IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand Mai 2021

GRS - 647

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand Mai 2021

Christian Korn
Claudia Quester
Oliver Rest
Alexander Schug

August 2021

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit (BMU) unter dem Förderkennzeichen 4718R01611 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 BMU übereinstimmen.

GRS - 647
ISBN 978-3-949088-36-0

Deskriptoren

Advanced Persistent Threats, Critical Infrastructures, ICS, Industrielle Steuerungssysteme, IT-Angriffe, IT-Bedrohungslage, IT-Sicherheit, IT-Sicherheitsvorfälle, Kerntechnische Anlagen, Kritische Infrastrukturen, Nuclear Facilities, Schadsoftware

Inhaltsverzeichnis

1 Einleitung

Im Bereich der Informationstechnik führen kurze Produktentwicklungszyklen und eine immer höhere Leistungsfähigkeit zu schnellen technischen Veränderungen, welche schließlich aufgrund ihrer Potenziale oder auch Verdrängungsprozesse auch in kerntechnischen Bereichen Einzug erhalten. Hierdurch 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. Diese Veränderungen führen auch zu immer neuen Möglichkeiten und Potenzialen im Bereich der Einflussnahme auf die Informationssicherheit durch Dritte. Aus dem Blickwinkel der Informationssicherheit ist es daher von großer Bedeutung, diese Möglichkeiten und Potenziale und die daraus resultierende IT-Bedrohungslage konstant zu erfassen und auszuwerten.

Die IT-Bedrohungslage entwickelt sich sehr dynamisch, beispielsweise durch das Bekanntwerden oder sogar die Ausnutzung neu erkannter oder bisher nicht geschlossener Schwachstellen in industriellen Steuerungssystemen bzw. in für kritische Infrastrukturen relevanten IT-Systemen, durch zunehmende, gezielte, technisch versierte und andauernde Angriffe mit fortgeschrittenen Methoden, Schadsoftwarekomponenten und IT-Angriffswerkzeugen sowie die sich kontinuierlich weiterentwickelnden Techniken, Taktiken und Vorgehensweisen der IT-Angreifer und insbesondere sogenannter APT-Gruppierungen (APT - Advanced Persistent Threats). Auf nationaler und internationaler Ebene sind regelmäßig IT-Sicherheitsvorfälle mit sicherungstechnischer Bedeutung und potenziell auf kerntechnische Anlagen und Einrichtungen übertragbaren Aspekten zu verzeichnen, woraus sich Veränderungen der IT-Bedrohungslage ergeben. Angesichts der sich dynamisch verändernden IT-Bedrohungslage werden international die bestehenden Regelwerke und Richtlinien zur IT-Sicherheit (insbesondere von IAEO, 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 gerade 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 und Detektion sowie zur Reaktion auf IT-Angriffe eine besondere Bedeutung zu.

Im laufenden Vorhaben FKZ 4718R01611 *„Erfassung, Auswertung und Weiterentwicklung des Standes von Wissenschaft, Technik und Erkenntnis zur Sicherung von Kernbrennstoffen und sonstigen radioaktiven Stoffen“* wurde daher über die Laufzeit des Vorhabens hinweg die Entwicklung der IT-Bedrohungslage (für industrielle Steuerungssysteme und kritische Infrastrukturen relevante IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-Angriffswerkzeuge, Schadsoftwarekomponenten, APTs) kontinuierlich verfolgt und ausgewertet. Hierzu wurden einschlägige nationale und internationale Quellen zur Informationssicherheit genutzt.

Für ein einheitliches Verständnis der jeweils enthaltenen Anforderungen aber auch als Grundlage für eine effektive und eindeutige Kommunikation im nationalen und internationalen Austausch zum Stand von Wissenschaft und Technik ist die Verwendung klar definierter Begrifflichkeiten unabdingbar. Daher wurde in AP 1 des Vorhabens ein Katalog zu wesentlichen Begriffen der IT-Sicherheit erstellt, wobei insbesondere konkurrierende Begriffe sowie Unterschiede und Konflikte zwischen einzelnen Definitionen zu gleichen oder ähnlichen Begriffen herausgearbeitet wurden. Dieses lebende Dokument wird von der GRS laufend erweitert und mit den im deutschen kerntechnischen Regelwerk verwendeten Begrifflichkeiten abgeglichen.

Aufbauend auf dem kontinuierlichen Screening der IT-Bedrohungslage wurden in AP 2 des Vorhabens ausgewählte IT-Sicherheitsvorfälle, IT-Angriffe und Schwachstellen im Rahmen von Ersteinschätzungen ausgewertet. Auch wurden Informationen zu den aktuell relevantesten APT-Gruppierungen und deren Aktivitäten zusammengetragen. Zusätzlich zu den jeweils aktuell bekannt gewordenen IT-Sicherheitsvorfällen, IT-Angriffskampagnen und Schwachstellen in industriellen Steuerungssystemen wurden auch frühere, herausragende Vorfälle, Angriffe und Schwachstellen ausgewertet, um ein möglichst vollständiges Bild der für die kerntechnischen Anlagen relevanten IT-Bedrohungslage zu erhalten. Hierbei hat sich gezeigt, dass aufgrund der sich ebenfalls kontinuierlich ändernden Informationslage zu Vorfällen, Angriffen und Schwachstellen auch die Ersteinschätzungen immer wieder auf ihre Aktualität geprüft und ggf. angepasst werden müssen.

Viele Ersteinschätzungen werden 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 Einschätzung 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 IT-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 IT-Angriffs 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 Ersteinschätzungen daher nicht um abschließende Einschätzungen, sondern um eine Momentaufnahme.

Wird bei der Auswertung der IT-Angriffe oder Schwachstellen eine besondere Relevanz für deutsche kerntechnische Anlagen ausgemacht, werden die entsprechenden Sachverhalte in Absprache mit dem BMU im Rahmen des Vorhabens FKZ 4718R01610 als beauftragte Forschungsarbeiten weiter verfolgt und vertieft ausgewertet.

In Kapitel 2 dieses Berichtes werden relevante Begriffe und Abkürzungen eingeführt. Kapitel 3 bietet grundlegende Hintergrundinformationen zu industriellen Steuerungssystemen. In Kapitel 4 werden relevante Aspekte der IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen wiedergegeben. Zusammenfassung und Fazit finden sich in Kapitel 5.

Generell ist zu beachteten, dass es sich bei dem vorliegenden Dokument um ein lebendes Dokument handelt und hier der Stand vom 11. Mai 2021 abgebildet ist.

2 Hintergrundinformationen

2.1 Industrielle Steuerungssysteme

Industrielle, verfahrenstechnische Prozesse werden typischerweise durch industrielle Steuerungssysteme (ICS) geregelt, gesteuert und überwacht (siehe Abb. 3.1). Mittels ICS erfolgt auch die Erfassung von Felddaten und die Bedienung der Prozesse.

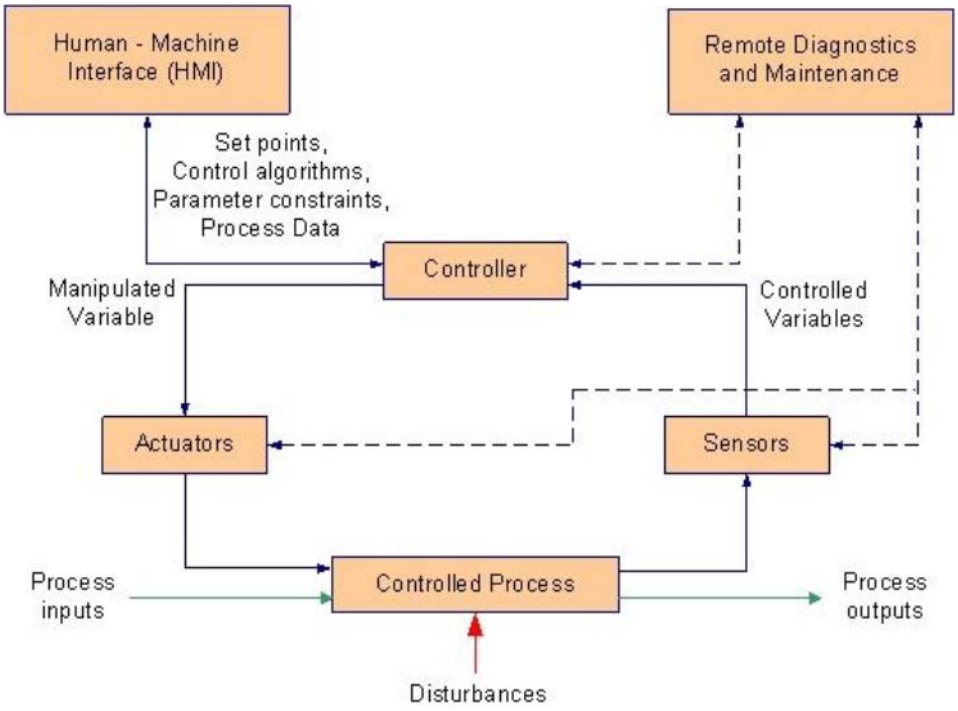

Figure 2-1. ICS Operation

Abb. 3.1 Übersicht über ein generisches industrielles Steuerungssystem

Dieses enthält typischerweise eine Vielzahl von Regelkreisen, Mensch-Maschine-Schnittstellen und Schnittstellen für Wartungs- und Instandhaltungszugriffe. Jeder Regelkreis besitzt Sensoren, Aktuatoren und Controller, um den verfahrenstechnischen Prozess zu regeln oder zu steuern. Grafik unverändert übernommen aus /NIS15t01/.

Der Begriff ICS ist dabei ein Überbegriff, der verschiedene, in kritischen Infrastrukturen gebräuchliche Typen von industriellen Steuerungssystemen einschließt. Im Bereich der betrieblichen Leittechnik sind dies beispielsweise SCADA-Systeme (Supervisory Control and Data Acquisition Systems), DCS (Distributed Control Systems) und andere Steuerungssystemkonfigurationen mit SPS (Speicherprogrammierbare Steuerungen – Programmable Logic Controllers, PLCs).

Ein typisches betriebliches Leittechniksystem ist aus einer Vielzahl von Komponenten und Funktionen aufgebaut, was neben Regelkreisen und HMIs (Human Machine Interfaces) auch Werkzeuge für remote ausgeführte Diagnose und Instandhaltung beinhaltet. Als Controller bezeichnet man den Teil des Systems, der hauptsächlich dafür verantwortlich ist, den verfahrenstechnischen Prozess innerhalb der spezifizierten Parameter zu halten. Der Controller interpretiert dabei die ihm von den Sensoren zur Verfügung gestellten Eingangssignale und errechnet auf Basis der hinterlegten Algorithmen und der eingestellten Grenzwerte Ausgangssignale, die er an die Aktuatoren übermittelt. Während SCADA-Systeme hauptsächlich für räumlich breit verteilte Steuerungsaufgaben wie beispielsweise bei der Energieübertragung eingesetzt werden, werden DCS vornehmlich zur Steuerung von Prozessen am gleichen geographischen Ort eingesetzt, wobei die tatsächliche Implementation eines ICS auch eine Mischform zwischen SCADA-Systemen und DCS sein kann. /NIS15t01/

Zur Konfiguration und Programmierung von Komponenten eines ICS werden sogenannte Engineering-Workstations (EWS) genutzt. Die Infektion einer EWS mit einer Schadsoftware ermöglicht beispielsweise eine Veränderung von Programmen und Algorithmen auf den Steuerungen, wodurch der Ablauf der Steuerungen oder deren Ausgangssignale geändert werden können, oder eine Entwendung der Programme. Laut BSI ist *„dieser Angriffsvektor besonders wertvoll, da hierdurch nicht nur die SPS kompromittiert und die Produktion auf eine gewünschte Weise gestört wird. Es wird gleichzeitig die Visualisierung des Steuerungszustands im Sinne des Angreifers beeinflusst. In der Folge bemerkt das Bedienpersonal die Auswirkung des Angriffs nicht, schöpft keinen Verdacht und setzt die Produktion unvermindert fort. Beeinträchtigte Systeme können dann über einen langen Zeitraum sabotiert werden, ohne dass dies bemerkt wird.“* /BSI13t01/

Bei einem Safety Instrumented System (SIS) handelt es sich grundsätzlich ebenfalls um ein ICS, wobei der Begriff SIS speziell Sicherheits- oder Schutzsysteme, also Sicherheitsleittechnik, bezeichnet. Ein SIS ist meist aus Sensoren und Messumformern, Grenzwertgebern, logischen Verknüpfungen und Auswahlschaltungen aufgebaut. Der Zweck eines SIS ist es, den verfahrenstechnischen Prozess in einen sicheren Zustand zu überführen, sobald die Prozessparameter den voreingestellten Bereich verlassen, der einen sicheren Zustand definiert /NIS15t01/. Ein Schutz- oder Notabschaltsystem ist beispielsweise ein SIS.

Die Manipulation eines SIS mittels Schadsoftware ist besonders kritisch, da bei einer potenziell ausbleibenden Schutzabschaltung eines verfahrenstechnischen Prozesses in der Auslegung nur noch passive Schutzeinrichtungen vorgesehen sind und anschließend nur auf Notfallverfahren und mitigative Maßnahmen zurückgegriffen werden kann. Dabei lassen sich in vielen kritischen Infrastrukturen eine Freisetzung von giftigen oder anderweitig gesundheitsgefährdenden Stoffen oder die Gefährdung von Gesundheit und Leben nicht mehr ausschließen. /FIR17w01, MID18w01/

2.1.1 Genereller Aufbau

Ein generischer Aufbau für die IT- und leittechnische Architektur einer Anlage mit kritischen Sicherheits- und Steuerungssystemen ist beispielsweise der von FireEye erstellten Grafik zu entnehmen (Abbildung 2). Dabei ist die IT der Anlage vom Internet durch eine oder mehrere Firewalls getrennt. Die sogenannte demilitarisierte Zone (DMZ), die sich zwischen der Anlagen-IT und den rechnerbasierten und programmierbaren leittechnischen Systemen und Komponenten befindet, ist beidseitig ebenfalls mit Firewalls geschützt. Die leittechnische Architektur teilt sich grob in die Systeme zur betrieblichen Steuerung und Regelung des verfahrenstechnischen Prozesses (hier DCS) und die Sicherheitssysteme zum Schutz vor potenziell gefährlichen Anlagenzuständen (SIS) auf.

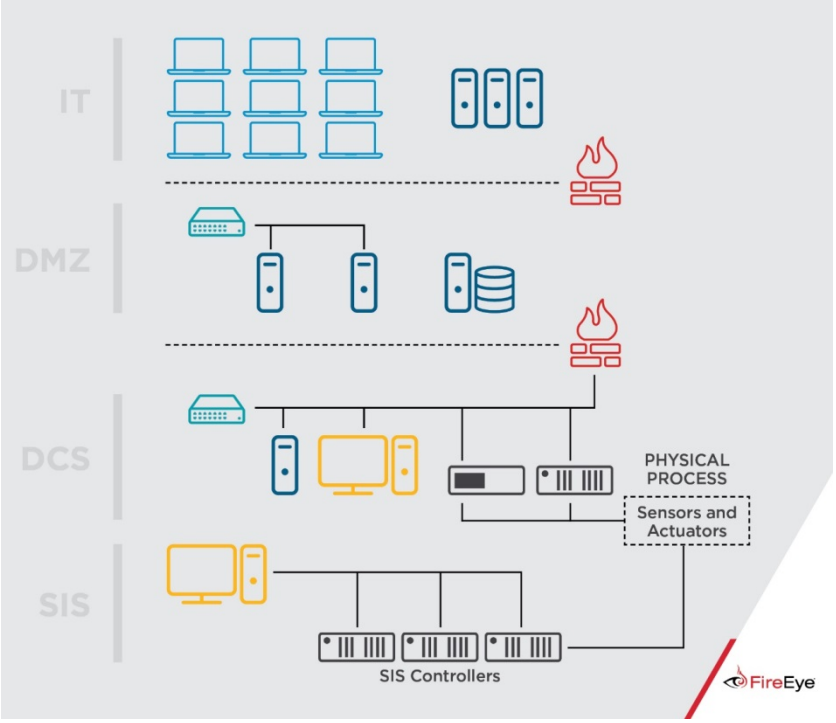

Abb. 3.2 Generischer Aufbau der IT- und leittechnischen Architektur einer Anlage mit kritischen Sicherheits- und Steuerungssystemen.

Grafik unverändert übernommen aus /FIR17w01/

3 IT-Bedrohungslage

Die IT-Bedrohungslage für kritische Infrastrukturen und insbesondere kerntechnische Anlagen und Einrichtungen und ihre dynamische Entwicklung wurden in diesem Vorhaben fortlaufend verfolgt, erfasst und ausgewertet. Relevante Aspekte hierzu sind insbesondere bekanntgewordene

- Schwachstellen in industriellen Steuerungssystemen und in für kritische Infrastrukturen relevanten IT-Systemen (siehe Abschnitt 4.1),
- IT-Angriffswerkzeuge, die unabhängig von IT-Angriffen bekannt werden (siehe ebenfalls Abschnitt 4.1)
- IT-Sicherheitsvorfälle und IT-Angriffe einschließlich der dabei eingesetzten IT-Angriffswerkzeuge und Schadsoftwarekomponenten (siehe Abschnitt 4.2) sowie
- APT-Gruppierungen (Advanced Persistent Threat – fortgeschrittene andauernde Bedrohung) und ihre Aktivitäten (siehe Abschnitt 4.3).

In den folgenden Abschnitten werden nach Jahren sortiert ausgewählte Schwachstellen und IT-Angriffswerkzeuge, IT-Sicherheitsvorfälle und IT-Angriffe sowie Advanced Persistent Threats der vergangenen Jahre vorgestellt. Hierbei handelt es sich nur um einen relevanten Ausschnitt der Gesamt-Bedrohungslage.

3.1 Schwachstellen und IT-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 schwerwiegenden Schwachstellen betroffen, zuletzt im Jahr 2021.

Darüber hinaus werden in den folgenden Abschnitten auch IT-Angriffswerkzeuge beschrieben, deren Einsatz zunächst keinem bekannt gewordenen IT-Angriff zugeordnet werden kann.

Das erste beschriebene IT-Angriffswerkzeug, welches bereits im Jahr 2017 bekannt wurde, dient dem Aufbau einer Kommunikation über Air-Gaps hinweg, beim zweiten IT-Angriffswerkzeug, das im Jahr 2020 bekannt wurde, handelt es sich um ein klassisches Spionagewerkzeug.

3.1.1 2017

3.1.1.1 Brutal Kangaroo – IT-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 IT-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 Überspringen 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 zurückgegriffen, 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 IT-Angriff 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 IT-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 IT-Angriffen im Zusammenhang mit der Schadsoftware Stuxnet (siehe Abschnitt 4.2.2.1).

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 IT-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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.2 2018

3.1.2.1 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 Schwachstelle 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 den folgenden Abschnitt 4.1.2.2).

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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.2.2 Spectre – Schwachstellen in CPUs

Übersicht

Im Januar 2018 veröffentlichten Forscher verschiedener Universitäten in Australien, Österreich und den Vereinigten Staaten von Amerika und 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 4.1.2.1) 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 4.1.2.1 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.3 2019

3.1.3.1 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 T-3000 handelt es sich um ein weltweit eingesetztes Distributed Control System (DCS), welches insbesondere in konventionellen Kraftwerken und Turbinensteuerungssystemen eingesetzt wird, wobei SPPA T-3000 keine Sicherheitsleittechnik direkt integriert unterstützt. Die Schwachstellen sind als äußerst schwerwiegend eingeschätzt worden und ermöglichen IT-Angreifern umfassende Kontrollübernahme über das betroffene Leittechniksystem.

Beschreibung

Bei dem System des Herstellers Siemens mit der Typenbezeichnung SPPA T-3000 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 ausreichend Zeit für die Erstellung von Patches und die Information der betroffenen Anlagen zu geben. Siemens arbeitete daraufhin gemeinsam mit Kaspersky an Patches, Softwareupdates 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.3.2 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 S7-1500 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 Schwachstellen 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.4 2020

3.1.4.1 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 leittechnischen Geräten 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.4.2 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 IT-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 und 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.4.3 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 Warnmeldung 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.4.4 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-Sicherheitsunterrnehmen 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 Amnesia: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[1] /CIS20r03/.

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

Das BSI berichtet, die Ausnutzung der Schwachstellen basiere in allen Fällen auf manipulierten Netzwerkpaketen, die zwischen betroffenem Gerät und IT-Angreifer ausgetauscht werden /BSI20r03/. Die CISA veröffentlichte bereits kurz zuvor ein speziell auf Siemens Produkte ausgerichtetes ICS Advisory /CIS20r04/ zu den entdeckten Amnesia: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

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 Siemens-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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.4.5 Ramsay - IT-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 Schadsoftware lieferte Hinweise darauf, dass sich das IT-Angriffswerkzeug derzeit noch im Entwicklungsprozess befindet /ESE20w01/.

Kerntechnischer Bezug

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

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.5 2021

3.1.5.1 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 IT-Angreifern ausgenutzt, wodurch potenziell eine hohe Anzahl von Unternehmen, Behörden und Betreibern kritischer Infrastruktur betroffen sein können.

Kerntechnischer Bezug

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

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.1.5.2 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.1.5.3 BadAlloc

Übersicht

Unter dem Namen BadAlloc werden 25 Schwachstellen in echtzeitfähigen OT- und IoT- bzw. IIoT-Geräten sowie deren unterstützenden Bibliotheken zusammengefasst. Die Ausnutzung dieser Schwachstellen könnte beispielsweise zur Manipulation der Geräte führen oder die Injektion von Schadcode ermöglichen. /CIS21i01/

Kerntechnischer Bezug

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

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2 IT-Sicherheitsvorfälle und IT-Angriffe

In den folgenden Abschnitten werden ausgewählte IT-Sicherheitsvorfälle und IT-Angriffe kurz beschrieben, bei denen im Rahmen des Screenings der IT-Bedrohungslage eine mögliche Relevanz für industrielle Steuerungssysteme und kritische Infrastrukturen einschließlich kerntechnischer Anlagen ausgemacht wurde. Dies schließt auch die IT-Angriffswerkzeuge und Schadsoftwarekomponenten ein, die bei diesen IT-Angriffen zum Einsatz kamen. IT-Angriffswerkzeuge, die bislang noch keinem IT-Angriff zugeordnet werden konnten, wurden bereits in Abschnitt 4.1 beschrieben.

Wie schon einleitend beschrieben, werden diese Ersteinschätzungen der GRS zu diesen IT-Sicherheitsvorfällen und IT-Angriffen 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 IT-Angriffen, 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 sowohl um kürzlich bekannt gewordene IT-Sicherheitsvorfälle und IT-Angriffe, 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 IT-Angriff 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 IT-Angriffe möglichst umfassend zu berücksichtigen. Daher sind im hier wiedergegebenen lebenden Dokument nicht nur IT-Sicherheitsvorfälle und IT-Angriffe 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 IT-Angriffe 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 IT-Angriffswellen werden dem Jahr zugeordnet, in dem ihr (teilweise auch vorläufiger) Höhepunkt ausgemacht werden kann.

3.2.1 2008

3.2.1.1 BlackEnergy 1 – IT-Angriffe auf georgische Einrichtungen

Übersicht

Bei BlackEnergy 1 handelt es sich um ein HTTP-basiertes IT-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 4.2.5.1 bzw. 4.2.7.1) erstmalig bekannt und in den Folgejahren jeweils breit eingesetzt, wobei von jeder Version zahlreiche Varianten in Umlauf sind.

Beschreibung

Die Schadsoftware BlackEnergy 1 wurde im Rahmen zahlreicher IT-Angriffe eingesetzt, unter anderem wohl auch bei mehreren IT-Angriffswellen 2008 auf georgische Einrichtungen im Vorfeld der militärischen Auseinandersetzungen zwischen Russland und Georgien. Betroffen waren unter anderem Webseiten zahlreicher Regierungseinrichtungen und Nachrichtenagenturen. /FSE14r01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.2 2010

3.2.2.1 Stuxnet – IT-Angriff 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 hinweg. 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Die GRS hat im Jahr 2010 eine Weiterleitungsnachricht zum Thema Stuxnet verfasst und später ergänzt, die neben den spezifischen Empfehlungen zum Umgang mit der Schadsoftware Stuxnet auch generelle Empfehlungen bezüglich der IT-Security in deutschen Anlagen beinhaltet. /GRS10i01, GRS11i01/ Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.3 2011

3.2.3.1 Duqu – IT-Angriff auf das iranische Atomprogramm

Übersicht

Bei Duqu handelt es sich um einen komplexe Schadsoftware, deren Schadcode Parallelen zu Stuxnet aufweist.

Kerntechnischer Bezug

Duqu wurde offenbar für Spionagetätigkeiten in Industrieanlagen, insbesondere in Bezug auf das iranische Atomprogramm entwickelt.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.4 2012

3.2.4.1 Flame/sKyWIper – IT-Angriff auf das iranische Atomprogramm

Übersicht

Bei Flame/sKyWIper handelt es sich um eine komplexe Schadsoftware, deren Schadcode Parallelen zu Stuxnet und Duqu aufweist.

Kerntechnischer Bezug

Flame/sKyWIper wurde offenbar für Spionagetätigkeiten in Industrieanlagen, insbesondere in Bezug auf das iranische Atomprogramm entwickelt.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.4.2 Shamoon – IT-Angriff auf Saudi Aramco

Übersicht

Die Schadsoftware Shamoon (auch W32.DistTrack) wurde im Jahr 2012 bei einem IT-Angriff 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 hinterlassen. 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 IT-Angriffen in Zusammenhang mit Flame (siehe Abschnitt 4.2.4.1) und Duqu (siehe Abschnitt 4.2.3.1) 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.5 2013

3.2.5.1 BlackEnergy 2 – Globaler IT-Angriff

Übersicht

Bei BlackEnergy 2 handelt es sich um eine Weiterentwicklung des als BlackEnergy 1 (siehe Abschnitt 4.2.1.1) bekannt gewordenen HTTP-basierten IT-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

Im Unterschied zu den Varianten der Schadsoftware-Version BlackEnergy 1 wurde BlackEnergy 2 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. Durch den modularen Aufbau ist die Schadsoftware sehr vielseitig einsetzbar. BlackEnergy 2 wurde ab 2010 bei zahlreichen IT-Angriffen 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.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.5.2 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/

Kerntechnischer Bezug

Bei diesem Angriff sollten Unbefugten sensible Informationen über nukleare Waffen zugänglich gemacht werden.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.6 2014

3.2.6.1 IT-Angriff auf südkoreanisches Kernkraftwerk

Übersicht

Im Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines IT-Angriffs 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 4.3.1.4.

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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden.

Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.6.2 IT-Angriff auf ein deutsches Stahlwerk

Übersicht

Im Jahr 2014 erfolgte ein IT-Angriff auf ein deutsches Stahlwerk. Dabei kam es zu massiven physischen Schäden an der Anlage. Welche APT-Gruppierung den Angriff durchgeführt 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 IT-Angriff handelt und das Angriffsziel ein Stahlwerk ist, besteht kein direkter Bezug zu kerntechnischen Anlagen.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.6.3 Havex und Karagany - Erste IT-Angriffswelle durch APT Dragonfly

Übersicht

Bei den IT-Angriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Abschnitt 4.3.1.1) handelt es sich um hochentwickelte, mehrstufige Angriffe. Die APT-Gruppierung setzt dabei ein breites Spektrum an IT-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 Höhepunkt 2013 erreichte und nach ihrer Entdeckung 2014 abflaute. Unabhängig von den letztlich eingesetzten IT-Angriffswerkzeugen und Schadsoftwarekomponenten nutzte Dragonfly während der ersten Angriffswelle drei verschiedene Angriffsvektoren /CIS14r01/: Spear Phising 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 IT-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 dazu, 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt bereits im Rahmen des Vorhabens verfolgt und ausgewertet. Auch wurde der Sachverhalt bereits im aktuellen Vorhaben in einem spezifisch auf IT-Angriffe über die Lieferkette ausgerichteten Bericht behandelt /GRS21r03/. Zusätzlich dazu ist vorgesehen, die Informationslage zu diesem Sachverhalt im Rahmen des bei der GRS geplanten Anschlussvorhabens für das laufende Vorhaben auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.6.4 Epic Turla – Globaler IT-Angriff

Übersicht

Bei Epic Turla handelt es sich um eine weltweite IT-Angriffswelle zur Cyber-Spionage in mindestens 45 Ländern.

Kerntechnischer Bezug

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

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.7 2015

3.2.7.1 BlackEnergy 3 – IT-Angriff 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 IT-Angriffs, 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, wurde die Anzahl der Plugins wieder stark reduziert, 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 IT-Angriff auf das ukrainische Stromnetz 2015 wird davon ausgegangen, dass die Angreifer vorher IT-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 IT-Angriff betroffenen Betreiber gaben bekannt, dass die Systeme von der Schadsoftware BlackEnergy 3 betroffen waren, aber in welchem Umfang diese Schadsoftware genutzt wurde, ist bislang nicht klar. Es ist aber sehr wahrscheinlich, dass BlackEnergy 3 bei den Angriffen auf das Stromnetz der Ukraine zumindest eine unterstützende 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.7.2 GreyEnergy – IT-Angriff auf Stromnetze in Osteuropa

Übersicht

Die Schadsoftware GreyEnergy wurde bei IT-Angriffen 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 4.2.7.1) auf. Gegen Ende des Jahres 2015 erfolgte ein IT-Angriff mit GreyEnergy auf ein Energieversorgungsunternehmen in Polen. Aber auch danach wurde GreyEnergy bei ähnlichen Angriffen eingesetzt, zuletzt wurden IT-Angriffe 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 aufgebaut. Im Gegensatz zur Schadsoftware Crashoverride (siehe Abschnitt 4.2.8.1) 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

Nach den der GRS derzeit vorliegenden Informationen ist mit der Schadsoftware GreyEnergy bisher kein IT-Angriff auf kerntechnische Anlagen und Einrichtungen erfolgt.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.8 2016

3.2.8.1 Crashoverride/Industryer – IT-Angriff 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 IT-Angriff 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 IT-Angriff auf das Umspannwerk in Kiew wird der APT-Gruppierung ELECTRUM (siehe Abschnitt 4.3.1.6) zugeschrieben, welche nach Einschätzung der Analysten in direkter Verbindung mit der APT-Gruppierung Sandworm (siehe Abschnitt 4.3.1.8) steht. /DRA20r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde oder wird der Sachverhalt bereits im Rahmen des Vorhabens verfolgt und ausgewertet. Zusätzlich dazu ist vorgesehen, die Informationslage zu diesem Sachverhalt im Rahmen des bei der GRS geplanten Anschlussvorhabens auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.8.2 Mirai – IT-Angriff 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 typischerweise unbemerkt. Die Infektion ist nicht persistent, sondern existiert vollständig im flüchtigen Speicher der infizierten Systeme. Daher reicht ein Neustart aus, um die Schadsoftware 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 Angriffe, 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.

Weitere Bearbeitung

Aus Sicht der GRS lässt sich keine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen auf Basis der derzeitigen Informationen ableiten. Diese Informationslage wird im bei der GRS geplanten Anschlussvorhaben auf Aktualität geprüft.

3.2.8.3 Kemuri Water – IT-Angriff auf eine Wasseraufbereitungsanlage

Übersicht

Im März 2016 wurde ein IT-Angriff auf eine namentlich nicht genannte Wasseraufbereitungsanlage bekannt, in dessen Rahmen es den Angreifern gelang, den Wasserdurchfluss durch Ventile und die Dosierung der zur Wasseraufbereitung eingesetzten Chemikalien zu manipulieren.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.2.8.4 Shamoon v2 – Weiterer IT-Angriff auf Saudi Aramco

Übersicht

Vier Jahre nach dem ersten Angriff mit Shamoon (siehe Abschnitt4.2.4.2) wurde eine neuere Version dieser Schadsoftware, Shamoon v2, im November 2016 im Rahmen einer weiteren Angriffswelle auf den saudi-arabischen Energiesektor eingesetzt.

Beschreibung

Eines der mit dieser neuen Version, Shamoon v2, angegriffenen Ziele war wie schon beim ersten Angriff Saudi Aramco /ZND18w01/. Im Vorfeld des koordiniert getriggerten Einsatzes der Wiper-Schadsoftware am 17. November 2016 erfolgte über einen längeren Zeitraum der Zugriff auf die Zielnetzwerke sowie die Ausbreitung der Schadsoftware in den Zielnetzwerken. Hierbei kamen einem Bericht von Symantec zufolge gestohlene Credentials zum Einsatz. /SYM16w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.9 2017

3.2.9.1 Ccleaner Hack – IT-Angriff über schadsoftwarebehaftete Ccleaner Version

Übersicht

Der als Ccleaner Hack bekanntgewordene IT-Angriff 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 IT-Angriff 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 IT-Angriff 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 IT-Angriffen unterschiedlichen Ausmaßes angewendet.

So beim Shadowhammer genannten IT-Angriff 2018 (siehe Abschnitt 4.2.10.1), 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 IT-Angriff, jedoch mit deutlich größerem Ausmaß und Wirkung, stellt der SolarWinds Angriff im Jahr 2020 dar (siehe Abschnitt 4.2.12.3). 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen. Auch wurde der Sachverhalt bereits im aktuellen Vorhaben in einem spezifisch auf IT-Angriffe über die Lieferkette ausgerichteten Bericht behandelt /GRS21r01/.

3.2.9.2 Triton/TriSIS – IT-Angriff 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 IT-Angriff ab, sondern stellt einen wesentlichen Baustein innerhalb eines komplexen, mehrstufigen IT-Angriffs dar.

Hierbei beschränken sich die Möglichkeiten von Triton/TriSIS nicht auf die Verhinderung des Eingriffs von Systemen, die Sicherheits-, Sicherungs- oder Schutzfunktionen ausführen, 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 4.2.11.3) und weitere Aktivitäten der Angreifer bekannt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt bereits im Rahmen des Vorhabens weiterverfolgt und ausgewertet. Nach eingehenden Beratungen zwischen BMU und GRS wurde zu dieser Thematik auch eine Weiterleitungsnachricht verfasst /GRS21i01/. Zusätzlich dazu ist vorgesehen, die Informationslage zu diesem Sachverhalt im Rahmen des bei der GRS geplanten Anschlussvorhabens auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.9.3 Karagany.B und Heriplor – Zweite IT-Angriffswelle durch APT Dragonfly

Übersicht

Bei den IT-Angriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Abschnitt 4.3.1.1) handelt es sich um hochentwickelte, mehrstufige Angriffe /BSI20i01/. Die APT-Gruppierung setzt dabei ein breites Spektrum an IT-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. 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 4.2.6.3, für Informationen zur APT-Gruppierung Dragonfly siehe Abschnitt 4.3.1.1). 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[2] 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/

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 4.2.6.3) 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 verfügbare 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/.

[2] Bei Red Teams handelt es sich um IT-Sicherheitsspezialisten, die zur Überprüfung von IT-Systemen Sicherheits- und Penetrationstests ausführen und dabei die Perspektive echter IT-Angreifer einnehmen.

Häufig greifen die Angreifer die eigentlich anvisierten Ziele nicht direkt an, sondern kompromittieren zunächst geeignete Zwischenziele in der Lieferkette.

Bei den eigentlich 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/.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.9.4 WannaCry – Globaler IT-Angriff

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/, [6].

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 Netzwerk kompromittieren /MIC17r01, BSI17i01/.

Der erste Schritt bei einer Infektion mit WannaCry erfolgt über eine eigenständig ausführbare 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 IT-Angriffen 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, bei der 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.

Weitere Bearbeitung

Aus Sicht der GRS lässt sich eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen auf Basis der derzeitigen Informationen nicht ableiten. Diese Informationslage wird im geplanten Anschlussvorhaben auf Aktualität geprüft.

3.2.9.5 Bad Rabbit – Globaler IT-Angriff

Übersicht

Im Oktober 2017 wurde bekannt, dass osteuropäische Unternehmen und Behörden vor allem in der Ukraine und Russland Opfer einer IT-Angriffswelle mit der Ransomware BadRabbit wurden. Betroffen waren unter anderem eine russische Nachrichtenagentur, die U-Bahn in Kiew und der Flughafen in Odessa. Es folgten außerdem weitere IT-Angriffe 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 IT-Angriffswerkzeug Mimikatz, um die lokalen Anmeldeinformationen der Benutzer oder Administratoren zu extrahieren. Dabei handelt es sich um ein für IT-Angriffe 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 Netzwerk im System des Opfers zu verbreiten und so weitere Computer zu infizieren. Dabei wird unter anderem eine modifizierte Version des Exploits EternalRomance 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 4.3.1.6) für die IT-Angriffe mit der Ransomware BadRabbit verantwortlich ist /NCS18i02/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.9.6 NotPetya – IT-Angriffe 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 IT-Angriffs die Strahlungsüberwachung manuell durchgeführt werden musste. Besonders betroffen von dem IT-Angriff 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 Unternehmen 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 IT-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 IT-Angriff einen direkten Bezug zu kerntechnischen Anlagen. /PRV17r01/

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen. Auch wurde der Sachverhalt bereits im aktuellen Vorhaben in einem spezifisch auf Supply-Chain-Angriffe ausgerichteten Bericht behandelt /GRS21r01/.

3.2.10 2018

3.2.10.1 Shadowhammer – IT-Angriff über schadsoftwarebehaftete ASUS Steuerungssoftware

Übersicht

Bei dem als Operation Shadowhammer genannten IT-Angriff handelt es sich um einen typverwandten oder womöglich Nachfolgeangriff zum beschriebenen Ccleaner IT-Angriff (siehe Abschnitt 4.2.9.1). 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 IT-Angriff vom Juni 2018 bis November 2018 und wurde dann am 29. Januar 2019 entdeckt. /SEN19r01/

Ähnlich zum Ccleaner IT-Angriff diente die initiale Schadsoftwarekomponente ausschließlich 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen. Auch wurde der Sachverhalt bereits im aktuellen Vorhaben in einem spezifisch auf Supply-Chain-Angriffe ausgerichteten Bericht behandelt /GRS21r01/.

3.2.10.2 IT-Angriff 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 Schadsoftware 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen. Auch wurde der Sachverhalt bereits im aktuellen Vorhaben in einem spezifisch auf Supply-Chain-Angriffe ausgerichteten Bericht behandelt /GRS21r01/.

3.2.10.3 Emotet – Globale IT-Angriffe 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) durchzuführen. 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. Da immer weniger Systeme mit den Command-and-Control-Server kommunizieren, ist davon auszugehen, dass die Aktivitäten von Emotet weiter zurückgehen und immer mehr Systeme von der Schadsoftware bereinigt werden. /BSI21r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS lässt sich eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen auf Basis der derzeitigen Informationen nicht ableiten. Diese Informationslage wird im geplanten Anschlussvorhaben auf Aktualität geprüft.

3.2.10.4 Operation Sharpshooter – Globale IT-Angriffe auf Behörden und Infrastruktur

Übersicht

Operation Sharpshooter wird eine große, international wirkende IT-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 IT-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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.10.5 Shamoon v3 – IT-Angriff 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, Indien 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden.

Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11 2019

3.2.11.1 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 Kernkraftwerks 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.2 IT-Angriff 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 IT-Angriff auf das indische Kernkraftwerk Kudankulam (2 russische DWR-Reaktoren) informiert /PUS19w01/.

Beschreibung

Die indischen Behörden leugneten einen solchen IT-Angriff zuerst, jedoch wurden Stück für Stück Informationen bekannt, welche aufzeigten, dass das Kernkraftwerk auf dem Niveau eines Domain Level Controllers (also zentralen Authentifizierungsservers) Anfang September 2019 kompromittiert worden war und damit die Angreifer einen weiten Zugriff zumindest auf das administrative Netzwerk des Kernkraftwerks erhalten hatten. /PKM20r01/

Der initiale IT-Angriff 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 Finanz-institute angewendet wurde. Die Herkunft des Trojaners und des gesamten IT-Angriffes 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 IT-Angriff betroffen und das administrative Netzwerk des Kraftwerks wurde von den Angreifern kompromittiert.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.3 Weiterer IT-Sicherheitsvorfall in Zusammenhang mit Triton/Trisis

Übersicht

Über den in Abschnitt 4.2.9.2 beschriebenen IT-Angriff 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 IT-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 IT-Angriffs, 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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Nach eingehenden Beratungen zwischen BMU und GRS wurde zu dieser Thematik auch eine Weiterleitungsnachricht verfasst /GRS21i01/. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.4 ZeroCleare – IT-Angriffe 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 Schadsoftware 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 Angriffen bereits eingesetzt wurden (siehe Abschnitte 4.2.4.2, 0, 4.2.9.5). ZeroCleare weist dabei Parallelen zur Schadsoftware Shamoon (siehe Abschnitt 4.2.4.2) 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.5 Dustman – IT-Angriff auf Bapco

Übersicht

Im Dezember 2019 wurde im Rahmen eines Angriffs auf das Bahrainische Ölunternehmen Bapco eine Wiper-Schadsoftware eingesetzt, die deutliche Parallelen zu Shamoon (siehe Abschnitte 4.2.4.2, 4.2.8.4, 0) und ZeroCleare (siehe Abschnitt 4.2.11.4) aufweist.

Beschreibung

IT-Sicherheitsanalysten halten die Wiper-Schadsoftware Dustman für eine direkte Weiterentwicklung von ZeroCleare. Wie die beiden Vorgänger setzt auch Dustman EldoS RawDisk ein, nutzt jedoch im Vorfeld unterschiedliche Exploits und Techniken zur Erlangung von Zugriff und zur Verbreitung. /ZDN20w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.6 IT-Angriff 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 IT-Angriffs 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 Aluminiummarkt. /BRI19w01/

Beschreibung

Die Schadsoftware LockerGoga wurde erstmals Anfang 2019 bei einem IT-Angriff 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 IT-Angriffe auf die europäischen bzw. US-amerikanischen Chemieunternehmen Hexicon und Momentive 2019 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 IT-Angriffs über Spear-Phishing oder Brute-Force-Angriffe bzw. über den ursprünglichen IT-Angriff der schadsoftwarebehafteten E-Mail erlangten. Das auf den Bereich IT-Sicherheit spezialisierte japanische Unternehmen Trend Micro geht davon 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 4.2.8.4) oder NotPetya (siehe Abschnitt 4.2.8.7). 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.7 IT-Angriffe über VPN-Schwachstellen

Übersicht

Auf der BlackHat 2019, einer jährlichen Konferenz zu Informationssicherheit und IT-Angriffen, wurde ein umfassender Vortrag über IT-Angriffe auf VPN-Clienten 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 Jahr 2019 sind eine Reihe von schwerwiegenden Schwachstellen in VPN-Clienten 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 IT-Angriffe 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 IT-Angriffe über VPN-Schwachstellen durch mehrere iranische APT-Gruppen 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.11.8 IT-Angriff 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 IT-Angriffs. Das Unternehmen verzeichnete eine 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 Stromerzeugungsstand-orten und dem Hauptkontrollzentrum. Die betroffenen Geräte sind Firewalls der amerikanischen Firma Cisco Systems, die als Sicherheitseinrichtungen gegen IT-Angriffe 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.12 2020

3.2.12.1 IT-Angriff 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 IT-Angriff auf einen nicht genannten Pipelinebetreiber. Im Rahmen des IT-Angriffes 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 abgeschaltet, die betroffenen IT-Systeme wurden getauscht und der Betrieb anschließend wieder aufgenommen.

Der IT-Angriff und seine Auswirkungen auf das leittechnische Netzwerk waren insbesondere dadurch möglich, dass der Betreiber der Pipeline kein IT-Sicherheitskonzept etabliert hatte und IT-Angriffe 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.

Weitere Bearbeitung

Aus Sicht der GRS lässt sich eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen auf Basis der derzeitigen Informationen nicht ableiten. Diese Informationslage wird im geplanten Anschlussvorhaben auf Aktualität geprüft.

3.2.12.2 SNAKE/EKANS – IT-Angriffe 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, indem 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 4.2.10.8).

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 IT-Angriffe mit der Schadsoftware Snake beobachtet. Laut /ABR20w01/ startete am 4. Mai 2020 eine weltweite Kampagne von IT-Angriffen, 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 IT-Angriff 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 IT-Angriff 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.12.3 SolarWinds – IT-Angriffe 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 IT-Angriffen 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 IT-Angriffen 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.

Das BSI veröffentlichte am 14.12.2020 eine Cyber-Sicherheitswarnung /BSI20i03/ zu den IT-Sicherheitsvorfällen, welche bereits am 28.12.2020 aktualisiert wurde /BSI20i04/.

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.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.13 2021

3.2.13.1 IT-Angriff auf Wasserwiederaufbereitungsanlage in Tampa, Florida

Übersicht

Im Februar 2021 wurde von der amerikanischen Bundespolizei FBI ein Bericht veröffentlicht, wie im Rahmen eines IT-Angriffes 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.

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 IT-Angriff folgend deaktiviert und es sollen Upgrades der Systeme durchgeführt werden. /NPR21r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS lässt sich eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen auf Basis der derzeitigen Informationen nicht ableiten. Diese Informationslage wird im geplanten Anschlussvorhaben auf Aktualität geprüft.

3.2.13.2 Centreon – IT-Angriffe über schadsoftwarebehaftete Centreon Produkte

Übersicht

Im Februar 2021 meldete die französische IT-Sicherheitsbehörde ANSSI die Entdeckung von IT-Angriffen auf mehrere französische Einrichtungen /HEI21w02/. Bei dem Angriff wurde die Monitoring- und Steuerungssoftware der Firma Centreon kompromittiert, welche die betroffenen Unternehmen einsetzen. Angaben der ANSSI zufolge gehen die ersten identifizierten Angriffe bis ins Jahr 2017 zurück. Im Bericht der ANSSI werden Parallelen zur Vorgehensweise der APT-Gruppierung Sandworm gezogen /ANS21r01/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS besteht hier eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen der Auftragsforschung weiterverfolgt und detailliert ausgewertet. Zusätzlich dazu ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.13.3 IT-Angriff 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 IT-Angriff betroffen.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.13.4 IT-Angriff über Codecov 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.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.13.5 Angriff auf Natanz

Übersicht

Im April 2021, einen Tag nach der Inbetriebnahme von 164 IR-6 Zentrifugen und dem Beginn von Tests mit IR-9 Zentrifugen, kam es in der iranischen Urananreicherungsanlage Natanz zu einer Explosion. Als Folge kam es anscheinend zu einem Stromausfall der internen Stromversorgung und physischen Schäden an weiten Teilen der geschützten, internen Stromversorgung von Natanz. Noch ist unklar, ob es sich um einen Cyberangriff, einen konventionellen Angriff oder einen kombinierten Angriff gehandelt hat. /NYT21w01, SEC21w06, TAG21w01/

Kerntechnischer Bezug

Ziel des Angriffs war die iranische Urananreicherungsanlage Natanz.

Weitere Bearbeitung

Eine Übertragbarkeit von Teilaspekten des Sachverhalts auch auf deutsche kerntechnische Anlagen und Einrichtungen kann aus Sicht der GRS auf Basis der derzeit vorliegenden Informationen nicht ausgeschlossen werden. Daher ist im Rahmen des bei der GRS geplanten Anschlussvorhabens vorgesehen, die Informationslage zu diesem Sachverhalt auf weitere Erkenntnisse zu überprüfen und die vorliegende Ersteinschätzung ggf. anzupassen.

3.2.13.6 IT-Angriff auf US-Pipelinebetreiber

Übersicht

Nach einem IT-Angriff auf einen US-amerikanischen Pipeline-Betreiber wurde der Betrieb der Pipeline, mit knapp 9000 km Länge eine der längsten Pipelines der USA, eingestellt.

Beschreibung

Die Colonial Pipeline Company gab am 07.05.2021 bekannt, Opfer eines IT-Angriffs mit Ransomware zu sein. Offen blieb zunächst allerdings, ob auch industrielle Steuerungssysteme vom Angriff direkt betroffen waren. Der Betreiber der Pipeline nahm auch nicht betroffene IT-Systeme, einschließlich Büro-IT und industriellen Steuerungssystemen, vorsorglich außer Betrieb. Die Colonial Pipeline, die pro Tag etwa 400 Millionen Liter Erdölprodukte wie Benzin, Diesel oder Heizöl von Texas in den Südosten und die Ostküste der USA transportiert, musste ihren Betrieb daraufhin einstellen, ebenso wie kleinere Pipelines des Betreibers. Auch Tage nach dem IT-Angriff war die Pipeline noch außer Betrieb und der Betreiber gab an, einen Plan für den Neustart zu erarbeiten. /SEC21w07, SEC21w08/

Die IT-Angreifer setzten dem FBI zufolge eine Ransomware ein, die unter dem Namen DarkSide bekannt ist /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/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Eine nähere Betrachtung des Sachverhalts wird im geplanten Anschlussvorhaben erfolgen.

3.3 APT-Gruppierungen

Hier beschrieben werden vornehmlich APT-Gruppierungen, die in Zusammenhang mit den in Abschnitt 4.2 beschriebenen IT-Angriffen stehen. Diese Liste ist keineswegs abdeckend.

3.3.1.1 APT29/Cozy Bear

Übersicht

APT29/Cozy Bear 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.

Weitere Bezeichnungen

Die APT-Gruppierung APT29 ist neben dem Namen Cozy Bear auch noch unter weiteren Namen bekannt. Hierzu zählen Office Monkey, Cozy Duke, The Dukes und Cozy Car. /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/. Manche Quellen bringen APT29/Cozy Bear auch in Verbindung mit den IT-Angriffen mit schadsoftwarebehafteten SolarWinds-Produkten, die Ende 2019 bekannt wurden /TWP20w01/; andere Analysten halten sich mit einer Attribuierung hierbei noch zurück.

3.3.1.2 APT 32/OceanLotus

Übersicht

Der APT-Gruppierung APT32 wird eine Nähe zur vietnamesischen Regierung nachgesagt. Sie ist seit mindestens 2014 aktiv und konzentriert ihre Angriffe auf die Bereiche Fertigungswirtschaft, Herstellung von Konsumprodukten und Gastgewerbe /CYB19w01, LIF19w01, AUT19w01/.

Weitere Bezeichnungen

Der APT-Gruppierung APT32 ist auch bekannt als SeaLotus, Ocean Lotus oder Ocean Buffalo.

Aktivitäten

Seit Februar 2019 werden der APT-Gruppierung zwischen fünf und 10 IT-Angriffe auf internationale Unternehmen der Automobilbranche zugerechnet. Nach Angaben des IT-Sicherheitsunternehmens FireEye geschah dies, um die Ziele der vietnamesischen Regierung im Bereich Automobilbau zu unterstützen, zum Beispiel durch das Sammeln wettbewerbsrelevanter Informationen. Zu den betroffenen Unternehmen zählen Toyota Japan, Toyota Australia, Toyota Vietnam, Toyota Thailand, BMW und Hyundai. /CYB19w01, LIF19w01, DOR19w01/

Für die IT-Angriffe setzte APT32 eine Kombination mehrerer IT-Angriffswerkzeuge für Windows- und Mac-Systeme ein.

Dazu zählen sowohl maßgeschneiderte, von der Gruppierung speziell entwickelte als auch frei verfügbare IT-Angriffswerkzeuge sowie ursprünglich nicht für maliziöse Zwecke entwickelte Software-Werkzeuge. Beispielsweise setzte APT32 die Software Cobalt Strike ein, das von Sicherheitsspezialisten zum Test von Netzwerken verwendet wird. Eigens von APT32 entwickelte Schadsoftware kam nur zum Einsatz, wenn für eine Aufgabe noch kein passendes IT-Angriffswerkzeug verfügbar war. Die APT-Gruppierung verwendete auch Shellcode und Loader-Komponenten um ihre Payloads zu verbergen. /CYB19w01, LIF19w01/

Bei den Angriffen ging APT32 ähnlich vor wie chinesische APT-Gruppierungen. Um sich Zugriff zum Netzwerk der Konzerne zu verschaffen, erstellte APT32 gefälschte Domänen. Diese konnten dann verwendet werden, um über Phishing-Mails Nutzerdaten zu stehlen und über diese, Zugriff auf das interne Firmennetzwerk zu erhalten. /AUT19w01/

Beim Angriff Ende Februar 2019 auf Toyota Australia, hatten die Angestellten keinen Zugriff mehr auf Cloud-basierte Systeme, darunter E-Mail-Server. Im März 2019 verschaffte sich APT32 über Toyota Japan Zugriff auf die Informationen von 3,1 Millionen Besitzern von Lexus- und Toyota-Automobilen. /DOR19w01/

3.3.1.3 APT 38/ Lazarus Group

Übersicht

Die Gruppe Lazarus ist eine der aktuell bekanntesten, ältesten und einflussreichsten APT-Gruppen, welche bisher der Öffentlichkeit bekannt geworden sind. Die Gruppe wird für einige der größten IT-Angriffe der Welt (Sony Pictures Hack, WannaCry) verantwortlich gemacht. Erste Erwähnungen der Gruppe existieren seit 2007, wobei der selbstgegebene und attribuierte Name der Gruppe regelmäßig wechselte, sie ist unter den Namen APT 38, Lazarus Group, Guardians of Peace, Whois Team, Gods Aposities, ZINC, HIDDEN COBRA und einigen weiteren bekannt. Die Lazarus Gruppe 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/

Beschreibung

Die erstmaligen Operationen der Lazarus Gruppe 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 IT-Angriffe 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 Gruppe 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 IT-Angriff auf den Filmanbieter Sony Pictures begann eine neue Phase der Aktivitäten der Lazarus Gruppe. Die Gruppe führte nun weltweit IT-Angriffe durch, welche als mit nordkoreanischen Interessen konvergierend beschrieben werden. Der Angriff auf Sony Pictures im Jahr 2014 gilt als umfassender gezielter IT-Angriff 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 IT-Angriff 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 Gruppe verantwortlich für den IT-Angriff war oder aber andere IT-Angreifer sich der Identität der Gruppe annahmen. /MED18r01/

In den Jahren nach dem IT-Angriff auf Sony-Pictures begann die Gruppe Lazarus nach bisherigen Erkenntnissen mit deutlich verstärkten IT-Angriffen auf Finanzdienstleister, Finanzunternehmen, Besitzer und Handelsbörsen von digitalen Währungen sowie auf Rüstungsunternehmen und genereller Informationsbeschaffung. So führte die Gruppe einen IT-Angriff auf die Zentralbank von Bangladesch aus, bei welchem die Gruppe insgesamt 81 Millionen Dollar erbeutete. Im Jahr 2018 konnte die Gruppe 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 Gruppe 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 Gruppe Lazarus zugeordnet. /INT19r01, AVI20r01/

Der IT-Angriff 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 IT-Angriffe von Lazarus. /INT19r01/

Die IT-Angriffe, welche Lazarus zugeschrieben werden, deuten auf ein umfassendes, sich ständig weiterentwickelndes Arsenal an Fähigkeiten der Gruppe. 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 erstelle 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 Gruppe Lazarus werden eine große Anzahl von IT-Angriffen zugeordnet, wobei die individuelle Zuordnung umstritten ist. Andere APT-Gruppen 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-Gruppen und die Unterscheidung von Lazarus und anderen Gruppen ist nicht immer vollständig möglich. So überschneiden sich die Tätigkeitsfelder der APT Kimsuky und der APT Lazarus oder es besteht Zusammenarbeit, weshalb beide Gruppen auch unter die Bezeichnung Hidden Cobra fallen könnten, welche aktuell von der amerikanischen Bundespolizei für Lazarus bzw. Kimsuky verwendet wird.

Kerntechnischer Bezug

Der IT-Angriff auf das indische Kernkraftwerk Kudankulam wird direkt der APT Lazarus zugeschrieben. Weiterhin richten sich die IT-Angriffe der Gruppe 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.

3.3.1.4 Avivore

Übersicht

Das IT-Beratungsunternehmen Context, das seit 1998 Unternehmen im Bereich IT-Sicherheit und Cyber-Bedrohungen berät, veröffentlichte am 3. Oktober 2019 Informationen über eine neu identifizierte APT-Gruppierung, die mutmaßlich für IT-Sicherheitsvorfälle in verschiedenen Unternehmen und Institutionen hauptsächlich aus den Bereichen der Luftfahrt-, Raumfahrt- und Verteidigungsindustrie in Großbritannien und Europa verantwortlich ist. Daneben wurden auch die Automobilindustrie und der (nukleare) Energiesektor als potenzielle Ziele genannt. /CON19w01/

Weitere Bezeichnungen

Derzeit werden der APT-Gruppierung Avivore keine weiteren Bezeichnungen zugeordnet.

Beschreibung

Die Aktivitäten der AVIVORE-Gruppierung wurden von Context seit Sommer 2018 verfolgt und lassen sich dessen Angaben zufolge bereits auf den Oktober 2015 zurückführen, wobei der Großteil der nachträglich untersuchten Aktivitäten zu Beginn des Jahres 2018 stattfand. Die IT-Angriffe erfolgten über die Kompromittierung der Lieferkette typischerweise über Software-Anbieter und Managed Services Provider. Betroffen waren neben nicht näher genannten großen multinationalen Unternehmen, die das Primärziel darstellten, auch insbesondere kleinere Ingenieur- oder Beratungsfirmen innerhalb der Lieferkette, die als Sekundärziele bezeichnet werden. Die Gruppierung nutzt nach Informationen von Context die gesamte Infrastruktur betroffener Sekundärziele aus, da diese oftmals Zulieferer für mehrere (große) Unternehmen sind und dabei häufig direkte Netzwerkverbindungen in Form von VPN-Verbindungen oder Programme zur Remote- und Zusammenarbeit einsetzen. Dabei nutzt AVIVORE diese Verbindungen zwischen dem eigentlichen Ziel und dem Zulieferer aus, um die oftmals ausgereifteren und aufwändigeren IT-Sicherheitsmaßnahmen großer Unternehmen zu umgehen.

Von Context wird AVIVORE als bisher unbekannter, auf nationalstaatlichem Niveau agierender Angreifer eingeschätzt, dessen Hauptziel Spionage ist und dessen zeitliche Aktivitäten im Bereich UTC +8 auf eine Gruppierung im asiatischen Raum hindeutet.

Die Vorgehensweise der Gruppierung beinhaltet neben der Tarnung als legitimer Benutzer auch das forensische Verwischen der eigenen Spuren. Sie zeigen laut Context detaillierte Kenntnisse über Schlüsselpersonen der mit für sie interessanten Projekten in Verbindung stehenden Unternehmen, wobei Arbeitszeiten und -muster einzelner Personen gezielt simuliert wurden, um unbemerkt agieren zu können. Das Angriffsmuster folgte demnach einem immer ähnlich ablaufenden Schema, bei dem zunächst der Zugriff auf das Opfer/Zielsystem mit Hilfe kompromittierter Benutzeranmeldedaten und legitimer externer Fernzugriffsdienste. Innerhalb des Zielsystems wurde dann durch den Missbrauch legitimer Tools oder mit Hilfe hochprivilegierter Administratorkonten eine Rechteausweitung durchgeführt, woraufhin weitere spezifische Angriffsschritte ermöglicht wurden und anschließend Hinweise auf das eigene Vorgehen – beispielsweise in Form von Ereignisprotokollen - stets sorgfältig entfernt wurden. Auf kompromittierten Systemen wurden mehrere Instanzen des Remote Access Trojaners PlugX gefunden, der bereits seit 2008 bekannt ist und Angreifern eine Backdoor zum Zielsystem bietet, wodurch weitere Angriffsschritte durchgeführt werden können. Die Schadsoftware wird von diversen APT-Gruppierungen verwendet. /CON19w01/

3.3.1.5 Dragonfly/Energetic Bear

Übersicht

Die Angreifergruppierung Dragonfly/Energetic Bear fällt seit einigen Jahren durch IT-Angriffe 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 IT-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 IT-Angriffen durch diese Gruppierung und der Veröffentlichung von Details zu den eingesetzten IT-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 auch 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.

3.3.1.6 Electrum

Übersicht

Die APT-Gruppierung ELECTRUM diente ursprünglich dazu die APT-Gruppierung Sandworm (siehe Abschnitt 4.3.1.6) 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 Angreifergruppe 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 IT-Angriff mit Crashoverride auf das ukrainische Stromnetz 2016, ist ELECTRUM vorerst nicht wieder öffentlich in Erscheinung getreten.

3.3.1.7 Kimsuky (teilweise beinhaltet in Hidden Cobra)

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-Gruppe Kimsuky veröffentlicht /CIS20i02/. Diese Gruppierung operiert weltweit, mutmaßlich bereits seit 2012, im Auftrag der nordkoreanischen Regierung. Hauptsächlich standen dabei Organisationen und Individuen in Südkorea, Japan und den USA im Fokus der Gruppe, 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.

Weitere Bezeichnungen

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

Aktivitäten

Die Gruppierung nutzt 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 die erstmals im November 2018 beobachtete, auf Microsoft Visual Basic skriptbasierte Malware Babyshark ein. Durch diese wird u. a. zusätzlicher Schadsoftwarecode heruntergeladen und es werden Informationen über das System gesammelt. Unter Ausnutzung verschiedener Exploits erfolgen zudem 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 Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines IT-Angriffs 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/.

3.3.1.8 Sandworm

Übersicht

Bei der APT-Gruppierung Sandworm handelt es sich um eine Gruppierung des russischen, militärischen Geheimdienstes GRU /BID20w01, 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 Gruppe auf IT-Angriffe 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 Gruppe der Name Sandworm gegeben wurde /ZDN14w01/. Nach der Entdeckung ihrer Tätigkeiten 2014 trat die Gruppe einige Monate lang nicht in Erscheinung bevor sie am 23.12.2015 /EWB20w01/ wieder einen viel beachteten IT-Angriff durchführte und mit der Schadsoftware Black Energy 3 (siehe Abschnitt 4.2.7.1) einen Blackout im ukrainischen Stromnetz verursachte. /FIR16w01/

Weitere Bezeichnungen

Die APT-Gruppierung Sandworm ist auch unter den Namen Quedagh und BlackEnergy bzw. BlackEnergy Group und Einheit 74455 bekannt. /BFV18r02/

Aktivitäten

Sandworm war in den letzten Jahren sehr aktiv. Im Juni 2017 wurden immense Schäden mit der Schadsoftware NotPetya (siehe Abschnitt 4.2.9.6) 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 Gruppe Zugriff auf neun Gigabyte der E-Mails der Präsidentschaftskampagne von Emmanuel Macron. 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. /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 Gruppe 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/

Nach Informationen der NSA /NSA20i01/ nutzt die Gruppe 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/

3.3.1.9 Tonto Team

Übersicht

Am 22. Oktober 2020 wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eine BSI-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 IT-Angriffe auf militärische, diplomatische und infrastrukturelle Ziele überwiegend in Osteuropa (Russland) und Asien (Japan, Südkorea) bekannt. Seit Anfang des Jahres wurden außerdem IT-Angriffe 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 soll der Remote Access Trojaner (RAT) Bisonal verwendet worden sein. 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-Gruppen 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 Gruppe 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 Gruppe 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/

3.3.1.10 Turla

Übersicht

Die ebenfalls russisch-basierte APT-Gruppierung Turla ist für IT-Angriffe zur Cyber-Spionage bekannt. Hierbei setzt sie häufig Spear-Phising-Angriffe, Watering-Hole-Attacken und Living-off-the-Land-Techniken ein.

Weitere Bezeichnungen

Turla ist ebenso unter den Namen Group 88, Belugasturgeon, Waterbug, VENOMOUS BEAR, Snake, Krypton und Uroboros 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.

Aktivitäten

Turla ist seit mindestens 2004 aktiv. Weltweite Aufmerksamkeit erlangte die APT-Gruppierung spätestens 2014 durch die unter dem Namen Epic Turla bekannt gewordenen IT-Angriffe (siehe Abschnitt 4.2.6.4). Turla ist auch dafür bekannt, immer wieder die Schadsoftwarekomponenten und IT-Angriffswerkzeuge sowie die Command-and-Control Infrastruktur anderer Angreifergruppierungen zu kapern und bei ihren eigenen Angriffen einzusetzen, wie beispielsweise 2019, als Turla IT-Angriffe auf britische Angriffsziele mit und über IT-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 IT-Angriffswerkzeuge von Turla bekannt.

3.3.1.11 Xenotime

Übersicht

Xenotime wurde 2017 mit Bekanntwerden der IT-Angriffe in Zusammenhang 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 mit Bekanntwerden der IT-Angriffe in Zusammenhang mit der Schadsoftware Triton/TriSIS 2017. Seither gab es mehrere, häufig nicht näher beschriebene mit Triton/TriSIS in Verbindung stehende IT-Angriffe, 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 Angriffe 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/.

4 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, IT-Angriffswerkzeuge, Schadsoftwarekomponenten, IT-Sicherheitsvorfälle, IT-Angriffe, und Aktivitäten von Advanced Persistent Threats regelmäßig aus. Das Gesamtbild, das sich im Rahmen dieses kontinuierlichen Screenings ergibt, macht folgendes deutlich: Das Spektrum der IT-Angriffswerkzeuge und Schadsoftwarekomponenten wird immer breiter und die einzelnen Werkzeuge ausgefeilter, während gleichzeitig die Angriffsoberfläche durch den wachsenden Einsatz von programmierbaren und rechnerbasierten Komponenten, die zunehmende Komplexität dieser Systeme und die zunehmenden Vernetzung gepaart mit einer steigenden Zahl noch unentdeckter oder neu erkannter aber noch ungepatchter Schwachstellen sowohl in industriellen Steuerungssystemen aber auch in der restlichen IT-Infrastruktur kontinuierlich größer wird. Zusätzlich muss sowohl von einem wachsenden Feld an Angreifern als auch von einer steigenden Komplexität der IT-Angriffe ausgegangen werden.

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 ebenfalls innerhalb der IT-Infrastruktur solcher Anlagen eingesetzt sind. Es zeigt sich wiederholt, dass es gerade auch Schwachstellen in gebräuchlicher Büro-IT sind, welche den IT-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 diesen 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.

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 IT-Angriffs mit der Schadsoftware Stuxnet bekannt gewordene LNK-Schwachstelle noch Jahre nach Veröffentlichung eines geeigneten Patches die von IT-Angreifern am häufigsten ausgenutzte Einzel-Schwachstelle. Darüber hinaus gibt es auch immer wieder Schwachstellen, mit deren Ausnutzung weitere, eigentlich bereits gepatchte Schwachstellen wieder zutage treten können, beispielsweise durch das Downgraden von Firm- und Softwareversionen.

Unter den in den vergangenen Jahren bekannt gewordenen IT-Sicherheitsvorfällen und IT-Angriffen befindet sich eine stetig wachsende Zahl an IT-Sicherheitsvorfällen und IT-Angriffen mit Relevanz für deutsche kerntechnische Anlagen und Einrichtungen. Dies schließt neben IT-Sicherheitsvorfällen mit direktem kerntechnischen Bezug sowohl IT-Angriffe auf andere kritische Infrastrukturen als auch IT-Angriffe auf industrielle Steuerungssysteme oder deren Lieferkette mit ein. Insbesondere IT-Angriffe auf und über die Lieferkette haben stark an Bedeutung gewonnen. Solche Supply-Chain-Angriffe haben hohes Gefährdungspotenzial, da sie auf die in Bezug auf IT-Sicherheitsmaßnahmen schwächeren Glieder in der Lieferkette zielen und damit letztlich die IT-Sicherheitsmaßnahmen der eigentlich anvisierten Ziele, die selbst meist besser gegen IT-Angriffe geschützt sind, umgehen. IT-Systeme in deutschen kerntechnischen Anlagen und Einrichtungen werden u. a. durch Vorgaben der *„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)“* /BMU13n03/ geschützt. Daraus abgeleitete Schutzmaßnahmen sollen IT-Angriffe auf die zu schützenden IT-Systeme verhindern. Einen wesentlichen Bestandteil dieser Schutzmaßnahmen bilden aber präventive Maßnahmen, die auf den Schutz der schutzbedürftigen IT-Systeme vor IT-Angriffen ausgerichtet sind. Eine bedeutsame Maßnahme besteht darin, um besonders wichtige IT-Systeme herum ein sogenanntes Air-Gap zu etablieren, durch das eine netzwerktechnische Trennung dieser IT-Systeme von den anderen IT-Systemen erreicht werden soll. Nicht nur bei Supply-Chain-Angriffen besteht allerdings die Möglichkeit, dass es den IT-Angreifern gelingt, die realisierten Sicherungsmaßnahmen teilweise zu umgehen und auch Air-Gaps zu überspringen.

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. Dies hat sich in den letzten Monaten besonders deutlich bei den IT-Angriffen über schadsoftwarebehaftete SolarWinds Produkte gezeigt.

Ein weiterer, zunehmend an Bedeutung gewinnender Angriffstyp, ist der Ransomware-Angriff. Gerade bei Ransomware 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.

Grundsätzlich zeigt die gegenwärtige IT-Bedrohungslage: Eine große Zahl der beobachteten IT-Angriffe ist mehrstufig, komplex und beinhaltet den Einsatz verschiedenster IT-Angriffswerkzeuge und Schadsoftwarekomponenten. Manche IT-Angriffe scheinen lediglich zu Testzwecken durchgeführt zu werden, andere wiederum nur, um durch die Demonstration von Fähigkeiten eine Drohkulisse aufzubauen. Die Mehrheit der IT-Angriffe folgt allerdings anderen Zielen, beispielsweise dem Ziel, finanziellen Gewinn zu erzielen, Manipulationen durchzuführen oder Informationen auszuspähen. IT-Angriffe 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. Da industrielle Steuerungssysteme insbesondere in kerntechnischen Anlagen und Einrichtungen gut geschützt und nicht direkt von außen erreichbar sind, gibt es für IT-Angreifer prinzipiell drei Möglichkeiten, zu ihnen vorzudringen. Zum einen das Überwinden mehrerer Barrieren und Aushebeln gestaffelter IT-Sicherheitsmaßnahmen, um sich langsam Stück für Stück von außen zu den industriellen Steuerungssystemen vorzuarbeiten. Zum anderen die Umgehung der äußeren Maßnahmen und Barrieren durch einen Angriff über die Lieferkette der industriellen Steuerungssysteme.

Darüber hinaus ist auch ein IT-Angriff mit Hilfe eines – wissentlich oder unwissentlich agierenden – Innentäters denkbar, wobei die ersten beiden Möglichkeiten deutlich häufiger beobachtet werden als letztere. Daher muss neben der Lieferkettenproblematik auch möglichen Einfallstoren, die IT-Angreifern von außen einen Erstzugriff auf die IT-Infrastruktur ermöglichen könnten, besondere Aufmerksamkeit gewidmet werden. Hierbei spielen insbesondere Spear-Phishing-Angriffe, Watering-Hole-Angriffe, Social Engineering und andere Formen von Credential Harvesting eine große Rolle. Dies ist insbesondere als kritisch anzusehen, da dabei gezielt Mitarbeiter als Ziel fokussiert werden, 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 IT-Sicherheitsbewusstsein sowie das unzureichende Verständnis für die Vielzahl der Gefahren.

Kritische Infrastrukturen sind inzwischen häufig von IT-Angriffen betroffen. Auch rückt die Ausspähung, Manipulation oder Sabotage von industriellen Steuerungssystemen immer stärker in den Fokus von IT-Angreifern. Gerade für und insbesondere in weiterführenden Angriffsschritten ist gezielte Spionage in Bezug auf industrielle Steuerungssysteme keine Seltenheit. Insgesamt sind industrielle Steuerungssysteme zunehmend von IT-Angriffen betroffen. Die beobachteten IT-Sicherheitsvorfälle und IT-Angriffe der vergangenen Jahre zeigen sehr deutlich, dass es eine ganze Reihe von Angreifer-Gruppierungen gibt, die durchaus in der Lage sind, komplexe und über lange Zeiträume unentdeckte IT-Angriffe 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.

In den vergangenen Jahren ist das Feld an Advanced Persistent Threats stetig gewachsen. Zu beobachten sind hierbei teils seit vielen Jahren aktive Gruppierungen, die immer komplexere IT-Angriffe durchführen, aber auch eine hohe Zahl an neueren APT-Gruppierungen. Viele dieser Gruppierungen verbreitern ihren Fokus nach und nach, beispielsweise von einem kritischen Infrastruktursektor auf weitere Sektoren. Wie breit der Fokus der Angreifer ist, hat hierbei jedoch nicht zwangsläufig etwas mit den eingesetzten Angriffstechniken und der Zahl der Angriffsziele zu tun.

So gibt es Angreifer, die bei einem breiten Spektrum von Angriffszielen äußerst zielgenau arbeiten, während es auch stark fokussierte Angreifer gibt, die nicht vor ersten Angriffsschritten nach dem „Gießkannenprinzip“ zurückschrecken. Insgesamt ist zu beobachten, dass von vielen Angreifern Kollateralschäden durchaus in Kauf genommen werden.

Prinzipiell zählen auch alle deutschen kerntechnischen Anlagen zu der Art Angriffsziel, auf die sich die Gruppierung der Angreifer mit ihren bisherigen IT-Angriffen und weiteren Aktivitäten konzentrieren könnte. Zudem sind auch in deutschen kerntechnischen Anlagen programmierbare und rechnerbasierte industrielle Steuerungssysteme und -komponenten vorhanden, so dass grundsätzlich hochentwickelte IT-Angriffe auf diese unterstellt werden können. Grundsätzlich bietet die korrekte und vollständige Umsetzung der SEWD-Richtlinie IT aus Sicht der GRS weitreichenden Schutz vor den Gefahren solcher hochentwickelter IT-Angriffe. In deutschen Kernkraftwerken fordert die SEWD-Richtlinie IT eine Trennung zwischen den betrieblichen und sicherheitstechnisch wichtigen Leittechniksystemen durch physische, technische und administrative Maßnahmen. 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, da die IT-Systeme verschiedener IT-Schutzbedarfsklassen konsequenter voneinander getrennt sind. Insgesamt ist allerdings zu beachten, dass auch die korrekte und vollständige Umsetzung der SEWD-Richtlinie IT – oder eines beliebigen anderen Regelwerks zur IT-Sicherheit – zwar einen weitreichenden, aber keinen vollumfänglichen Schutz vor den Gefahren eines langfristig angelegten IT-Angriffs 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 IT-Angriffe 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 Detection Evasion und nehmen diesbezüglich erheblichen zeitlichen, finanziellen und personellen Aufwand auf sich.

In Bezug auf die eingesetzten IT-Angriffswerkzeuge und Schadsoftwarekomponenten ist deutlich zu beobachten, dass viele IT-Angriffswerkzeuge über Jahre hinweg weiterentwickelt und verfeinert werden. Immer weniger IT-Angriffswerkzeuge und Schadsoftwarekomponenten werden von Grund auf neu entwickelt, sondern entstehen auf Basis anderer, häufig auch öffentlich oder im Darknet verfügbarer IT-Angriffswerkzeuge. Neben IT-Angriffswerkzeugen und Schadsoftwarekomponenten, die nur von einer Angreifer-Gruppierung eingesetzt werden, gibt es auch viele, die von verschiedensten Angreifern genutzt werden. Diesbezüglich wird auch immer wieder die Zusammenarbeit von APT-Gruppierungen und teilweise auch das Kapern von IT-Angriffswerkzeugen und der entsprechenden IT-Infrastruktur einer APT-Gruppierung durch eine andere APT-Gruppierung beobachtet. Auch gibt es einen regen Handel mit IT-Angriffswerkzeugen und Schadsoftware. Sehr häufig ist auch der maliziöse Einsatz von an sich nicht maliziösen IT-Werkzeugen und der Einsatz sogenannter Living-off-the-Land-Techniken zu beobachten.

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 IT-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 IT-Angriff vorzubereiten und durchzuführen. Dies schließt beispielsweise terroristische Vereinigungen ein. 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 Vulnerabilitiesss, impact on System 800xA, Compact HMI and Controler 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 campaigntargets 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 dattaque du mode opératoire Sandworm ciblant des serveurs Centreon, v. 1.0, 27.01.2021, TLP:White

/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]

/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

/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 SourceNetzwerkstacks (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]

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

/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 (AMNE-SIA: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

/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]

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

/CON19w01/ Context, AVIVORE Hunting Global Aerospace through theSupply 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 Spyware Suite, https://www.cybereason.com/, 02.11.2020 [abgerufen am 21.12.2020]

/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. Higgins, 11 September 2012, https://www.darkreading.com [abgerufen am 22.04.2021]

/DAR21w01/ Dark Reading, More SolarWinds Attack Details Emerge, K. Higgins, January 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]

/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]

/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 APTGruppen 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

/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 Report 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]

/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 dicsover nine new vunlerabilities 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 SIMATle WinCC und SIMATlC 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

/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

/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]

/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

/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]

/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

/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]

/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 spread-ing, 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 Vorporation, Lesson Learned, Risks Posed by Firewall Firmware Vulnerabilities, https://www.nerc.com/, 04.9.2021[abgerufen am 08.05.2021]

/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

/NPR21r01/ NPR: FBI Called In After Hacker Tries To Poison Tampa-Area City's Water With Lye, Februar 2021

/NSA20i01/ NSA, National Security Agency, Cybersecurity Advisory, Sandworm Actors Exploiting Vulnerability in Exim Mail Transfer Agent, 28 May 2020

/NVD18w01/ National Vulnerability Database NVD, CVE 2017-0144 Details, 20 June 2018, 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]

/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.

/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]

/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 litte 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

/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

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

/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 Aagainst 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

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

/TRE14w01/ Trendmicro, 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: Information 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, 208

/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]

/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 Attributions-Aussagen 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 Phising) mit dem Ziel, sich innerhalb eines IT-Angriffs 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 Erstel-lung 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-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 IT-Angriffe, 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 IT-Angriffen typischerweise diejenigen Schadsoftwarekomponenten, die maliziöse Aktivitäten (Manipulation von Daten oder Prozessen, Diebstahl von Nutzerdaten, Spionage etc.) ausführen. Ein IT-Angriff 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 IT-Angriffe 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 bereit stehen. /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 IT-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/

Abkürzungen

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

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Forschungszentrum
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 978-3-949088-36-0