unterbunden wurde. Der Bericht der Washington Post stützt sich dabei auf Aussagen früherer US-amerikanischer und auch japanischer Beamter, welche den Angriff als weitreichend und persistent beschreiben. Die japanische Regierung hat diese Aussagen bislang nicht offiziell bestätigt.

Den zweiten Vorfall gab die japanische Cybersicherheitsbehörde NISC selbst am 4.8.2023 bekannt. Aus der entsprechenden Meldung geht hervor, dass die Angreifer ab Anfang Oktober 2022 Zugriff auf die Systeme der NISC hatten. Entdeckt wurde der Angriff jedoch erst im Juni 2023, als „Spuren unbefugter Kommunikation im Zusammenhang mit E-Mail-Systemen“ aufgefunden wurden. Es wurde eingeräumt, dass Daten möglicherweise nach außen gesickert sind. Das Ausmaß des Datenabflusses in diesem neunmonatigen Zeitraum wurde in der Meldung des NISC jedoch nicht thematisiert. Japan hat inzwischen die finanziellen Ausgaben im Bereich Cybersicherheit deutlich erhöht – im Bericht der Washington Post ist von einer Verzehnfachung die Rede – und eine Aufstockung des militärischen Personals zur Cyberabwehr um den Faktor vier angekündigt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.26 Volt Typhoon – Cyberangriffe auf kritische Infrastrukturen in den USA

Übersicht

Ende Mai 2023 warnte das IT-Unternehmen Microsoft vor einer Cyber-Spionagekampagne mit dem Ziel der Ausspähung kritischer Infrastrukturen in den USA. Diese Cyberangriffe werden einer chinesischen, staatlich geförderten APT-Gruppierung zugeschrieben, die unter dem Namen Volt Typhoon bekannt ist. Das besondere an den Cyberangriffen von Volt Typhoon ist der deutliche Fokus auf der Verschleierung der Angriffshandlungen und der fast ausschließliche Einsatz von Living-off-the-Land Techniken.

Beschreibung

Laut dem Beitrag von Microsoft ist die APT-Gruppierung Volt Typhoon, die offenbar einen chinesischen Hintergrund hat und mutmaßlich vom chinesischen Staat gefördert wird, bereits seit 2021 aktiv. Ziele waren kritische Infrastrukturen in den USA, unter anderem in den Bereichen Kommunikation, Transport, Herstellung und IT. Als konkrete Angriffsziele werden beispielsweise militärnahe Einrichtungen auf der Pazifikinsel Guam genannt, auf der sich ein wichtiger US-Luftwaffenstützpunkt befindet. China wies die Berichte als unwahr zurück.

Microsoft leitet aus dem beobachteten Vorgehen der Angreifer ab, dass das Ziel zunächst eine langfristige, verdeckte Spionageoperation sei. Darüber hinaus spricht Microsoft vom Aufbau von Kapazitäten für weitergehende Angriffsschritte wie beispielsweise der Sabotage von kritischer Kommunikationsinfrastruktur zwischen den USA und Asien. Hierfür werden in den vorliegenden Informationen keine konkreten technischen Belege genannt, dennoch erscheint es sowohl angesichts zahlreicher historischer Beispiele zur Sabotage von Kommunikationsinfrastruktur in Krisenfällen als auch vor dem Hintergrund des politischen Spannungsfeldes zwischen den USA und China nicht unplausibel, dass ein solches Vorgehen in chinesischem Interesse liegen könnte.

Den vorliegenden Informationen zufolge legt Volt Typhoon großen Wert auf die Verschleierung der eigenen Aktivitäten, um langfristig unentdeckten Zugriff auf die kompromittierten Systeme zu behalten. Hierbei greift die Gruppierung fast ausschließlich auf den Einsatz von Living-off-the-Land Techniken und Hands-on-keyboard Aktivitäten zurück. Living-off-the-land bezeichnet hierbei ein Angreiferverhalten, bei dem die Angreifer auf Dateien, Skripte, Werkzeuge und Informationen zurückgegriffen wird, die auf dem angegriffenen System bereits vorhanden sind, und diese maliziös einsetzen. Es werden also auf dem angegriffenen System legitim vorhandene Tools zweckentfremdet und von den Angreifern für ihre eigenen Ziele eingesetzt. Auf diese Weise wird häufig das Einbringen von Angriffswerkzeugen oder Schadsoftwarekomponenten von außen umgangen und damit die Detektion der Angreiferhandlungen signifikant erschwert.

Als konkrete System-Tools, die Volt Typhoon bei seinen Angriffen zweckentfremdete, werden beispielsweise PowerShell, wmic, ntdsutil und netsh genannt. Als Einfallstor für die Angriffe nennt Microsoft Fortigate-Lösungen von Fortinet. Auch nutzen die Angreifer Netzwerkkomponenten verschiedener Firmen, wie beispielsweise ASUS, Cisco, Netgear und anderen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.27 Swift Slicer – Cyberangriffe auf Ziele in der Ukraine

Übersicht

Im Januar 2023 veröffentlichten IT-Sicherheitsforscher von ESET Erkenntnisse zu einer neuen Schadsoftware. Bei der Schadsoftware, die ESET der APT-Gruppierung Sandworm zuschreibt, handelt es sich um einen Wiper, also eine Schadsoftware, die Daten auf angegriffenen Systemen durch gezieltes Löschen und Überschreiben dauerhaft unbrauchbar macht.

Beschreibung

Den Erkenntnissen von ESET zufolge wurde die Schadsoftware über die Group Policy des zuvor kompromittierten Active Directory der angegriffenen Organisation eingesetzt. Solch eine Group Policy erlaubt es den Administratoren der Windows Domains, Befehle oder Skripte auf allen Geräten im betroffenen Windows-Netzwerk auszuführen. Kommt die Schadsoftware zur Ausführung, überschreibt sie gezielt für das Windows-Betriebssystem zentrale Dateien mit zufällig generierten Datenblöcken. Dass Swift Slicer dabei insbesondere Dateien im Ordner %CSIDL_SYSTEM_DRIVE%\Windows\NTDS angreift, zeigt an, dass die Schadsoftware nicht nur auf die Zerstörung von Dateien ausgerichtet ist, sondern auf das Lahmlegen ganzer Windows Domains.

Swift Slicer ist in Go programmiert. Diese Programmiersprache wird bei IT-Angreifern immer beliebter, da sie insbesondere was die Einsetzbarkeit auf verschiedensten Plattformen und für verschiedenste Hardware betrifft sehr flexibel ist.

ESET rechnet die Schadsoftwarekomponente Swift Slicer der russischen APT-Gruppierung Sandworm zu, die als Teil des Main Center for Special Technologies (GTsST) für den russischen Militärgeheimdienst GRU arbeitet.

Wiper wie SwiftSlicer werden seit Beginn des russisch-ukrainischen Krieges vermehrt von russischer Seite gegen Ziele in der Ukraine eingesetzt. Zu den weiteren in diesem Zusammenhang beobachteten Wiper-Schadsoftwarekomponenten zählen beispielsweise auch DoubleZero, HermeticWiper, IsaacWiper, WhisperKill, WhisperGate (Abschnitt B.14.1) und AcidRain (Abschnitt B.14.2).

Da im Moment nicht bekannt ist, bei welcher Organisation Swift Slicer entdeckt wurde, und genauso wenig bekannt ist, wie stark die Schadsoftware zwischenzeitlich bei weiteren Organisationen eingesetzt wurde, kann über die Verbreitung der Schadsoftware derzeit keine belastbare Aussage getroffen werden. Klar hingegen ist, dass die Schadsoftware bei einer Organisation in der Ukraine entdeckt wurde und von den IT-Sicherheitsforschern eindeutig als weiteres Angriffswerkzeug im russisch-ukrainischen Spannungsfeld beschrieben wird.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.28 CaddyWiper – Cyberangriff auf Ukrinform

Übersicht

Am 18.01.2023 gab das SSSCIP (State Service of Special Communication and Information Protection) der Ukraine einen Cyberangriff auf die nationale Nachrichtenagentur der Ukraine, Ukrinform, bekannt. Das Computer Emergency and Response Team der Ukraine (CERT-UA) brachte die dabei eingesetzte Schadsoftware mit der APT-Gruppierung Sandworm in Verbindung.

Beschreibung

Nach Aussage des SSSCIP wurde der Angriff auf Ukrinform zügig entdeckt und so in seinen Auswirkungen beschränkt. Den vorliegenden Informationen zufolge hatte der Angriff einen „destruktiven Effekt auf Teile der Informationsinfrastruktur“ von Ukrinform, die Nachrichtenagentur konnte den Betrieb aber aufrechterhalten und durchgehend Informationen über die Situation in der Ukraine für die Bevölkerung und weitere interessierte Kreise zur Verfügung stellen.

Eingesetzt wurde bei den beobachteten Angriff eine Wiper-Schadsoftware mit Namen CaddyWiper. Diese Schadsoftware wurde über eine Windows AD Group Policy ausgeführt, was zeigt, dass die Angreifer die Netzwerke von Ukrinform bereits zuvor kompromittiert hatten. Die APT Gruppierung Sandworm hatte die Schadsoftware CaddyWiper bereits früher im Rahmen von Cyberangriffen auf ukrainische Ziele eingesetzt. Hierzu zählt auch der Cyberangriff mit Industroyer-2 im April 2022 auf das ukrainische Stromnetz (Abschnitt B.14.5). Dabei wurde CaddyWiper eingesetzt, um Spuren der Industroyer-2 Schadsoftware zu verwischen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.29 Infamous Chisel – Cyberangriff auf Ziele in der Ukraine

Übersicht

Im August 2023 veröffentlichten Sicherheitsbehörden der Five-Eyes-Staaten USA, Großbritannien, Kanada, Australien und Neuseeland einen gemeinsamen Schadsoftware Analyse Report zu einer Toolbox aus Schadsoftwarekomponenten unter dem Namen Infamous Chisel. Diese Schadsoftwarekomponenten haben offenbar Angriffe auf Android-Mobilfunkgeräte, die vom ukrainischen Militär genutzt werden, zum Ziel. Infamous Chisel wird der russischen APT-Gruppierung Sandworm zugerechnet.

Beschreibung

In einem gemeinsamen Schadsoftware Analyse Report zu Infamous Chisel der US-Cybersicherheitsbehörde (CISA), der US-Sicherheitsbehörde (NSA), der amerikanischen Bundespolizei (FBI), des Neuseeland Cyber Security Centre (NCSC-NZ), des kanadischen Zentrum für Cybersicherheit (CCCS) und des australischen Geheimdienstes (ASD) wird die Schadsoftware Infamous Chisel beschrieben.

Infamous Chisel besteht aus einer Reihe von Schadsoftwarekomponenten, die insgesamt einen persistenten, langfristigen Remote-Zugriff auf kompromittierte Android-Geräte über das Tor-Netzwerk und SSH ermöglicht. Zudem ist mit Infamous Chisel ein periodisch erfolgendes Sammeln und Ausschleusen von Daten von den kompromittierten Geräten möglich. Hierbei werden die vorhandenen Dateien mit einer Liste von aus Angreifersicht interessanten Dateiendungen abgeglichen, bevor sie exfiltriert werden. Hierbei stehen vor allem Systeminformationen sowie Informationen zu kommerziellen Anwendungen, aber auch zu Anwendungen, die spezifisch für das ukrainische Militär sind, im Fokus. Das lokale Netzwerk wird ebenfalls periodisch gescannt, wobei Informationen zu aktiven Hosts und offenen Ports im Vordergrund stehen. Exfiltrierte Informationen werden von Infamous Chisel laut den Analysten mindestens einmal täglich an russische Server gesendet.

Weitere Schadsoftwarekomponenten, die mit unter Infamous Chisel zusammengefasst werden, ermöglichen es den Angreifern, den Netzwerkverkehr zu überwachen und mitzuschneiden, einen Zugriff über SSH zu erlangen und per scp Dateien zu übertragen. Eine wichtige Rolle für die Persistenz spielt hierbei der Austausch der legitimen Systemkomponente netd durch eine maliziöse Version. Diese maliziöse Version sorgt

beispielsweise bei jedem Neustart eines kompromittierten Geräts dafür, dass Infamous Chisel ausgeführt wird. Indem sie darüber hinaus für das Ausspähen und Ausschleusen wesentlicher Informationen von den kompromittierten Geräten verantwortlich ist, dient die maliziöse netd als zentrale Schadsoftwarekomponente von Infamous Chisel.

Folgende Komponenten von Infamous Chisel sind gemäß CISA bislang bekannt:

- netd – Maliziöse Version der legitimen Systemkomponente netd zur automatisierten Erfassung, Sammlung und Ausschleusung von Informationen über das kompromittierte Gerät.
- killer – Schadsoftwarekomponente zum Beenden des netd Prozesses.
- blob – Schadsoftwarekomponente, die von netd ausgeführt wird und für die Konfiguration und Ausführung des Tor-Dienstes td verantwortlich ist.
- td – Tor-Dienst ohne offensichtliche Änderungen. Tor (the onion router) erlaubt die anonyme Kommunikation über das Internet.
- tcpdump – tcpdump ebenfalls ohne offensichtliche Änderungen. tcpdump erlaubt das Abfangen und die Analyse von Netzwerkverkehr.
- ndbr_armv7 und ndbr_i686 – Hierbei handelt es sich um Multi-call binaries, also ausführbare Dateien, welche in Abhängigkeit von den Parametern, mit denen sie aufgerufen werden, die Funktionen von einer ganzen Reihe von Diensten ausführen können. Genannt werden in diesem Zusammenhang dropbear (SSH client mit modifizierter Authentifizierungsfunktion), dropbearkey (zur Generierung von SSH keys), ssh (secure shell Netzwerkprotokoll), scp (secure copy Protokoll), nmap (Network Scanning and Mapping), dbclient, watchdog (zur Überwachung von Aktivitäten im Dateisystem; Watchdog stellt das setup bereit und führt dropbear aus), rmflag (zur Entfernung der flag-Datei), mkflag (zum Erzeugen von Dateien).
- Db – Hierbei handelt es sich ebenfalls um eine Multi-call binary. Genannt werden hier dropbear, dropbearkey, ssh, scp, nmap, dbclient, watchdog, rmflag und mkflag.

Die CISA hebt in ihrer Analyse der Schadsoftwarekomponenten insbesondere auf den Ersatz der legitimen nmap Datei sowie die Modifikation der Authentifizierungsfunktion, die von Komponenten wie dropbear genutzt werden, hervor. Insgesamt schätzt die CISA die Komplexität von Infamous Chisel allerdings auf gering bis mittel ein und weist in ihrer Analyse der Schadsoftwarekomponenten darauf hin, dass bei der Entwicklung von

Infamous Chisel offensichtlich nur wenig Wert auf die Umgehung von Sicherungsmaßnahmen und die Verschleierung von Angreiferaktivitäten gelegt wurde. Die CISA äußert hierbei die Vermutung, dass die Entwickler eine Verschleierung der Aktivitäten als nicht notwendig betrachteten, da Android Geräte in der Regel nicht über ein Detektionssystem verfügen. Trotz des Mangels an Verschleierungsaufwand warnt die CISA jedoch, dass die Schadsoftwarekomponenten von Infamous Chisel eine ernsthafte Bedrohung darstellen, insbesondere im Hinblick auf den potenziellen Impact der mit Infamous Chisel gesammelten und exfiltrierten Informationen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.30 Cyberangriff auf Adesso

Übersicht

Im Frühjahr 2023 wurde bekannt, dass der deutsche IT-Dienstleister Adesso, zu deren Kundenkreis neben Behörden der Bundes-, Landes- und Kommunalverwaltung (z. B. das BKA und die Bundesbank) auch Betreiber kritischer Infrastrukturen wie beispielsweise die Energieversorgungskonzerne RWE und Eon gehören, Opfer eines Cyberangriffs wurde, wobei im Wesentlichen durch die Angreifer Informationen eingesehen und Daten heruntergeladen wurden. Das BSI hat am 09.03.2023 zu diesem IT-Sicherheitsvorfall eine Cyber-Sicherheitswarnung veröffentlicht. Aus dieser Meldung sowie den eigenen Angaben von Adesso geht hervor, dass sich die Angreifer bereits Monate vor der Entdeckung und möglicherweise über Monate hinweg unerkannt im Netzwerk befanden und somit Zugriff u. a. über VPN-Verbindungen auch auf die Netzwerke der Kunden von Adesso hatten. /ADE23w01, BSI23r19/

Beschreibung

Der Cyberangriff auf Adesso begann mutmaßlich bereits im Mai 2022, wobei die Angreifer eine Schwachstelle bzw. einen Zero-Day-Exploit in der vom Unternehmen Atlassian entwickelten Dokumentationssoftware Confluence ausnutzten, welche von Adesso eingesetzt wird. Die Angreifer erlangten somit initialen Zugriff auf das Netzwerk von Adesso über deren Lieferkette, bevor weitere Angriffsschritte durchgeführt wurden und ggf. weiterführende Cyberangriffe auf Kunden von Adesso ausgeführt wurde.

Zu den Auswirkungen des Angriffs liegen nur begrenzt Informationen vor. Adesso selbst bestätigt, dass Angreifer Zugriff auf Informationen hatten und Daten exfiltriert wurden, wobei keine Angaben zu genaueren Inhalten oder betroffenen Kunden gemacht wurden /ADE23w01/. Die Angreifer waren dabei nach derzeitigen Erkenntnissen bemüht, eine Aufdeckung ihrer Aktivitäten zu vermeiden. Um nicht entdeckt zu werden verwischten sie ihre Spuren und hinterließen beispielsweise keine auffällige Schadsoftware, agierten zu deutschen Bürozeiten und nutzten als Kontrollserver Systeme mit deutschen IP-Adressen. Nach Informationen des BSI kompromittierten die Angreifer bestehende administrative Zugänge, richteten darüber hinaus zusätzliche administrative Zugänge ein (teilweise unter Beachtung bestehender Namenskonventionen) und nutzten spezifische und generische Angriffswerkzeuge wie beispielsweise Mimikatz. Informationen über den IT-Sicherheitsvorfall wurden dem BSI und einigen Medien am 19. Januar 2023 durch einen Whistleblower übermittelt, nachdem Adesso nach eigenen Angaben am 11. Januar 2023 von dem Angriff erfahren hat. Anfang Februar 2023 erfuhren die Kunden von Adesso von dem Vorfall, nachdem verschiedene Medien und Adesso selbst darüber berichteten. /ADE23w01, BSI23r19, INS23w01, HEI23w13, SUD23r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor, dieser kann zukünftig jedoch nicht ausgeschlossen werden.

B.15.31 CosmicBeetle

Übersicht

Am 22. August 2023 veröffentlichten Forscher des slowakischen Unternehmens für Sicherheitssoftware ESET Informationen über Ransomware-Angriffe durch die Gruppierung „CosmicBeetle“. Die Gruppierung greift im Rahmen einer mindestens seit Mai 2020 bis heute andauernden Kampagne Webserver weltweit in verschiedenen Bereichen unter anderem mit Hilfe der Ransomware „Scarab“ an. /ESE23w01/ Zu den Angriffszielen, die nach Informationen von ESET keinem spezifischen Muster folgen, zählen unter anderem ein Krankenhaus, eine polnische Regierungsbehörde, eine Schule in Mexico sowie ein im Umweltbereich tätiges Unternehmen in der Türkei. Insgesamt sind neben den o. g. Zielen insbesondere Länder der EU, wie beispielsweise Spanien, Frankreich, Belgien oder Ungarn, betroffen.

Die Angreifer verschaffen sich im Rahmen der Angriffe die notwendigen Zugriffsmöglichkeiten durch Ausnutzung der Zerologon-Schwachstelle (siehe Abschnitt A.3.3) und durch Brute-Force-Angriffe für Remote-Desktop-Zugangsdaten. ESET geht aufgrund zahlreicher türkischer Zeichenfolgen in analysierten Codeelementen davon aus, dass es sich um eine türkischstämmige Gruppierung handelt. /ESE23w01, ZDN23w02/

Beschreibung

Die Forscher von ESET beschreiben in ihrem Blogeintrag zu CosmicBeetle das Toolset Spacecolon, welches von der Gruppierung verwendet wird, um die bei den Cyberangriffen eingesetzte Ransomware zu verbreiten und die Cyberangriffe durchzuführen. Das Set besteht dabei aus drei Komponenten, die aufeinander aufbauend eingesetzt werden, um eine Backdoor zu etablieren, über die die Angreifer beliebige Befehle ausführen, sowie Schadsoftwarekomponenten herunterladen, Informationen sammeln und entsprechende Payloads platzieren können. Neben den von CosmicBeetle selbst erstellten Komponenten des Toolsets werden außerdem diverse Third-Party-Werkzeuge verwendet, bei denen es sich sowohl um einschlägige breit verfügbare Schadsoftwares als auch um legitime Werkzeuge handelt. Im Wesentlichen dienen die ersten Angriffsschritte dazu, das angegriffene System mit Ransomware zu verschlüsseln. Von ESET wurde in diesem Zusammenhang der Einsatz der Ransomware „Scarab“ sowie seit kurzem auch einer neu entwickelten Ransomware beobachtet. Die eingesetzte Ransomware beinhaltet dabei außerdem Schadsoftware vom Typ „ClipBanker“, welche unter anderem die Zwischenablage überwacht und darüber finanzielle Transaktionen beispielsweise über Kryptowährungen beeinflussen kann. /ESE23w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor, dieser kann zukünftig jedoch nicht ausgeschlossen werden.

B.15.32 Cyberangriff der Hackergruppierung Anonymous auf Websites der japanischen Regierung

Übersicht

Nachdem sich die japanische Regierung entschieden hat, aufbereitetes Wasser aus den zerstörten Teilen des Kernkraftwerks Fukushima Daiichi in das angrenzende Meer abzuleiten und die Internationale Atomenergie-Organisation (IAEA) Anfang Juli 2023 einen Bericht veröffentlichte, demzufolge dieses Vorgehen vertretbar ist /HEI23w03/, hat die Hackergruppierung Anonymous als Protestaktion mehrere Websites im Zusammenhang mit dem japanischen Atomprogramm angegriffen. Insgesamt wurden insbesondere mehrere Websites der japanische Atomenergiebehörde, der Japan Atomic Power Company und der Atomic Energy Society of Japan im Rahmen einer Distributed Denial-of-Service-Kampagne angegriffen. Nach Anhaben der japanischen Atomenergiebehörde wurden die Auswirkungen für Nutzer mit Hilfe ergriffener Gegenmaßnahmen begrenzt. /HEI23w02, KYO23w01/

Beschreibung

Infolge des durch ein Erdbeben vor der japanischen Küste ausgelösten Tsunamis im März 2011 kam es in mehreren Blöcken des Kernkraftwerks Fukushima Daiichi zu weitreichenden Beschädigungen einschließlich des Reaktorkerns. Eingeleitete Maßnahmen des Betreibers zur Begrenzung der Unfallfolgen umfassten unter anderem eine provisorische Bespeisung mit Wasser zur Kühlung, da entsprechende Systeme der Anlage aufgrund der durch den Tsunami hervorgerufenen Schäden nicht zur Verfügung standen. Seit dem Ereignis befindet sich zur Kühlung der Reaktoren verwendetes Wasser in Tanks auf dem Anlagengelände, welches einer Entscheidung der japanischen Regierung entsprechend seit dem 24. August 2023 nach einer Aufbereitung kontrolliert ins angrenzende Meer geleitet wird. Die Hackergruppierung Anonymous hat hierzu Bedenken aufgrund residualer Spuren von Radionukliden in diesem Wasser, beispielsweise von Tritium geäußert, und Protestaktionen diesbezüglich angekündigt und durchgeführt. /HEI23w02, KYO23w01/

Es handelt sich bei Anonymous um ein Kollektiv aus internationalen Mitgliedern ohne feste Hierarchien in Form einer dezentralen Gruppierung, welches Hacktivismus (Hacking und Aktivismus) betreibt, um ideologische und politische Ziele zu verdeutlichen und durchzusetzen.

Die Gruppierung setzt dabei unter anderem Hacking-Tools für Protest- und/oder Propagandazwecke ein. Die Aktionen bestehen üblicherweise aus Cyberangriffen auf Zielsysteme, bei denen unter anderem Informationen gestohlen und ggf. veröffentlicht werden, generell die Kontrolle über Systeme übernommen wird oder Distributed-Denial-of-Service-Angriffe ausgeführt werden. Bisherige Operationen umfassen beispielsweise verschiedene Cyberangriffe auf russische Unternehmen, Medien und Regierungseinrichtungen in Folge des russischen Angriffs auf die Ukraine.

Nachdem die japanische Regierung im Jahr 2021 formal beschlossen hat, das aufbereitete Wasser ins Meer zu leiten, veröffentlichte Anonymous eine Liste mit Angriffszielen, die unter anderem die japanische Atomenergiebehörde, die Japan Atomic Power Company, die Atomic Energy Society of Japan, das Ministerium für Wirtschaft, Handel und die Industrie, den japanischen Energieversorger und Betreiber TEPCO sowie die japanische liberaldemokratische Partei umfasst. Cyberangriffe wurden insbesondere seit der Veröffentlichung des IAEA-Berichts und dem Beginn der Ableitung des aufbereiteten Wassers intensiviert durchgeführt und zielten vor allem auf die japanische Atomenergiebehörde, die Japan Atomic Power Company und die Atomic Energy Society of Japan ab. Es handelte sich dabei um Distributed-Denial-of-Service-Angriffe, bei denen das Ziel durch eine Vielzahl Anfragen von unterschiedlichen Quellen überlastet und somit die Verfügbarkeit beeinträchtigt werden soll. Die japanische Atomenergiebehörde berichtet von einem etwa 100-fachen Netzwerkverkehr ihrer auf ihren Websites, wobei die Auswirkungen für Nutzer aufgrund ergriffener Gegenmaßnahmen begrenzt wurden. Japanische IT-Sicherheitsexperten beobachten die Lage fortwährend, da ggf. im Laufe des Prozesses des Ablassens des aufbereiteten Wassers weitere bzw. umfangreichere Cyberangriffe erfolgen könnten. /HEI23w02, HEI23w03, KYO23w01/

Kerntechnischer Bezug

Die Cyberangriffe durch die Gruppierung Anonymous im Zusammenhang mit der Ableitung des aufbereiteten Wassers aus dem Kernkraftwerk Fukushima Daiichi ins Meer zielten auf Organisationen ab, die mit der Atomenergie in Japan in Zusammenhang stehen. Grundsätzlich können auch deutsche Behörden, Betreiber kritischer Infrastrukturen oder sonstige Institutionen mit kerntechnischem Bezug potenziell Angriffsziele derartiger Gruppierungen werden, jedoch gibt es aktuell hierzu keine Anhaltspunkte, da insbesondere keine direkten Verbindungen zu den Ereignissen im Zusammenhang mit dem Kernkraftwerk Fukushima Daiichi bestehen.

B.15.33 Cyberangriffe durch Kimsuky im Zusammenhang mit südkoreanischer Militärübung

Übersicht

Im August 2023 veröffentlichte eine südkoreanische Polizeibehörde Informationen über Cyberangriffe im Zusammenhang mit einer für Ende August 2023 geplanten gemeinsamen Militärübung der Vereinigten Staaten von Amerika und Südkorea. Demzufolge startete die nordkoreanische APT-Gruppierung Kimsuky (siehe Abschnitt 2.10.8) eine breit angelegte (Spear)Phishing-Kampagne gegenüber Auftragnehmern, die im Zusammenhang mit der Militärübung stehen. Angaben der südkoreanischen Polizei zu Folge wurden keine militärischen Informationen gestohlen.

Beschreibung

Für den 21. August 2023 wurde von den USA und der Republik Korea (Südkorea) der Beginn einer jährlich stattfindenden, elf Tage andauernden gemeinsamen Militärübung (Ulchi Freedom Shield 23) angesichts der insbesondere von der Demokratischen Volksrepublik Korea (Nordkorea) ausgehenden Bedrohungslage angekündigt. Südkoreanische Auftragnehmer, die im Zusammenhang mit dem Zentrum für kombinierte Militärübungen zwischen Südkorea und den USA stehen, erhielten im Rahmen einer (Spear)Phishing-Kampagne nach Angaben der Polizeibehörde der Provinz Gyeonggi Nambu in Südkorea maliziöse E-Mails. Eine von der südkoreanischen Polizei und dem U.S. Militär durchgeführte gemeinsame Untersuchung führte zu der Erkenntnis, dass dabei IP-Adressen verwendet wurden, die bereits im Jahr 2014 bei einem Cyberangriff auf ein südkoreanisches Kernkraftwerk (siehe Abschnitt B.6.1) verwendet wurden. Dieser IT-Sicherheitsvorfall wurde der mit Nordkorea in Verbindung stehenden APT-Gruppierung Kimsuky zugeschrieben. Diese Gruppierung ist unter anderem für umfangreiche (Spear)Phishing-Kampagnen bekannt, mit denen Passwörter beschafft oder Schadsoftwarekomponenten verteilt werden sollen. /REU23w01/

Die Ermittlungen ergaben, dass der Cyberangriff bereits im April 2022 begann, als Kimsuky maliziöse E-Mails an Mitarbeiter einer Organisation zur Kriegssimulation in Südkorea schickte. Im Januar 2023 konnten die Angreifer erfolgreich Schadsoftware auf einem zu der Organisation zugehörigen Computer installieren, nach der E-Mail-Account eines Mitarbeiters kompromittiert wurde. Seit diesem Zeitpunkt waren die Angreifer in der Lage, entsprechend gesendete und empfangene E-Mails in Echtzeit zu überwachen und

persönliche Informationen über Mitarbeiter zu sammeln. Mit Hilfe dieser Informationen begannen die Angreifer weitere maliziöse E-Mails an Mitarbeiter zu verteilen, die als Quittungen für einbehaltene Steuern getarnt waren. Obwohl einige Mitarbeiter versuchten angehangene Dokumente der maliziösen E-Mails zu öffnen, wurden keine relevanten militärischen Daten gestohlen, da Sicherheitssysteme des Netzwerks des U.S. Verteidigungsministeriums Aktionen der Schadsoftware verhinderten. /KOR23w01/

Kerntechnischer Bezug

Bislang liegen neben der Tatsache, dass die mutmaßlich für die Cyberangriffe verantwortliche Gruppierung Kimsuky bereits im Jahr 2014 einen Cyberangriff auf ein Kernkraftwerk durchgeführt hat, keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.15.34 COSMIC Energy

Übersicht

Am 25.05.2023 veröffentlichte Mandiant einen Bericht /MAN23r01/ zur Schadsoftware COSMICENERGY, welche ähnlich wie z. B. die im vergangenen Jahr bekannt gewordene Schadsoftware Industroyer2 Designschwachstellen des industriellen Standards IEC-104 von Systemen ausnutzt, die in Übertragungsnetzen eingesetzt werden. Im Gegensatz zu Industroyer2 wurde die Schadsoftware COSMICENERGY nach bisherigen Kenntnissen bislang noch nicht für Cyberangriffe eingesetzt. Aufgrund ihres eingeschränkten Funktionsumfangs und Überschneidungen zu bekannt gewordenen Schadsoftwarevarianten eines Informationssicherheitsunternehmens, handelt es sich womöglich um eine Schadsoftware für Trainingszwecke. Darüber hinaus wurden vom Unternehmen Dragos im Juni 2023 mit /DRA23r01/ weitere Informationen zu COSMICENERGY veröffentlicht.

Beschreibung

Erstmalig bekannt wurde die Schadsoftware COSMICENERGY im Dezember 2021, als ein russischer Nutzer sie auf einer Plattform für Schadsoftwareanalyse und Erkennung veröffentlichte. Ähnlich wie Industroyer und Industroyer2 aus den Jahren 2016 und 2022 zielt die Schadsoftware COSMICENERGY auf industrielle Steuerungssysteme ab, welche auf dem Industriestandard IEC 60870-5-104 (IEC-104) basieren.

Dieses Protokoll wird allgemein für die Überwachung und Kontrolle von Systemen im Übertragungsnetz verwendet. Jedes System, in dem das Protokoll IEC-104 zum Einsatz kommt, ist prinzipiell durch die in Schadsoftware wie COSMICENERGY und Industroyer2 beinhalteten Methoden und Werkzeuge angreifbar. Die Schadsoftware COSMICENERGY selbst besitzt weniger Funktionen als Industroyer oder Industroyer2. COSMICENERGY besteht insgesamt aus nur zwei Unterprogrammen, welche die Kernfunktionen von COSMICENERGY abbilden:

- PIEHOP: Ein erstmalig mit COSMICENERGY entdeckter Schadsoftwareteil, welcher auf Basis der Programmiersprache Python geschrieben wurde. PIEHOP dient der Übertragung von Befehlen auf MSSQL Server (ein von Microsoft veröffentlichtes Serverbetriebssystem basierend auf der Structured Query Language), welche selbst in Verbindung ICS stehen. /MAN23r01/
  Auf dem entsprechenden MSSQL Server lässt PIEHOP dann über den Port TCP/1433 die Schadsoftwarekomponente LIGHTWORK ausführen und löscht diese anschließend wieder. /MAN23r01/

- LIGHTWORK: Ein erstmalig mit COSMICENERGY entdeckter Schadsoftwareteil, welche auf Basis der Programmiersprache C++ programmiert wurde und auf dem MSSQL Server Nachrichten an über das Protokoll IEC-104 angebundene ICS sendet. LIGHTWORK kann ausschließlich die Befehle „On“ und „Off“ übersenden. /MAN23r01/

Die Schadsoftware COSMICENERGY besitzt keine Fähigkeiten zum Ausspähen der Netzwerke von ICS, so kann sie weder die IP-Adresse des MS SQL Servers identifizieren noch der daran angeschlossenen ICS. Auch fehlen der Schadsoftware sämtliche Funktionalitäten für externe Steuerungs- und Befehlsmöglichkeiten. Die Schadsoftware kann also nur in dem Anwendungsfall verwendet werden, in welchem bereits genaue Kenntnisse des anzugreifenden IT-Netzwerks bekannt geworden sind, z. B. durch Informationsgewinnung anderer Schadsoftwarevarianten oder in bekannten Trainingsumgebungen.

Auf der Basis der bekannt gewordenen Fähigkeiten der Schadsoftware lässt sich vermuten, dass es sich bei COSMICENERGY möglicherweise um ein Red Teaming Tool oder eine Trainingsschadsoftware für die Übungen von Cyberangriffen zur Unterbrechung der elektrischen Energieversorgung handelt.

Dragos hat nach eigener Analyse bekannt gegeben, dass die Schadsoftware weit entfernt von den Fähigkeiten anderer auf ICS abzielender Schadsoftware wie Industroyer2 oder Crashoverride sei. Sie beinhalte Fehler und es fehlen notwendige Bestandteile für einen Angriff mit COSMICENERGY. Ihre interne Benennung referenziere teilweise das MITRE ATT&CK Framework, was weiter auf eine Trainingsschadsoftware hinweise. Die LIGHTWORK Komponente von COSMICENERGY nutzt mehrheitlich die open source Bibliothek „lib60870-c“, welche vom Unternehmen MZ Automation GmbH gepflegt wird, um ihre Funktionalität zu verwirklichen. Lib60870-c ist eine freie Softwarebibliothek für die Implementierung von Spezifikationen entsprechend der Standard IEC 60870-5-101 und IEC 60870-5-104. Eine Aufdeckung bzw. Erkennung der Schadsoftware im Angriffsfall ist insbesondere durch eine systematische Protokollierung und Auswertung potenziell betroffener IT-Systeme möglich und basiert gemäß Mandiant auf der Aufdeckung von unbekannten bzw. unautorisierten Python-Anwendungen. /MAN23r01, DRA23r01/

Bisher sind keine Cyberangriffe mittels COSMICENERGY bekannt geworden. Nach den Kenntnissen von Mandiant und Dragos ist es wahrscheinlich, dass die Schadsoftware COSMICENERGY in ihrer vorliegenden Version nicht für funktionierende Cyberangriffe geeignet ist. /MAN23r01, DRA23r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

Weitere Bearbeitung

Aus Sicht der GRS besteht keine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen. Die GRS verfolgt fortwährend aktuelle Entwicklungen und Entdeckungen für Schadsoftware, welche auf ICS-Systeme abzielt und somit eine Bedeutung für deutsche kerntechnische Anlagen und Einrichtungen haben könnten im Rahmen der Auswertung der Bedrohungslage deutscher kerntechnischer Einrichtungen.

B.15.35 MOVEit Transfer Zero Day Schwachstelle und zugehöriger Cyberangriff durch die Cl0P Ransomware Gang

Übersicht

MOVEit Transfer (kurz MOVEit) ist eine Software für das Management großer Daten und deren Übertragung und Bewegung auf Datenträgern, hergestellt durch das Unternehmen Progress Software. Die Software ist unter Unternehmen und Regierungsbehörden weit verbreitet und wurde als Softwarelösung für das Management und die Bewegung großer Datenmengen angewendet. Eine bis dahin unbekannte Schwachstelle (Zero Day Schwachstelle) ermöglichte den IT-Angreifern mit dem Namen CL0P Ransomware Gang umfassenden Zugriff auf die Software, welche als Datenmanagementsoftware selbst Zugriff auf große Datenmengen besaß. Hierdurch waren die Angreifer in der Lage, umfassende Datensätze großer Organisationseinheiten, nach aktuellem Stand (Oktober 2023) von über 2.500 Organisationen, digital zu entwenden. /CIS23r02, /PRO23w01/

Beschreibung

CL0P ist seit 2019 aktiv und griff bereits mehrfach unterschiedliche Software wie Accellion File Transfer Appliance (FTA) oder Fortra/Linoma GoAnywhere MFT an. Zusätzlich wurde CL0P als Ransomware as a Service Dienstleister bekannt, welcher Phishing und Spear Phishing Methoden für Ransomware Angriffe einsetzte. Durch Verschlüsselung der Daten und gleichzeitigen Diebstahl der Daten wurden die Opfer der Cyberangriffe anschließend zweifach auf Herausgabe eines Entschlüsselungsschlüssels und der Nichtveröffentlichung der Daten erpresst. /EMS23r01/

In der Software MOVEit Transfer existierte in allen bis Mai 2023 veröffentlichten Versionen eine kritische Schwachstelle in von MOVEit Transfer etablierten und genutzten SQL-Servern, auf welche direkt über das Internet zugegriffen werden kann. CL0P nutzte die Schwachstelle mindestens seit dem 27.05.2023 aus und erlangte hierdurch Zugriff auf eine Vielzahl von Unternehmen, welche MOVEit Transfer in Kombination mit einem mit dem Internet verbundenen SQL-Server verwendeten. CL0P installierte auf den betroffenen IT-Systemen anschließend die Web-Shell basierte Schadsoftware LEMURLOOT, welche Funktionen zur Sicherstellung des Zugriffs, zur Aufklärung und für den eigentlichen Datendiebstahl ausführte. Weiterhin ermöglicht LEMURLOOT direkte Befehlseingabe durch die Angreifer über http Anfragen. /EMS23r01, CIS23r02/

Am 31.05.2023 veröffentlichte Progress Software eine erste Warnung zur dann mit CVE-2023-34362 genannten Schwachstelle. Für alle von Progress Software unterstützen Versionen von MOVEit Transfer wurden Updates im Verlauf des Juni 2023 veröffentlicht, welche auch nachfolgend bekanntgewordene Schwachstellen behoben. Jedes System, welches MOVEit Transfer ohne Update in Kombination mit einem SQL-Server nutzt, ist weiterhin direkt angreifbar. /PRO23w01/

Zu den betroffenen Organisationen gehören Unternehmen beinahe jeder Branche und verschiedene Regierungsorganisationen; so sind z. B. das Louisiana Office of Motor Vehicles mit über 6 Millionen individuellen Personen zugeordneten Datensätzen wie auch das Colorado Department of Health Care Policy and Financing mit 4 Millionen individuellen Personen zugeordneten Datensätzen ebenso betroffen wie Unternehmen wie British Airways, Ernest & Young oder verschiedene deutsche Krankenkassen wie die Barmer und mehrere AOKs. Insgesamt wird davon ausgegangen, dass bis zu 70 Millionen Individuen (Kunden und Mitarbeiter) von 2.553 Organisationen betroffen sind. /EMS23r01/

Der CL0P Cyberangriff auf MOVEit Transfer wurde insbesondere durch die öffentlichkeitswirksamen Warnungen und Ankündigungen von CL0P bekannt. Am 06.06.2023 veröffentlichte CL0P ein Informationsblatt, welches MOVEit Transfer einsetzende Unternehmen dazu aufrief mit CL0P Kontakt aufzunehmen. CL0P bot Beweise für den Besitz von Daten an und drohte mit einer späteren Veröffentlichung sowohl der Namen der betroffenen Unternehmen als auch der Daten. Nach Kontaktaufnahme würde CL0P Zahlungsoptionen bereitstellen, nach deren Ausführung CL0P die entwendeten Daten vernichten würde. CL0P gab weiterhin an die Daten von Regierungsbehörden von selbst zu vernichten, jedoch gab CL0P später auch Regierungsbehörden als betroffene Organisationen im Rahmen ihrer Veröffentlichungen an. Es wurde bekannt, dass auch das U.S. Department of Energy (US DoE) von dem Cyberangriff betroffen ist. Dazu wurde zeitweise berichtet, dass das kerntechnische Oak Ridge National Labratory von dem Cyberangriff betroffen sei. Es stellte sich jedoch heraus, dass das DoE Waste Isolation Pilot Plant, ein Versuchsendlager innerhalb eines Salzstocks in der Nähe der Stadt Carlsbad im Bundesstaat New Mexiko, von dem Cyberangriff betroffen ist. Es seien zwar keine internen IT-Systeme des DoE betroffen, jedoch wurden Daten durch CL0P entwendet. /EMS23r01, CYB23w01, FNN23w01/

Ab Ende Juni veröffentlichte CL0P Namen verschiedener namhafter betroffener Unternehmen auf ihrer Webseite. Dazu veröffentlichten eine Vielzahl von Organisationen von

sich aus ihre Betroffenheit und warnten ihre Nutzer, Kunden oder Mitarbeiter vor dem Abfluss möglicherweise personenbezogener Daten. Mit mehreren Aufrufen und der Drohung der Veröffentlichung der entwendeten Daten ersuchte CL0P die Zahlung für die Löschung der Daten. Da jedoch keine Verschlüsselung bestehender Daten auf den betroffenen IT-Systemen stattfand, galt es als unwahrscheinlich, dass eine hohe Zahl von Organisationen das Angebot von CL0P annahmen. /EMS23r01, CYB23w01/

CL0P begann mit der Veröffentlichung von Daten solcher namhafter Organisationen, welche eine Zahlung verweigerten oder in Verhandlungen nicht das gewünschte Ergebnis von CL0P erzielt wurde. Hierzu gehörten Ende Juli Shell und Pricewaterhouse Coopers (PWC). Anfang August 2023 drohte CL0P dann mit der Veröffentlichung aller Daten der von ihnen bisher benannten und direkt kontaktierten Unternehmen im freien Internet, was am 15 August 2023 ausgeführt wurde. CL0P veröffentlichte Daten hunderter Unternehmen auf der Filesharing Plattform Torrent. /CYB23w01/

Es ist unbekannt, wie erfolgreich CL0P tatsächlich Gelder von den betroffenen Organisationseinheiten einnehmen konnten. Während der Schaden auf bis zu 10 Mrd. $ geschätzt wurde, wurde vermutet, dass CL0P bis zu 100 Millionen $ in Lösegeldern einnehmen konnte. /EMS23r01/

Bei der ausgenutzten Schwachstelle CVE-2023-34362 handelte es sich nicht nur um eine bis dahin nicht bekannte Zero Day Schwachstelle, sondern auch eine komplexe Schwachstelle innerhalb einer weniger bekannten Unterfunktion der MOVEit Transfer Software. Sicherheitsforscher gehen davon aus, dass allein die Entdeckung der Schwachstelle nur durch Experten in einem aufwendigen Analyseverfahren möglich war. Die CL0P Ransomware Group wurde bisher nicht durch solche Tätigkeiten bekannt, sodass Sicherheitsforscher vermuten, dass die Schwachstelle von einer anderen Gruppierung vorher entdeckt wurde und diese an CL0P verkauft oder übergeben wurde. Ein solcher Markt für Schwachstellen hat sich in den letzten Jahren etabliert und ist zu einem veritablen Geschäftsmodell angewachsen. /DAR23w03/

Kerntechnischer Bezug

Mit dem Versuchsendlager Waste Isolation Pilot Plant sind Daten eines kerntechnischen Versuchsendlagers durch den Cyberangriff auf die Schwachstelle CVE-2023-34362 von der Gruppierung CL0P entwendet worden. Es ist unbekannt, welche Daten genau vom Versuchsendlager der U.S. DoE gestohlen wurden oder ob weitere Anlagen des

U.S. DoE oder andere kerntechnische Anlagen in oder außerhalb der USA ebenfalls betroffen sind. /FNN23w01/

Weitere Bearbeitung

Bei dem Cyberangriff auf MOVEit Transfer durch die CL0P Ransomware Gruppierung handelt es sich um einen der schwersten Datenabflüsse der vergangen Zeit. Weiterhin ist mindestens eine kerntechnische Anlage betroffen. Die GRS verfolgt daher sowohl die veröffentlichten Informationen zu diesem Cyberangriff in den bestehen Vorhaben als auch die Veröffentlichung von Zero Day Schwachstellen und deren zugehörigen Cyberangriffen fortwährend.

B.15.36 Cyberangriff der APT Sandworm auf Energieunternehmen in der Ukraine im Oktober 2022

Übersicht

Am 10. Oktober 2022 führte ein Cyberangriff durch die Russland zugezählte APT-Gruppierung Sandworm zu einem ungeplanten Stromausfall in der Ukraine. Die Angreifer erlangten Zugriffe auf die IT-Systeme des angegriffenen Energieunternehmens und anschließend ohne den Einsatz von weiterer Schadsoftware Zugriff auf die OT-Systeme. Der Angriff erfolgte im Kontext der zu dieser Zeitpunkt stattfindenden Angriffskampagne Russlands gegen das ukrainische Strom- und Wärmenetz im Rahmen des russisch-ukrainischen Krieges.

Beschreibung

Im Rahmen des Russisch-Ukrainischen Krieges führte Russland verschiedene Cyberangriffe durch. Ein solcher Angriff wurde erst im November 2023 vom Cybersicherheitsunternehmen Mandiant mit /MAN23r03/ bekannt gegeben. Hierbei nutzten die Angreifer ab Juni 2022 bislang unbekannte Zugriffspfade für Zugriffe auf die IT-Umgebung des angegriffenen Unternehmens und erlangten im Anschluss Zugriff auf die OT-Umgebung des Unternehmens in Form des eingesetzten SCADA (Supervisory Control and Data Acquistion) Steuerungssystem. Am 10. Oktober 2022 nutzten die IT-Angreifer ihre erlangten Zugriffe und führten Native Befehle des SCADA Systems (Typ MicroSCADA) aus, welche zur Schaltung der Leistungsschalter der Anlage und im Anschluss zum Ausfall der

Anlage führten, welche zu ungeplanten Stromausfällen innerhalb der Ukraine führten. /MAN23r03/

Herausstechend wurde der Angriff zum einen aufgrund der direkten Einwirkung auf die OT-Umgebung der betroffenen Anlage und zum anderen aufgrund der kurzen Zeitabstände, die zwischen initialem Zugriff auf die IT-Umgebung im Juni 2022 und der letztlichen schadhaften Wirkung auf die OT-Umgebung im Oktober 2022 lag. Dies wurde möglich durch eine umfassende Nutzung bestehender Software, Systeme und Zugänge innerhalb des angegriffenen Netzwerkes durch Nutzung von Living off the Land Techniken. /MAN23r03/

Das eingesetzte MicroSCADA System wurde mit einem Softwarestand, welcher als EOL vom Hersteller gekennzeichnet wurde, betrieben und besaß daher eine Reihe nicht behobener Schwachpunkte. Hierdurch war es für die Angreifer möglich, mit den bestehenden Tools der Software dem MicroSCADA System Befehle im Sinne der Angreifer zu geben, welche zum Stromausfall führten. Weiterhin wurde auch keine weiteren umfangreichen Cybersicherheitsmaßnahmen getroffen, welche die Möglichkeit zur Erkennung der Einwirkung gegeben hätten.

Zwei Tage später nutzten die Angreifer ihre Zugriffe auf die IT-Systeme, um auf diesen einen Wiper zur weiteren Schädigung und Verschleierung auszuführen. Die Ausführung des Wipers auf den OT-Systemen war grundsätzlich nicht möglich, da die Angreifer keine Schadsoftwarezugriffe auf diese hatten.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Die GRS verfolgt fortwährend die Aktivitäten der APT-Gruppierung Sandworm, da es sich bei dieser Gruppierung um eine der profiliertesten und aktivsten APT-Gruppierungen handelt. Die Ergebnisse dieser Beobachtung fließen in die allgemeine Auswertung der Bedrohungslage ein. Bei besonderen Ereignissen, werden die Handlungen der APT Sandworm von der GRS gesondert im Rahmen bestehender vorhaben ausgewertet.

B.15.37 Cyberangriff auf das Helmholtz-Zentrum Berlin

Übersicht

Am 15.06.2023 wurde das Helmholtz-Zentrum Berlin Opfer eines nicht näher definierten Cyberangriffes, welchen das Helmholtz-Zentrum Berlin am 16.06.2023 in einer kurzen Stellungnahme veröffentlichte /HZB23w01/. Das Helmholtz-Zentrum Berlin ist ein Großforschungszentrum mit den Schwerpunkten Materialien und Energie und gleichzeitig Betreiber des seit 2019 abgeschalteten und sich in der Nachbetriebsphase befindlichen 10-MW-Schwimmbadreaktors Berliner Experimentier-Reaktor 2 (BER-II) sowie der Synchrotronstrahlungsquelle BESSY II.

Beschreibung

Am 15.06.2023 wurde das HZB Opfer eines Cyberangriffes, in dessen Folge die Telekommunikation und die eigene Webseite des HZB nicht zur Verfügung stehen. Das HZB hat in Folge des Cyberangriffes sämtliche IT-Systeme heruntergefahren. Weiterhin wurde ebenfalls die 1,7 GeV Synchrotronstrahlungsquelle BESSY II heruntergefahren. Bis sämtliche IT-Systeme des HZB wieder neu aufgesetzt worden sind, dauerte es mehrere Wochen, in denen die Kommunikation zwischen den mehr als 1.500 Mitarbeitern nicht zur Verfügung stand.. Das HZB ist auch der Betreiber des abgeschalteten Versuchsreaktors BER-2, welcher jedoch nach Aussagen des HZB vom IT-Netzwerk des HZB getrennt ist und damit nicht vom Cyberangriff betroffen war. /TAG23r01/

Es ist unbekannt, welche Schadsoftware beim HZB durch die Angreifer eingesetzt wurde.

Kerntechnischer Bezug

Ein kerntechnischer Bezug liegt vor, da das HZB Betreiber des abgeschalteten Forschungsreaktors BER II ist. Nach Aussagen des HZB ist der BER II nicht vom Cyberangriff betroffen, da dessen Netzwerke unabhängig vom HZB Netzwerk sind.

B.15.38 Cyberangriff auf GKV-Dienstleister Bitmarck

Übersicht

Am 30. April 2023 wurde bekannt, dass der IT-Dienstleister Bitmarck Opfer einer Cyberattacke wurde. Bitmarck selbst ist Dienstleister insbesondere für deutsche gesetzliche Krankenkassen und bearbeitet hierbei die Daten von mehr als 20 Millionen Patienten für mehr als 80 Krankenkassen. Der Cyberangriff veranlasste Bitmarck seine IT-Dienstleistungen zwischenzeitlich zu beenden und die IT-Systeme des Unternehmens vom Netz zu nehmen. In der Folge konnten die Krankenversicherungen nicht mehr auf Patientendaten zugreifen, Krankschreibungen über die digitalen Systeme ausstellen und teilweise konnten Ärzte nicht mehr auf die elektronischen Patientenakten der bei den betroffenen Krankenkassen Versicherten zugreifen. /BTB23w01/

Bereits im Januar 2023 wurde Bitmarck Opfer eines Cyberangriffes, bei welchem später zugegeben wurde, dass bis zu 300.000 Kundendaten verschiedener Krankenkassen durch Angreifer entwendet wurden. /BIT23r01/

Beschreibung

Bitmarck ist von einer Gemeinschaft verschiedener gesetzlicher und betrieblicher Krankenversicherungen als Dienstleistungsgesellschaft für eben diese gegründet worden und betreut die Daten von mehr als 20 Millionen Versicherten und 30.000 Mitarbeitern von mehr als 80 Krankenkassen. Im Jahr 2023 wurde Bitmarck zweimal Opfer eines Cyberangriffes. Zuerst im Januar 2023, bei welchem die Systeme und Dienstleistungen von Bitmarck nicht eingeschränkt wurden, jedoch eine 350MB große Sammlung von bis zu 300.000 personenbezogenen Datensätzen durch die Angreifer veröffentlicht wurden. Die Daten beinhalteten keine medizinischen Informationen, jedoch andere personenbezogene Daten. Gemäß Bitmarck erlangte „ein unberechtigter Dritter“ kurzfristig Zugriff auf ein einzelnes IT-System mittels gestohlener Zugangsdaten. /HEI23w14/

Ende April wurde Bitmarck dann Opfer eines schwerwiegenden IT-Angriffes, in dessen Konsequenz Bitmarck sämtliche IT-Systeme herunterfuhr und nur über einen längeren Zeitraum wieder in Betrieb nahm. Die Wiederinbetriebnahme aller von Bitmarck angebotenen Dienstleistungen dauerte bis in den Juli 2023 an. Es ist nicht bekannt, auf welche Art die Angreifer Zugriff auf die Bitmarck Systeme für diesen Angriff erlangten oder welche schadhaften Handlungen ausgeführt wurden.

Gemäß Bitmarck wurden keine Daten gestohlen und der Angriff in einem frühen Stadium durch das Herunterfahren der IT-Infrastruktur unterbunden. /BIT23r02/

Kerntechnischer Bezug

Nach bisherigen Erkenntnissen gibt es keinen kerntechnischen Bezug.

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-910548-48-0