IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

2024

GRS - 850

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

2024

Robert Arians
Henriette Gatz
Christian Korn
Claudia Quester
Oliver Rest
Alexander Schug
Birte Ulrich

August 2025

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4724R01610 durchgeführt.

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

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

GRS - 850
ISBN 978-3-911727-43-3

Deskriptoren

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

Kurzfassung

Die IT-Bedrohungslage in Bezug auf kritische Infrastrukturen und industrielle Steuerungssysteme wird von der GRS kontinuierlich verfolgt, ausgewertet und in einem jährlichen Bericht dargestellt. Der Fokus liegt dabei insbesondere auf Cyberangriffen mit Bezug zu kerntechnischen Anlagen und Anlagen im Umgang mit radioaktiven Stoffen sowie Cyberangriffe auf den Energiesektor. Für das Jahr 2024 wurden darüber hinaus sieben weitere Themenschwerpunkte identifiziert, die in den vergangenen Monaten die IT-Bedrohungslage signifikant geprägt haben oder eine besondere Relevanz besitzen. Hierzu zählen neben Cyberangriffen in Zusammenhang mit geopolitischen Spannungsfeldern auch KI-gestützte und KI-gesteuerte Cyberangriffe, Cyberangriffe auf kryptographische Verfahren und Cyberangriffe auf Fahrzeuge. Darüber hinaus wurden Supply Chain Angriffe im Zusammenhang mit IT-Dienstleistern und Netzwerküberwachungssysteme, physische Angriffe auf IT-Systeme und IT-Angriffe mit physischen Auswirkungen sowie die Angreifbarkeit in der Softwareentwicklung näher betrachtet. Zusätzlich spielen Schwachstellen in industriellen Steuerungssystemen als Angriffsvektor für Cyberangriffe eine wichtige Rolle. Der Bericht beschäftigt sich zudem mit den Aktivitäten von ausgewählten Advanced Persistent Threats. In den Anhängen befinden sich Informationen zu relevanten Schwachstellen, Angriffswerkzeugen, IT-Sicherheitsvorfällen und Cyberangriffen. Da es sich dabei um von Bericht zu Bericht weitergeführte und ergänzte Anhänge handelt, umfassen sie im Gegensatz zum Hauptteil des Berichtes einen deutlich längeren Betrachtungszeitraum als nur das Jahr 2024.

Abstract

GRS continuously screens and analyses the cyber threat landscape, focusing on industrial control systems and critical infrastructures. Special attention is paid to cyberattacks targeting the nuclear or energy sector. Additionally, this summary report for 2024 comprises seven main topics including geopolitically motivated cyberattacks, AI-assisted or AI-controlled cyberattacks, cyberattacks on cryptographic processes and cyberattacks on vehicles as well as supply chain attacks in connection with IT service providers and network monitoring systems, physical attacks on IT systems and cyberattacks causing physical effects, as well as vulnerabilities in the software development process. Emphasis is also placed on ICS vulnerabilities as attack vector. Moreover, this report includes an overview concerning relevant advanced persistent threat activities. The appendices summarize relevant vulnerabilities, cyber-attack tools, incidents and cyberattacks. As living appendices, they cover a much longer period than 2024 alone.

Inhaltsverzeichnis

1 Einleitung

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

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

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

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

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

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

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

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

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

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

Die IT-Bedrohungslage entwickelt sich sehr dynamisch. Es werden zunehmend Cyberangriffe beobachtet, wobei industrielle Steuerungssysteme stärker in den Fokus der Angreifer rücken. Die Bandbreite bei den eingesetzten Schadsoftwarekomponenten reicht von einfachen, aber bei erfolgreichem Einsatz häufig dennoch sehr effektiven Schadsoftwarekomponenten bis hin zu ausgefeilten Schadsoftwarekomponenten für mehrstufige, komplexe Cyberangriffe. Hierbei ist allerdings zu bemerken, dass ausgefeilte Schadsoftwarekomponenten bei ihrem Einsatz häufig unentdeckt bleiben, weil die Angreifer auf persistenten, langfristigen Zugriff auf Systeme und Informationen großen Wert legen und daher erheblichen Aufwand im Bereich Detektionsevasion betreiben. Dies stellt einen erheblichen Unterschied zu Cyberangriffen beispielsweise mit Ransomware[1] dar, bei denen eine zeitnahe Entdeckung des Angriffs von den Angreifern nicht nur einkalkuliert wird, sondern erwünscht ist. Der Aufwand, den Angreifer betreiben, um unentdeckt zu bleiben, zeigen auch während des Softwareentwicklungsprozesses eingebrachte Manipulationen. Angriffe auf den Softwareentwicklungsprozess sind meist deutlich aufwändiger als Angriffe auf Prozesse zur Verteilung bereits entwickelter Software, bieten aber für Angreifer den großen Vorteil, dass diese deutlich schwerer zu erkennen sind.

Die bei den beobachteten Cyberangriffen verwendeten Angriffstechniken sind sehr vielfältig. Der Trend, dass Anwendungen künstlicher Intelligenz einen rasanten Fortschritt sowohl in Bezug auf ihre Fähigkeiten als auch in Bezug auf ihre Anwendungsmöglichkeiten und Verbreitung erleben, hat sich auch im Jahr 2024 fortgesetzt. Mit den stetig wachsenden Funktionen und Fähigkeiten von KI-Modellen wachsen auch die Möglichkeiten, diese im Rahmen von Cyberangriffen einzusetzen. Ebenfalls zunehmend sind

[1] 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/

Angriffe auf kryptografische Verfahren, die darauf abzielen, Schwachstellen in der Methodik und Etablierung von Verschlüsselungen zu nutzen, um die verschlüsselten sensiblen Informationen zu erlangen. Aufgrund der Vielzahl von IT-Systemen und der damit deutlich komplexer gewordenen Netzwerkarchitekturen von Fahrzeugen rücken auch Cyberangriffe auf Fahrzeuge stärker in den Fokus. Diese werden als hochgradig problematisch angesehen, da sie den Straßenverkehr gefährden und potenziell lebensgefährlich für Verkehrsteilnehmer sein können.

Bei den hier beobachteten Angreifergruppierungen wurden vielfältige Aktivitäten und häufig eine breite Streuung bei den Angriffszielen festgestellt. Insgesamt ist von einem breiter werdenden Feld an Angreifern auszugehen, da viele der beobachteten Angreifergruppierungen bereits seit Jahren aktiv sind und neue Angreifergruppierungen hinzukommen. Eine bereits im vergangenen Jahr deutlich gewordene Entwicklung betrifft APT-for-hire, wobei etablierte, befähigte Angreifer ihre Fähigkeiten und Kenntnisse gegen Bezahlung zur Verfügung stellen. Hinzu kommt, dass auch viele Angriffswerkzeuge nicht mehr nur ihren Entwicklern, sondern einem deutlich größeren Angreiferkreis zur Verfügung stehen, der häufig selbst nicht in der Lage gewesen wäre, diese Werkzeuge in Anbetracht ihrer Komplexität zu entwickeln.

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

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

Für die IT-Sicherheit kommt damit der regelmäßigen Analyse der Bedrohungslage, aber auch der Bewertung des Standes von Wissenschaft, Technik und Erkenntnis zur Prävention und Detektion von Cyberangriffen sowie zur Reaktion auf Cyberangriffe, eine besondere Bedeutung zu. Die GRS verfolgt daher die Entwicklung der IT-Bedrohungslage für industrielle Steuerungssysteme und kritische Infrastrukturen, relevante IT-Sicherheitsvorfälle, Cyberangriffe, Schwachstellen, Angriffswerkzeuge, Schadsoftwarekomponenten sowie APTs kontinuierlich. Aufbauend auf diesem kontinuierlichen Screening der IT-Bedrohungslage, werden die wichtigsten Vorkommnisse in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen ausgewählt und vor dem Hintergrund der IT-Bedrohungslage ausgewertet. Eine kurze Beschreibung der betrachteten Vorkommnisse findet sich im Anhang dieses Berichtes.

Typischerweise werden die Auswertungen der relevanten Vorkommnisse bereits kurz nach Bekanntwerden der zugrunde liegenden Vorfälle oder Angriffe erstellt, um möglichst zeitnah ihre Relevanz für die IT-Sicherheit deutscher kerntechnischer Anlagen abzuschätzen, d. h. die erste Auswertung erfolgt häufig zu einem Zeitpunkt, an dem die forensischen Analysen der IT-Sicherheitsvorfälle oder sogar die entsprechenden Angriffswellen selbst noch andauern. Die forensische Analyse eines IT-Sicherheitsvorfalls kann sich hierbei ebenso hinziehen, wie die Untersuchung der von den Angreifern eingesetzten Schadsoftwarekomponenten und Angriffswerkzeuge. Gleiches gilt bei Schwachstellen in industriellen Steuerungssystemen und weiteren relevanten IT-Systemen, und zwar sowohl für deren Ausnutzung und das Bekanntwerden entsprechender Exploits[2] als auch für Patches und Updates zum Schließen oder Mitigieren der Schwachstellen. Dabei bedeutet die Entdeckung eines Cyberangriffs häufig nicht dessen

[2] 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/

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 ergänzt, angepasst oder vollständig überarbeitet werden müssen. Um dieser Dynamik gerecht zu werden, handelt es sich bei den im vorliegenden Bericht wiedergegebenen Beschreibungen daher nicht um abschließende Bewertungen der jeweiligen Vorkommnisse, sondern um eine Momentaufnahme. Aufgrund dieser sich unter Umständen auch noch Jahre nach dem ersten Bekanntwerden ändernden Informationslage zu IT-Sicherheitsvorfällen, Angriffen und Schwachstellen müssen auch bisherige Auswertungen auf ihre Aktualität geprüft und ggf. angepasst werden. Daher werden die Anhänge dieses Berichts von Jahr zu Jahr weitergeführt und bei Bekanntwerden relevanter Informationen entsprechend ergänzt oder angepasst. Aus diesem Grund umfassen die Anhänge des Berichtes im Gegensatz zu dessen Hauptteil einen deutlich längeren Betrachtungszeitraum, aktuell die Jahre 2007 bis 2024.

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

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

2 IT-Bedrohungslage

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

- **Schwachstellen** in industriellen Steuerungssystemen und in für kritische Infrastrukturen relevanten IT-Systemen,
- **Angriffswerkzeuge**, die unabhängig von Cyberangriffen bekannt werden,
- **IT-Sicherheitsvorfälle und Cyberangriffe** einschließlich der dabei eingesetzten Angriffswerkzeuge und Schadsoftwarekomponenten sowie
- **APT-Gruppierungen** (Advanced Persistent Threat[3] – fortgeschrittene andauernde Bedrohung) und ihre Aktivitäten.

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

- **Supply-Chain-Angriffe im Zusammenhang mit IT-Dienstleistern und Netzwerküberwachungssystemen** – Supply-Chain Angriffe sind in Anbetracht der zunehmenden Digitalisierung eine der größten Herausforderungen für die Gewährleistung der Cybersicherheit. Dabei wird das eigentliche Angriffsziel nicht direkt angegriffen, sondern zunächst ein Zwischenziel in der Lieferkette kompromittiert. Vor allem bei gut geschützten Angriffszielen wählen Angreifer diesen Weg, um Sicherheitsmaßnahmen beim eigentlichen Angriffsziel zu umgehen. Eine besondere Bedeutung kommt dabei Angriffen auf IT-Dienstleister zu, da durch einen solchen Angriff eine Vielzahl möglicher Opfer erreicht werden können. Angriffe auf ein Netzwerküberwachungssystem, welches eingesetzt wird, um Angriffe zu erkennen, kann Angreifern

[3] 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

die unbemerkte Ausführung weiterer Angriffsschritte sowie weitreichende Zugriffsmöglichkeiten auf das Zielsystem ermöglichen.

- **Angreifbarkeit in der Softwareentwicklung** – Angriffe in den frühen Phasen des Lebenszyklus eines Softwareproduktes können eine erhebliche Gefahr darstellen. Bereits während der Softwareentwicklung vorgenommene Manipulationen sind für den Endanwender nur sehr schwer zu erkennen, insbesondere wenn das manipulierte Softwareprodukt vom Hersteller offiziell freigegeben wird. Ein solcher Angriff kann viele Sicherheitsmaßnahmen zur Detektion der Manipulationen umgehen.

- **KI-gestützte und KI-gesteuerte Cyberangriffe** – Die Fähigkeiten von Anwendungen künstlicher Intelligenz haben in den letzten Jahren einen rasanten Fortschritt erreicht. Insbesondere im Bereich Social Engineering wird KI bereits stark eingesetzt, um hochspezifizierte, personalisierte, automatisierte oder auch stark skalierte Angriffe auszuführen. Aber auch in anderen Bereichen wie Angriffen auf datentechnische Systeme oder bei der Entwicklung von Schadsoftware ist KI in der Lage, Angriffe effizienter zu machen.

- **Cyberangriffe auf kryptografische Verfahren** – Cyberangriffe auf kryptografische Verfahren sind für Angreifer hochinteressant, da sie durch solche Angriffe an sensible Informationen gelangen können, die eigentlich mit diesen Verfahren vor unbefugten Zugriffen geschützt werden sollen. Bei solchen Angriffen werden Schwachstellen bei Erzeugung und Verbreitung von Schlüsseln oder Schwachstellen in der Programmierung der Verschlüsselungsprogramme genutzt.

- **Cyberangriffe auf Fahrzeuge** – Die Nutzung von IT-Systemen in modernen Fahrzeugen nimmt weiter zu, wobei oftmals eine Vielzahl von Systemen miteinander vernetzt sind und untereinander kommunizieren können. Cyberangriffe auf Fahrzeuge sind hochgradig problematisch, da durch solche Angriffe der Straßenverkehr gefährdet werden kann und es zu potenziell lebensgefährlichen Situationen für Verkehrsteilnehmer kommen kann. Techniken wie drahtlose Kommunikation und Standortbestimmung erhöhen dabei die Angriffsoberfläche für Angriffe aus der Ferne zusätzlich. Im kerntechnischen Bereich besitzen Cyberangriffe auf Fahrzeuge und die dabei eingesetzten Techniken eine besondere Relevanz für die Beförderung von kerntechnischem Material oder radioaktiven Stoffen.

- **Cyberangriffe auf den Energiesektor** – Die Energieversorgung ist in vielerlei Hinsicht die Achillesferse der modernen Gesellschaft. Eine Unterbrechung der Energieversorgung ist mit Rückwirkungen auf eine Vielzahl von Anlagen und Tätigkeiten

verbunden. Cyberangriffe auf den Energiesektor stellen daher eine wachsende Bedrohung dar, auch aufgrund der Verfügbarkeit speziell ausgelegter Schadsoftware für Angriffe auf Systeme, die im Bereich der Energieversorgung eingesetzt werden.

- **Cyberangriffe in politischen Spannungsfeldern** – Cyberangriffe kommen heute in praktisch allen politischen Spannungsfeldern zum Einsatz. Bereits vor dem Hintergrund der wachsenden Spannungen zwischen Russland und der Ukraine und noch einmal seit Kriegsausbruch ist es zu einem starken Anstieg der politisch und strategisch motivierten Cyberangriffe nicht nur in der Ukraine, sondern auch darüber hinausgekommen. Weitere Spannungsfelder, in denen es zu Cyberangriffen gekommen ist und die beispielhaft beleuchtet werden, sind der Krieg in Gaza, die Konflikte zwischen China und Japan, Nordkorea und Südkorea sowie Iran und Israel.
- **Physische Angriffe auf IT-Systeme und IT-Angriffe mit physischen Auswirkungen** – Insbesondere für kritische Infrastrukturen ist die physische Sicherheit von großer Bedeutung. Der alleinige Blick auf die Cybersicherheit reicht nicht aus, um IT-Systeme gegen die wachsende Bedrohungslage zu schützen, da IT-Systeme auch durch physische Angriffe in Mitleidenschaft gezogen werden können. Andererseits können IT-Angriffe auch gezielt Schäden in der physischen Welt hervorrufen, wie Beschädigungen oder Zerstörungen verfahrenstechnischer Komponenten.

Diese Themenschwerpunkte werden in den folgenden Abschnitten 2.1 bis 2.8 vorgestellt.

2.1 Supply-Chain-Angriffe im Zusammenhang mit IT-Dienstleistern und Netzwerküberwachungssystemen

Supply-Chain-Angriffe sind in Anbetracht der andauernden und zunehmenden Digitalisierung und Globalisierung weltweit in nahezu sämtlichen Bereichen inklusive der Lieferketten von IT-Systemen und industriellen Steuerungssystemen für die Gewährleistung der Cybersicherheit eine der größten Herausforderungen. Die steigende Komplexität von Software, Hardware und IT-Dienstleistungen in diesem Zusammenhang bietet Angreifern vielfältige Möglichkeiten, insbesondere innerhalb der Lieferkette von Komponenten oder Diensten. In den letzten Jahren beobachtete Supply-Chain-Angriffe auf lokale und globale Unternehmen bzw. Produkte, die weltweit große Aufmerksamkeit erfuhren, verdeutlichen die potenziell verheerenden Folgen und weitreichenden Auswirkungen derartiger Angriffe.

Grundsätzlich betrifft die Frage der IT-Sicherheit in der Lieferkette alle IT-Systeme, die in kritischen Infrastrukturen und kerntechnischen Anlagen und Einrichtungen eingesetzt werden. Dies beinhaltet sowohl Software- als auch Hardwarebestandteile, die in der Regel durch verschiedene und häufig mehrere Zulieferer bereitgestellt werden. Zudem sind nicht zwangsläufig alle Softwarebestandteile, die für ein IT-System erforderlich sind, lokal auf dem betreffenden IT-System vorhanden, sodass externe Softwarebestandteile genutzt werden, die über entsprechende Abhängigkeiten eingebunden sind. Die Lieferkette eines IT-Systems setzt sich typischerweise aus mehreren Hard- bzw. Softwarebestandteilen mit eigenen unterschiedlichen Lieferketten zusammen, von denen jedes einzelne für sich allein genommen als Zwischenziel eines potenziellen IT-Angriffs dienen kann. Zudem sind Angriffe auf die Lieferkette eines IT-Systems nicht auf die „erste Lieferung“ eines IT-Systems bzw. seiner Komponenten beschränkt, sondern umfassen den gesamten Lebenszyklus. Dies beinhaltet u. a. neben der Konzeptions-, Entwurfs- und Entwicklungsphase auch Betrieb, Wartung und Pflege nach der Auslieferung sowie die Ausmusterung und Entsorgung. Somit umfasst das Thema IT-Sicherheit in der Lieferkette nicht nur der Erstlieferung einer Soft- oder Hardware, sondern auch jegliche im weiteren Verlauf erfolgte weitere Hardware- und Software-Lieferung, -Aktualisierung oder -Modifizierung, beispielsweise im Rahmen von Instandhaltungen oder zu Update-, Patch-, Konfigurations- und Parametrierzwecken. Cyberangriffe im Zusammenhang mit der Lieferkette unterscheiden sich dementsprechend grundsätzlich dadurch, an welcher Stelle der Lieferkette, d. h. in welcher Phase des Software- bzw. Hardwarelebenszyklus, ein Angriff erfolgt, wobei ein Angriff nicht auf eine Phase beschränkt sein muss.

Durch die Abhängigkeiten und Wechselwirkungen der einzelnen Schritte im Lebenszyklus eines IT-Systems, der Involvierung von in der Regel mehreren Zulieferern und der sich dadurch bietenden unterschiedlichen Angriffsmöglichkeiten, liegen bei Supply-Chain-Angriffen die Möglichkeiten zur Verhinderung, Abwehr oder Unterbrechung der Angriffe nur bis zu einem gewissen Grad im Einflussbereich des potenziellen Angriffsziels. Beispielsweise können Betreiber kritischer Infrastrukturen indirekt von IT-Angriffen über die Lieferkette betroffen sein, wenn mit den Betreibern in Verbindung stehende IT-Dienstleister Ziele solcher Angriffe sind. Zudem pflegen Hersteller bzw. IT-Dienstleister unter Umständen einen unterschiedlichen Umgang mit IT-Angriffen und Schwachstellen, wobei insbesondere die Kommunikation infolge solcher IT-Sicherheitsvorfälle oftmals nicht optimiert ist und Informationen nur verspätet, nicht vollständig oder gar nicht weitergegeben werden. Für Betroffene ist eine gesicherte und aktuelle Informationslage essenziell, um Risiken für die eigene Organisation einschätzen

und ggf. frühzeitig Maßnahmen ergreifen zu können, da auf Schwachstellen oder Sicherheitsrisiken nur reagiert werden kann, wenn diese bekannt sind. Insgesamt sind somit zur Vermeidung von IT-Sicherheitsvorfällen für Betreiber kritischer Infrastrukturen nicht nur das Sicherheitsmanagement und entsprechende Sicherungsmaßnahmen vor Ort, sondern auch darüberhinausgehende organisatorische Maßnahmen relevant, die den gesamten Lebenszyklus von Hard- und Softwarekomponenten eingesetzter IT-Systeme einschließen und permanent aktualisiert und an neue Erkenntnisse angepasst werden müssen.

IT-Dienstleistern kommt im Zusammenhang mit Supply-Chain-Angriffen oftmals eine besondere Bedeutung zu. Dies ist im Wesentlichen darin begründet, dass IT-Angriffe auf derartige Unternehmen Angreifern potenziell eine Vielzahl möglicher Opfer bieten und somit die Auswirkungen eines einzelnen erfolgreichen Angriffs sich auf eine große Zahl mit dem IT-Dienstleister in Verbindung stehender Unternehmen erstrecken. Dabei sind bei derartigen IT-Angriffen auf IT-Dienstleister nicht nur deren direkte Kunden betroffen, sondern potenziell auch Unternehmen und Einrichtungen, die selbst keine Beziehung zum angegriffenen Dienstleister haben, deren Zulieferer und IT-Dienstleister jedoch eine entsprechende Verbindung zum Angriffsziel haben. Außerdem werden in der heutigen Zeit immer mehr Dienste und Dienstleistungen durch externe Unternehmen und Dienstleister bereitgestellt, wodurch sich die potenzielle Angriffsoberfläche fortwährend vergrößert. Oftmals dienen IT-Dienstleister Angreifern als Einfallstore für die eigentlich anvisierten Ziele, um sich Zugang zu den Netzwerken und Systemen zu verschaffen. Dabei nutzen Angreifer die enge Vernetzung und gegebenenfalls vorhandene Vertrauensverhältnisse zwischen IT-Dienstleistern und deren Kunden aus, um die Systeme zu infiltrieren, korrumpieren und beispielsweise Schadsoftware einzuschleusen, die weitere Angriffsschritte ermöglicht. Wenn Angreifer dabei für ihre Angriffe auf das eigentliche Ziel legitime Zugriffswege des IT-Dienstleisters nutzen, ist die Detektion der Angreiferhandlungen je nach Vorgehen der Angreifer nur schwer oder gegebenenfalls für das Opfer gar nicht möglich.

Grundsätzlich sind Systeme zur System- und Netzwerküberwachung ein essenzielles Werkzeug, um derartige IT-Angriffe zu erkennen. Diese werden dazu eingesetzt, den Netzwerkverkehr zu überwachen, ungewöhnliche oder verdächtige Aktivitäten zu erkennen und Alarmmeldungen zu generieren, wenn Angriffe erkannt werden. Umso kritischer können IT-Angriffe sein, wenn solche Systeme kompromittiert wurden und von Angreifern für ihre Zwecke eingesetzt werden. Eine erfolgreiche Kompromittierung ermöglicht

Angreifern dabei beispielsweise die unbemerkte Ausführung weiterer Angriffsschritte im Netzwerk, die Manipulation von Überwachungsmechanismen sowie weitreichende Zugriffsmöglichkeiten, da derartige Systeme typischerweise Zugriff auf viele bzw. alle Bereiche mit entsprechenden Zugriffsrechten besitzen. Die wesentlichen Gefahren von IT-Angriffen im Zusammenhang mit der Lieferkette, die Systeme zur Netzwerküberwachung betreffen, erwachsen somit einerseits aus der möglichen Verschleierung der Angriffe, indem Angreifer die Systeme, die zur Aufdeckung solcher Angriffe eingesetzt werden, kompromittieren, und andererseits aus weitreichenden Möglichkeiten zur Manipulation der Sicherheitsinfrastruktur durch die Angreifer, wenn sie Zugriff auf diese Systeme haben. Je nachdem, welche Systeme zur Netzwerküberwachung auf den Zielsystemen eingesetzt werden, ergeben sich dabei unterschiedliche Einflussmöglichkeiten für potenzielle Angreifer. Diese erstrecken sich bei einer potenziellen Kompromittierung von Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) Systemen oder anderen Monitoring Tools im Wesentlichen auf die Verschleierung von Angriffshandlungen oder ausbleibende bzw. falsche Interpretation von Angriffen. Bei Systemen mit aktiven Funktionen zur automatisierten Einleitung von Maßnahmen bei erkannten Angriffen, wie zum Beispiel Intrusion Prevention Systems (IPS), kann eine Kompromittierung zur Einleitung falscher Maßnahmen oder zum Ausbleiben entsprechender Funktionen führen. Insgesamt stellen IT-Angriffe im Zusammenhang mit der Lieferkette, die Netzwerküberwachungssysteme betreffen, eine ernstzunehmende Bedrohung dar, die im Rahmen der IT-Sicherheitskonzeption entsprechend berücksichtigt werden müssen.

Generell gab es in den vergangenen Jahren diverse IT-Angriffe auf sicherheitskritische Einrichtungen, die mit der Lieferkette von IT-Systemen zusammenhängen. In Anbetracht dessen ist die Gewährleistung der Cybersicherheit in der gesamten Lieferkette eine wesentliche und herausfordernde Aufgabe für kritische Infrastrukturen, insbesondere für Kernkraftwerke sowie sonstige kerntechnische Anlagen und Einrichtungen. Die Angreifer setzen dabei unter anderem explizit auf bekannte oder zum Angriffszeitpunkt unbekannte Schwachstellen in der Lieferkette von IT-Systemen, um ihre Ziele zu erreichen. Insbesondere kleinere oder mittelständische Hersteller oder IT-Dienstleister, die bezüglich IT-Sicherheitsmaßnahmen verglichen mit internationalen Großunternehmen lediglich eingeschränktere Möglichkeiten haben, stellen sich oftmals als schwächstes Glied in der Lieferkette heraus, das Angreifer gezielt auswählen, um darüber Zugriff auf andere Unternehmen, Organisationen oder Betreiber kritischer Infrastrukturen zu erhalten, die besser geschützt sind. Aber auch global agierende Unternehmen mit hohen

Sicherheitsstandards können Opfer von IT-Angriffen über die Lieferkette werden, wobei dies oft Folgen erheblichen Ausmaßes hat. Nachfolgend werden bedeutende IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette von IT-Systemen kurz exemplarisch beschrieben.

- Im Juli 2021 ereignete sich ein IT-Angriff auf Server verschiedener weltweit verbreiteter Unternehmen über die Software VSA des amerikanischen IT-Dienstleisters Kaseya /VAR21w01, HEI21w06, CIO21w01/. Die betroffene Software, ein Remote-Monitoring und -Management-Tool, mit dem Dienstleistungen wie beispielsweise Fernwartung o. Ä. durchgeführt werden können, wird von über 1.000 Firmen verwendet. Die Angreifer nutzten dabei mehrere Sicherheitslücken und Zero-Day-Exploits[4] aus, um die VSA-Server zu manipulieren und so ein vorher präpariertes, schadsoftwarebehaftetes Update zu platzieren, welches entsprechend durch die Server an die Clients weitergegeben wurde und zur Verschlüsselung der betroffenen Systeme führte. Neben den direkt betroffenen Unternehmen, die mit Kaseya in Verbindung standen, waren auch Firmen betroffen, die selbst keinen direkten Bezug zu Kaseya hatten, sondern lediglich deren IT-Dienstleister oder Zulieferer VSA nutzten.

- Einer der kritischsten und weitreichsten IT-Angriffe im Zusammenhang mit einem IT-Dienstleister bzw. einer Netzwerkmanagement-Software betraf die Software-Plattform SolarWinds Orion, die unter anderem Monitoring und Management von IT-Netzwerken, -Systemen und -Anwendungen ermöglicht und von 33.000 SolarWinds Kunden genutzt wird. Dabei wurde im Dezember 2020 eine entsprechende Angriffswelle von IT-Angriffen über die Lieferkette entdeckt /BUS20w01, FIR20r01, POL20w01, SEC21w01/. Bei diesem IT-Sicherheitsvorfall gelang es den Angreifern, unbemerkt eine Reihe von SolarWinds Orion Versionen mit einer Schadsoftwarekomponente zu infizieren, welche dann digital signiert und somit für Endkunden vom Hersteller zertifiziert ab März 2020 über den offiziellen Update-Server von SolarWinds verteilt wurden. Der IT-Angriff war insbesondere für die Endkunden sehr schwer detektierbar und blieb über ein halbes Jahr lang unbemerkt. Von den IT-Angriffen betroffen waren unter anderem eine Reihe von US-Ministerien und Behörden sowie große, private IT-Unternehmen wie Microsoft oder Cisco und auf Analysen von IT-Angriffen spezialisierte Firmen wie FireEye. Anfang 2024 wurden

[4] Ausnutzung einer Schwachstelle, die vor Beginn des Angriffs (day 0) nur dem Angreifer, d. h. zunächst weder der Öffentlichkeit noch der Hersteller des von der Schwachstelle betroffenen Produktes, bekannt ist. Diese erlangen erst mit Bekanntwerden von Angriffen unter Ausnutzung der Schwachstelle Kenntnis davon und können erst ab diesem Zeitpunkt (day 1) Maßnahmen zur Behebung ergreifen.

zudem Informationen über kritische Sicherheitslücken in der Netzwerkmanagement-Software Solarwinds Security Event Manager bekannt, die Angreifer unter anderem zur Ausführung von beliebigem Code nutzen können /SEC24w05/.

- Im Juli 2024 kam es global aufgrund eines fehlerhaften Softwareupdates der Falcon Sensor Software, die zur Bedrohungsanalyse und Auswertung von Echtzeit-Angriffsindikatoren eingesetzt wird, zu massiven Betriebsstörungen von Windows-Systemen, bei denen die entsprechende Software installiert war /CRO24w01/. Das fehlerhafte Update, das automatisiert an die betroffenen Systeme übertragen wurde, hatte Auswirkungen auf weltweit etwa 8,5 Millionen Windows-Systeme hauptsächlich im Unternehmensbereich und führte zu zahlreichen Ausfällen mit weitreichenden Auswirkungen beispielsweise im Flugverkehr und Telekommunikationsunternehmen /MIC24w01/. Obwohl es sich nicht um einen gezielten IT-Angriff, sondern ein vom Hersteller fehlerhaft ausgerolltes Update handelte, kam es infolgedessen zu Phishing[5]-Vorfällen und weiteren bösartigen Aktivitäten durch unterschiedliche Bedrohungsakteure, die den IT-Sicherheitsvorfall ausnutzten und für ihre Zwecke instrumentalisieren wollten. Zudem illustriert dieser Vorfall, welch massive Auswirkungen bereits durch ein ohne jegliche maliziöse Absicht fehlerhaftes Update hervorgerufen werden können.

- Neben IT-Sicherheitsvorfällen im Zusammenhang mit globalen Unternehmen, weitreichenden Auswirkungen und einer über die IT-Sicherheitsbranche hinausgehende Berichterstattung, gab es in den letzten Jahren wiederholt Cyberangriffe auf kleinere, mittelständische und lokal agierende Dienstleister, die verschiedene IT-Dienstleistungen für Unternehmen, Behörden und Institutionen anbieten. Die Auswirkungen dieser Supply-Chain-Angriffe betrafen neben den Dienstleistern selbst oftmals direkt deren Kunden und resultierten beispielsweise in Informationsdiebstahl oder dem Ausfall von Diensten und IT-Dienstleistungen. Neben internationalen Fällen, wie beispielsweise im Zusammenhang mit Cellcom in Israel /HEI22w08, MAL22w02/ oder Okta in den USA /OKT22w01, OKT22w02/, gab es in den letzten Jahren auch IT-Sicherheitsvorfälle im Zusammenhang mit IT-Dienstleistern in Deutschland. Zum Beispiel kam es 2023 zu einem von Fall

[5] 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/

Informationsdiebstahl im Zusammenhang mit einem IT-Dienstleister, als das Unternehmen Adesso, zu dessen Kundenkreis neben Behörden der Bundes-, Landes- und Kommunalverwaltung auch Betreiber kritischer Infrastrukturen gehören, Opfer eines Cyberangriffs wurde. Dabei verschafften sich die Angreifer, mutmaßlich über Monate hinweg, unbemerkt Informationen über Adesso und dessen Kunden /ADE23w01/. Der deutsche IT-Dienstleister Bitmarck, der mit diversen Krankenkassen in Deutschland zusammenarbeitet und beispielsweise Dienstleistungen im Zusammenhang mit der elektronischen Krankenkassenkarte und elektronischen Patientenakte anbietet, wurde im Jahr 2023 Opfer von Cyberangriffen. Neben dem Abfluss von Informationen kam es dabei temporär unter anderem zu technischen Störungen und Einschränkungen im Tagesgeschäft mehrerer gesetzlicher Krankenversicherungen in Deutschland /BTB23w01/. Weitere Cyberangriffe im Zusammenhang mit der Lieferkette erfolgten beispielsweise auf die Software- bzw. IT-Dienstleistungsunternehmen Centreon /ANS21r01/, CodeCov /HEI21w01/, und Ivanti /FOR20w02/.

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

2.2 Angreifbarkeit in der Softwareentwicklung

Die zunehmende Digitalisierung weltweit führt dazu, dass ein Großteil der heute eingesetzten industriellen Steuerungssysteme rechnerbasiert aufgebaut bzw. programmierbar ist, weswegen die Gewährleistung der Cybersicherheit von größter Bedeutung für solche Systeme ist. Hinsichtlich der Angriffsmöglichkeiten auf Softwareprodukte können in unterschiedlichen Phasen von deren Lebenszyklus verschiedene Angriffsmuster von Relevanz sein, wobei sich die verschiedenen Phasen des Lebenszyklus in die Bereiche Upstream, Midstream und Downstream unterteilten lassen. Gleiches gilt für Angriffe auf diese Phasen. Upstream-Angriffe betreffen die Phasen Design, Entwicklung und Produktion und somit den Softwareentwicklungsprozess bis hin zum fertigen, getesteten Produkt. Midstream-Angriffe betreffen die Phase der Distribution und beinhalten die Prozesse zur Verteilung, Auslieferung und Übertragung auf der Hersteller- bzw. Händlerseite. Downstream-Angriffe umfassen die Phasen Akquisition, Betrieb, Instandhaltung und Entsorgung und betreffen somit alle Prozesse zur Beschaffung auf Kundenseite, Integrations-, Installations- und Inbetriebnahme-Prozesse, Prozesse bei Betrieb und Wartung, Updates[6], Patches sowie Prozesse bezüglich Ausmusterung, Vernichtung und Wiederverwendung.

Insbesondere Angriffe in den frühen Phasen des Lebenszyklus, also Upstream-Angriffe, können eine enorme Gefahr darstellen. Das Vornehmen von Manipulationen bereits während der Softwareentwicklung führt dazu, dass diese später im weiteren Verlauf, insbesondere durch den Endanwender, nur schwer zu erkennen und zu entfernen sind. Vom Endanwender aus gesehen handelt es sich bei Angriffen auf den Softwareentwicklungsprozess um Angriffe auf die Lieferkette. Aus Sicht des Prozesses der Softwareentwicklung gibt es für die Einbringung von Manipulationen im Wesentlichen dieselben Angriffsmöglichkeiten, die sich an allen anderen Stellen der Lieferkette sowie beim Endanwender bieten. Dies können Cyberangriffe von außen, kombinierte Angriffe von außen, Angriffe über weitere Verzweigungen in der Lieferkette oder Angriffe von innen sein.

Die während des Softwareentwicklungsprozesses eingebrachte Manipulation kann von den Angreifern später beim Endanwender ausgenutzt werden. Insbesondere der Fall,

[6] Bei Downstream betrifft dies vor allem das Einspielen von Updates und Patches auf Kundenseite. Die Entwicklung, Programmierung und das Release des entsprechenden Updates oder Patches fällt unter Upstream, während dessen Distribution unter Midstream fällt.

dass die verdeckte Manipulation während der Softwareentwicklung unbemerkt vom Hersteller abläuft, führt dazu, dass der Hersteller die Software offiziell freigibt und zertifiziert und diese über die etablierten Prozesse beim Endanwender eingebracht wird. Dadurch werden viele Sicherungsmaßnahmen zur Detektion der Manipulationen umgangen. Bei einem solchen Vorgehen stehen für den Endanwender nur sehr eingeschränkte Detektionsmöglichkeiten hinsichtlich der Manipulation zur Verfügung, was eine Detektion der Manipulation entsprechend unwahrscheinlicher macht. Häufig sind diese Manipulationen nur indirekt detektierbar, z. B. erst dann, wenn die Schwachstellen tatsächlich ausgenutzt werden bzw. das Ausführen der Schadsoftware zu – beabsichtigten oder unbeabsichtigten – Auffälligkeiten führt.

Für Angreifer ist ein Angriff auf die Softwareentwicklung meist deutlich aufwändiger als ein Angriff auf die Prozesse zur Verteilung der bereits entwickelten Software. In der Regel setzen solche Angriffe ein langfristiges, persistentes und fachkundiges Vorgehen der Angreifer voraus. Dennoch bietet ein Angriff auf die Softwareentwicklung aus Sicht der Angreifer einige Vorteile. Manipulationen, die bereits bei der Softwareentwicklung eingebracht wurden, erreichen häufig eine sehr große Verteilung bei den Kunden dieser Software und damit eine große Menge möglicher Ziele für die Angreifer. Darüber hinaus ist eine Manipulation typischerweise umso schwerer zu erkennen, je früher im Softwareentwicklungsprozess diese vorgenommen wurde.

Auch zufällig im Rahmen der Softwareentwicklung eingebrachte Fehler können zu weitreichenden Auswirkungen führen. Obwohl es sich dabei nicht um gezielte Angriffe handelt, können zufällig eingebrachte Fehler zu erheblichen IT-Sicherheitsvorfällen führen. Generell ist davon auszugehen, dass die Auswirkungen bei absichtlichen Angriffen mindestens genauso schwerwiegend sein können, wie bei zufälligen Softwarefehlern. Daher sind auch zufällige Angriffe für die Einschätzung der Bedrohungslage relevant. Ein Beispiel für einen zufällig während der Softwareentwicklung eingebrachten Fehler ist das fehlerhafte Softwareupdate der Falcon Sensor Software des Unternehmens Crowdstrike aus dem Jahr 2024 /CRO24w01, MIC24w01/. Dieses ohne Nutzerinteraktion von der Software nachgeladene Update verursachte aufgrund eines Mismatches bei den übergebenen bzw. erwarteten Parametern weltweit massive Betriebsstörungen von Windows-Systemen, auf denen die entsprechende Software installiert war. Insgesamt waren von den Störungen etwa 8,5 Millionen Systeme betroffen, unter anderem bei Fluggesellschaften, Medien- und Telekommunikationsunternehmen sowie Krankenhäusern

und Handelsunternehmen. Auch Betreiber kritischer Infrastrukturen in Deutschland meldeten Ausfälle sowie Einschränkungen bei der Erbringung kritischer Dienstleistungen.

Dass Software während ihrer Entwicklung nicht nur für zufällige Fehler im Coding anfällig ist, sondern auch eine Vulnerabilität gegenüber absichtlichen Angriffen und Manipulationen aufweist, zeigt das Beispiel der Manipulation der Software-Plattform SolarWinds Orion im Jahr 2020 /FIR20r01, BUS 20w01, POL20w01/. Bei diesem IT-Sicherheitsvorfall gelang es den Angreifern, eine Reihe von SolarWinds Orion Versionen während des Softwareentwicklungsprozesses mit einer Schadsoftwarekomponente zu infizieren. Die manipulierte Software wurde dann digital signiert und somit für den Endanwender vom Hersteller zertifiziert über den offiziellen Update-Server verteilt. Die schadsoftwarebehafteten Updates wurden von ca. 18.000 Endanwendern heruntergeladen, bei mindestens 250 Endanwendern kam es zu individuellen, weiterführenden Angriffsschritten. Aufgrund dessen, dass der Angriff insbesondere für die Endanwender sehr schwer zu detektieren war, blieb dieser mindestens ein halbes Jahr lang unbemerkt. Von den Angriffen betroffen waren u. a. eine Reihe von Ministerien und Behörden in den USA sowie große private Unternehmen wie Microsoft oder Cisco.

Ein weiteres Beispiel für die Angreifbarkeit in der Softwareentwicklung ist das Einbringen einer Backdoor[7] in die Open-Source-Datenkompressionssoftware XZ Utils im Jahr 2024 /FRE24r01, KAS24t01, RSC24r01/. Das Ziel des Angriffs war das Einbringen einer Backdoor in SSH (Secure Shell), welche ausschließlich durch die Angreifer genutzt werden konnte. Diese ermöglichte es Angreifern, über eine manipulierte SSH-Authentifizierung Zugriff auf betroffene Linux-Systeme zu erhalten und unbefugten Code auf den betroffenen Systemen auszuführen. Der Angriff zeichnete sich nicht nur durch geschickt eingebrachten, komplexen Schadcode und langfristig angelegtes Social-Engineering aus, sondern auch durch ausgeklügelte Methoden zur Detektionsevasion. Dabei erfolgten Angriffe auf mehrere Phasen des Softwareentwicklungsprozesses unter Etablierung eines mit weitreichenden Rechten ausgestatteten Innentäters, der in den innersten Kreisen der Softwareentwicklung tätig war. Dieser vollführte eine systematische Unterwanderung des Softwareentwicklungsprozesses mit Hilfe von vier Scheinidentitäten. Zudem setzte der Innentäter alle am Projekt Mitarbeitenden sowie den Hauptentwickler über einen langen Zeitraum unter Druck. Die Platzierung der Angreifer-Identität als Innentäter

[7] Eine Backdoor ist ein Programm oder Code, der Dritten einen unbefugten und versteckten Zugang ("Hintertür") zum IT-System und somit etablierte Sicherungsmaßnahmen umgeht.

mit weitgehenden Rechten erfolgte schrittweise über mehrere Jahre hinweg, wobei zunächst über mehrere Jahre eine zuverlässig erscheinende Mitarbeit erfolgte. Insgesamt setzten die Angreifer Social-Engineering mehrschichtig, langfristig und in aller Öffentlichkeit ein, um in der Lieferkette eines wichtigen Softwarepaketes einen Innentäter zu etablieren, seine Rechte auszuweiten und ihn an einer für den Angriff strategisch günstigen Stelle zu platzieren. Nur eine sehr zeitnahe Erkennung der Manipulation in Verbindung mit einer umgehenden Reaktion auf Entwicklungs- und Distributionsseite verhinderte die potenziell enorme Verbreitung der Malware[8].

Auch nicht-sicherheitsgerichtete menschliche Entscheidungen im Verlauf des Softwareentwicklungsprozesses haben einen deutlichen Einfluss auf die Angreifbarkeit von Softwareprodukten. Hierzu zählen insbesondere Entscheidungen zum Umgang mit bislang nicht öffentlich bekannten Schwachstellen, zur Vergabe von Zugriffsrechten oder zum Outsourcing von Teilen der Softwareentwicklung. Ein Beispiel hierfür ist ein Upgrade des Intranets von Rolls-Royce Submarines, welches ab dem Jahr 2020 vorgesehen war und durch einen Unterauftragnehmer, den Dienstleister WM Reply, durchgeführt werden sollte. Entsprechend der Vorgaben des Verteidigungsministeriums sah Rolls-Royce-Submarines vor, dass die Aufgaben nur von Personen durchgeführt werden durften, die im Vereinigten Königreich ansässig sind und eine gültige Sicherheitsprüfung haben. Der Dienstleister WM Reply setze allerdings neben sicherheitsüberprüften Mitarbeitern in Großbritannien auch Entwickler aus Belarus und Russland ohne entsprechende Freigaben ein. Dies erfolgte vermutlich aus Kostengründen und ohne Absprache mit Rolls-Royce Submarines. Auch nachdem Mitarbeiter von WM Reply Bedenken äußerten und vorschlugen, Rolls-Royce Submarines zu informieren, versuchte WM Reply diesen Vorgang geheim zu halten. Vorgesetzte bestanden darauf, Rolly-Royce Submarines nicht zu informieren und diskutieren stattdessen Alternativen zur Verschleierung des Vorgangs, wie beispielsweise die Verwendung von Namen verstorbener britischer Staatsbürger anstelle der tatsächlichen belarussischen/russischen Namen, die Mitteilung der Zugangsdaten der in Großbritannien am Projekt mitarbeiten, sicherheitsüberprüften Entwickler an die Entwickler in Belarus und Russland oder die Durchführung der Kompilierung der in Belarus erstellten Software durch einen britischen Entwickler. Es ist nicht öffentlich bekannt, ob und welche dieser Maßnahmen letztendlich eingesetzt wurden.

[8] Malware ist ein Kunstwort, abgeleitet aus "Malicious software" und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. /BSI20w01/

Hinsichtlich der Angreifbarkeit in der Softwareentwicklung zeigt sich, dass eine Berücksichtigung solcher Angriffsmöglichkeiten von hoher Bedeutung für die Cybersicherheit von Softwareprodukten ist und zunehmend an Bedeutung gewinnt. Aufgrund der zunehmenden Komplexität der Produkte und ihrer Abhängigkeiten sowie der häufig verteilten Arbeitsweise und der zunehmenden Verlagerung des Entwicklungsprozesses in die Cloud wächst die Angriffsoberfläche bei der Softwareentwicklung an. Ein weiterer Punkt für die wachsende Angriffsoberfläche bei der Softwareentwicklung ist die Beteiligung zahlreicher Personen, Prozesse und Stakeholder am Softwareentwicklungsprozess.

2.3 KI-gestützte und KI-gesteuerte Cyberangriffe

In den letzten zwei Jahren haben Anwendungen künstlicher Intelligenz (KI) einen deutlichen Fortschritt sowohl in Bezug auf ihre Fähigkeiten als auch in Bezug auf ihre Anwendungsmöglichkeiten und Verbreitung erlebt. Dieser Trend setzte sich im Jahr 2024 fort mit der Veröffentlichung neuerer und leistungsfähigerer KI-Modelle und wird sich aller Voraussicht auch in den kommenden Jahren weiter verstärken.

KI wird hierbei als Überbegriff für eine Reihe von Techniken und Systemen verwendet, bei welchen typischerweise menschliche kognitive Fähigkeiten Softwareprogrammen zugeschrieben werden. Hierbei können sowohl vorprogrammierte Abläufe als auch maschinelles Lernen genutzt werden. Die Fortschritte der letzten Jahre, bei denen KI-Modelle mit immer stärkeren Rechenleistungen und einer größeren Basis an Trainingsdaten genutzt werden, basieren überwiegend auf maschinellem Lernen. Bei diesem werden Algorithmen entwickelt, welche auf Basis von Trainingsdaten und definierten Zielen durch Wiederholung erlernen, die Ziele zu erfüllen, wobei kein direkter Lösungsweg vorgegeben wird. Durch Erhöhung der Rechenleistung und der Erhöhung der Datenmengen für das Training werden größere und leistungsfähigere KI-Modelle geschaffen.

Wird aktuell über KI gesprochen, sind zumeist drei unterschiedliche Modelle gemeint:

- **Large Language Modelle (LLM)** – Diese Modelle dienen dazu, Wahrscheinlichkeiten für Wort-, Satz- und Zeichenfolgen zu errechnen und hieraus einen sprachlich nutzbaren Output zu generieren. Die Modelle erhalten teilweise mehrere Milliarden individueller Trainingsdaten und nutzen eine hohe Rechenleistung, um auf bestimmte textliche Eingaben wie Fragestellungen eine Antwort zu generieren, die von Nutzern als sinnvoll bzw. nutzbar angesehen wird. Bekannte Modelle sind z. B. neuere Versionen von ChatGPT, Google Gemini oder Meta LLaMA.

- **Visuelle Intelligenz** – Hierbei werden KI-Algorithmen entwickelt, die auf Basis von Trainingsdaten erlernen, Muster zu erkennen, wobei hierbei typischerweise optische Muster gemeint sind. Diese können z. B. zur Gesichtserkennung, zur Auswertung bildgebender medizinischer Verfahren, zur Zielerfassung oder zur Handschrifterkennung genutzt werden. Weiter können diese Verfahren jedoch auch zur Spracherkennung genutzt werden. Muster gesprochener Sprache ermöglichen es, dass mittels Sprachsynthese die Sprache des eingesprochenen Sprechers repliziert werden kann.
- **Generative Adversariale Netzwerke (GAN)** – Diese Modelle basieren auf zwei Netzwerken, welche als Gegenspieler fungieren. Das eine Netzwerk erhält Trainingsdaten, um aus diesen abgeleitete Werke wie Bilder oder Videos zu erzeugen. Das zweite Netzwerk wird trainiert, Unterschiede zwischen echten und erzeugten Werken zu erkennen. Schlussendliches Ziel ist, dass von der Realität bzw. realen Werken kaum oder nicht mehr unterscheidbare Werke erzeugt werden.

Mit stetig wachsenden Funktionen und Fähigkeiten von KI-Modellen wachsen auch die Möglichkeiten der Nutzung von KI in Cyberangriffen. Die britische Regierung geht in /NCS24r01/ davon aus, dass sowohl APT-Gruppierungen als auch unabhängige und finanziell oder anderweitig motivierte Gruppierungen ihre Fähigkeiten in vielen Bereichen der Cyberkriminalität mit KI-Funktionen ausbauen werden. Der aktuell bekannteste und auch bereits im Jahr 2024 ausgenutzte Bereich betrifft hierbei Social Engineering. Auf LLM basierende KI ermöglicht z. B. die Generierung von spezifischen, an Informationen der Opfer angepassten Texten, welche massenhaft erstellt werden können, dennoch aber die Glaubhaftigkeit von hochspezifizierten Social Engineering Angriffen erreichen können. Generative KI kann z. B. täuschend echt wirkende Dokumente erzeugen, welche kaum mehr von legitimen Originalen zu unterscheiden sind. Visuelle Intelligenz kann dazu genutzt werden, dass aus einzelnen Stimmproben, z. B. aus einem Werbevideo des Geschäftsführers, eine täuschend echte synthetische Stimme erzeugt wird, welche für Social Engineering auf Mitarbeiter dieses Geschäftsführers verwendet werden kann. Mittels erster Live-Techniken können Sprache und Videos basierend auf kurzen Sprachproben und eines einzelnen Fotos erzeugt werden, die täuschend echte Teilnehmer an Videotelefonaten erzeugen.

Bei Cyberangriffen auf datentechnische Systeme können KI-Modelle oder auf KI basierende Schadsoftwarefunktionen eingesetzt werden. So sind KI-Modelle in der Lage, große Datenmengen in kurzer Zeit nach spezifischen Informationen zu durchsuchen,

wodurch bei Cyberangriffen die Ermittlung und Exfiltration von Daten stark beschleunigt werden kann.

KI kann auch direkt für die Entwicklung von Schadsoftware eingesetzt werden. LLM-Modelle sind bereits jetzt in der Lage, Code mit begrenztem Funktionsumfang in einer Form zu erzeugen, die anschließend von Fachpersonen angepasst und genutzt werden kann. KI-Modelle können z. B. auch genutzt werden, um effizienter nach Schwachstellen zu suchen oder Exploits für diese Schwachstellen zu entwickeln.

Aktuell werden umfassende Ressourcen in die Entwicklung von KI-Modellen unterschiedlicher Art investiert, wodurch es zu einem bedeutsamen Fortschritt der KI-Modelle gekommen ist. So erhöhte sich die Leistungsfähigkeit des Modells GPT 4 gegenüber seinem Vorgänger GPT 3 um ungefähr das 10-fache innerhalb von 3 Jahren. Open Source Modelle wie das Modell LLaMA von Meta, mittlerweile in der Version 3.2 verfügbar, werden darüber hinaus nicht nur als Produkte an Anwender und Geschäftskunden vermarktet, sondern grundsätzlich als Open Source Produkt frei verfügbar bereitgestellt.

Unter diesen Voraussetzungen ist anzunehmen, dass die Möglichkeiten, die sich durch KI-Modelle ergeben, sowohl für äußerst fähige staatsnahe Akteure (z. B. APT-Gruppierungen) als auch für allgemeine und mit weniger Ressourcen ausgestatte und weniger fähige Gruppen verfügbar sein werden. Es ist weiterhin anzunehmen, dass z. B. durch generative KI und LLM auch Gruppen mit geringen Ressourcen z. B. komplexe Spear-Phishing-Angriffe[9] oder Pig-Butchering-Angriffe[10] durchführen können. Auch die Entwicklung, Anpassung und Optimierung von Schadsoftware wird sich voraussichtlich mittels KI für solche Gruppen erheblich erleichtern und damit mehr potenziellen Angreifern zugänglich werden. Die bereits mit erheblichen Ressourcen ausgestatten Gruppen werden dagegen ihre tatsächlichen Fähigkeiten vielfach nicht direkt ausweiten, jedoch insbesondere verfeinern und optimieren können. Schon lange sind Cyberangriffe bekannt, bei denen vermutlich APT-Gruppierungen durch Social Engineering zu umfassendem Erfolg kamen. Auch besitzen APT-Gruppierungen bereits umfassende Kenntnisse im Bereich der Programmierung und Entwicklung von Schadsoftware und der Ermittlung

[9] Bei Spear-Phishing-Angriffen wird im Unterschied zu allgemeinen Phishing-Angriffen nicht breitflächig, sondern nur ein kleiner, ausgewählter Empfängerkreis attackiert, wobei der Angriff meist personalisiert und in einen für das Opfer spezifischen und glaubwürdigen Kontext eingebettet wird.

[10] Bei Pig-Butchering-Angriffen handelt es sich durch lang angelegten Investmentbetrug unter Einsatz von Social Engineering Techniken, zumeist unter Verwendung von Scheinidentitäten kombiniert.

von Schwachstellen. Die Nutzung von KI wird für diese Gruppierungen die Prozesse voraussichtlich effizienter machen und damit eine breitere Aufstellung und weitere Angriffsmuster ermöglichen.

2.4 Cyberangriffe auf kryptografische Verfahren

Kryptografische Verfahren sind essenzielle Techniken in der Informationssicherheit, die darauf abzielen, Daten vor unbefugtem Zugriff und Manipulation zu schützen. Durch die Anwendung mathematischer Algorithmen werden Informationen in eine unlesbare Form umgewandelt, die im Idealfall nur von autorisierten Parteien wieder entschlüsselt werden kann. Diese Verfahren spielen eine zentrale Rolle in vielen Bereichen, wie z. B. bei der sicheren Kommunikation im Internet, dem Schutz von Finanztransaktionen und der Wahrung der Privatsphäre in digitalen Netzwerken. Von klassischen Methoden wie der symmetrischen Verschlüsselung bis hin zu fortschrittlichen Techniken wie der Quantenkryptografie, entwickeln sich kryptografische Verfahren ständig weiter, um den wachsenden Herausforderungen der Cybersicherheit gerecht zu werden.

Weil mit kryptografischen Verfahren insbesondere sensible Informationen geschützt werden, sind diese im Blick von Cyberangreifern. Typischerweise basieren Verschlüsselungsalgorithmen auf komplexen mathematischen Problemstellungen wie der Primfaktorzerlegung oder der Lösung diskreter Logarithmen. Die Sicherheit der Verschlüsselungsverfahren entsteht hierbei durch die Komplexität der Lösungsverfahren, sodass Dritte ohne die zur Entschlüsselung vorgesehenen Schlüssel auch mit leistungsstarker Hardware mehrere Jahre bis Jahrmillionen zur Entschlüsselung benötigen würden. Solche Brute Force[11] Methoden haben daher zumeist nur bei veralteten Verschlüsselungsmethoden mit geringer Komplexität Erfolg, weshalb insbesondere Schwachstellen in der Programmierung und Etablierung von Verschlüsselungen durch Angreifer und Cybersicherheitsforscher im Fokus sind. Ebenso werden die Schlüssel selbst zu Angriffszielen, da eine Aneignung eines Schlüssels Angreifer ebenfalls zur Entschlüsselung befähigt.

Dabei basieren Schwachstellen zum einen auf Schwachstellen der Erzeugung und Verbreitung von Schlüsseln zur Verschlüsselung, zum anderen auf Schwachstellen in der Programmierung der Verschlüsselungsprogramme und der dahinterstehenden

[11] Knacken eines Passworts durch systematisches und meist automatisiertes Ausprobieren der verschiedenen Passwortmöglichkeiten.

Bibliotheken. Typische Angriffe auf die Schlüsselgenerierung basieren insbesondere auf der Vorhersehbarkeit der erzeugten Schlüssel bzw. bei Public-Private-Schlüsselsystemen des Schlüsselpaares. Dies basiert zumeist darauf, dass der Erzeugungsalgorithmus des Schlüssels bzw. der Schlüsselpaare keine ausreichende Zufälligkeit erreicht und damit vorhersehbar ist. Dies ist z. B. der Fall, wenn große Primzahlen für die Verschlüsselung genutzt werden, die Erzeugung dieser großen Primzahlen jedoch nur auf einzelnen Variablen basiert, um die Geschwindigkeit des Prozesses zu erhöhen, wie bei der ROCA-Schwachstelle aus dem Jahr 2017. Andere Schwachstellen betreffen direkt die Programme zur Ver- bzw. Entschlüsselung und ermöglichen z. B. Angreifern, trotz Verschlüsselung Daten und Informationen unverschlüsselt auszulesen. Außerdem wurde mehrfach die Entwendung von Schlüsseln bekannt gegeben. In den letzten Jahren sind dabei z. B. folgende Schwachstellen bzw. Schlüsselentwendungen bekannt geworden:

- Heartblead 2014 /NIS14n01/: Ein Fehler in OpenSSL, der ermöglichte, dass verschlüsselte TLS-Verbindungen von Dritten ausgelesen wurden. TLS wird als Standardverschlüsselung in der IP-basierten Kommunikation eingesetzt, wodurch Heartblead massenhaft Geräte und Personen betraf. Die Schwachstelle basierte darauf, dass im Rahmen der Kommunikation von OpenSSL unterstützenden Systemen die Kommunikationspartner wiederkehrende kleine Nachrichten austauschten, um zu erkennen, ob weiterhin eine Verbindung besteht. Jedoch wurde die Größe dieser Nachrichten vom Programm nicht überprüft (Stack Overflow), sodass Angreifer mit speziellen Nachrichten Informationen aus dem Arbeitsspeicher der betroffenen Systeme auslesen konnten, wozu auch private Schlüssel, Passwörter und andere kritische Informationen gehörten.

- ROCA 2017 /NIS17n02/: Eine Schwachstelle in der Schlüsselerzeugung der Bibliothek RSALib ermöglichte es Angreifern, bei Millionen von Systemen mit Trusted Plattform Modulen die privaten und öffentlichen Schlüssel auszulesen. Bei der Schlüsselgenerierung wurde ein optimiertes Verfahren zur schnellen Generierung der Schlüssel angewendet, welches jedoch keine ausreichende Zufälligkeit erreichte. In der Konsequenz konnten Angreifer die Schlüssel ermitteln.

- Spectre und Meltdown 2018 /KOC18r01, LIP18r01/: Moderne Prozessoren führen mittels der Out-of-Order-Execution solche Prozesse aus, welche von Nutzer bzw. dem System nicht angefordert wurden, jedoch spekulativ als baldig auszuführen erwartet werden. Nach der Ausführung werden diese verworfen, wenn sie nicht benötigt wurden. Angriffe auf diese Funktion ermöglichen es, dass trotz Verwerfung

Systemänderungen ausgeführt werden, die es den Angreifern ermöglichen, bestimmte Informationen aus dem Adressraum von Prozessen oder anderweitig auszulesen. In der Konsequenz können Angreifer insbesondere auf Speicherorte zugreifen, die eigentlich geschützt werden sollen, wie die Speicherung privater Schlüssel oder Passwörter.

- OAuth 2023 /CLO18r01/: OpenAuthentification (OAuth) ist ein Protokoll zur einfachen und sicheren Teilung von Anmeldedaten von Nutzern. Eine Schwachstelle in der Umsetzung von OAuth durch Google ermöglichte es Angreifern, Anmeldecookies für Services von Google für fremde Personen zu erzeugen, wenn die Angreifer Zugriff auf die Systeme dieser hatten.

- Microsoft Signing Key 2023 /MIC23r02/: Angreifer gelangten an einen inaktiven Microsoft Security Authentificator Signing Key, also einen Schlüssel zur Signierung von legitimen, authentifizierten Nutzern. Dies ermöglichte den Angreifern die Signierung von Anmeldungen und damit Zugriff auf Programme wie Outlook oder die Azure Cloud.

- Apple Airdrop 2024 /CNN24w01, TUD21r01/: Apple Airdrop ist eine Funktion zur Nahfeldteilung von Informationen und Daten über Geräte des Unternehmens Apple. Sie nutzt die TLS-Verschlüsselung und sendet und empfängt Signale über die Wi-Fi-Funktionen der Geräte, wobei gebildete Hashwerte[12] aus E-Mail-Adressen und Telefonnummern dazu dienen, dass Geräte anonymisiert sind. Da die Eingabewerte der Hashwertbildung auf bekannten wiederkehrenden Formaten basieren, lassen sich diese Hashwerte zumeist deanonymisieren.

- CRYSTAL-Kyber 2024 /TEC24r01/: Der quantensichere Verschlüsselungsalgorithmus CRYSTAL-Kyber wird seit dem Jahr 2023 als Standardalgorithmus für eine quantensichere Verschlüsselung vom amerikanischen National Institute of Standards and Technology vorgesehen. Im Januar 2024 wurden die Schwachstellen KyberSlash 1 und Kyberslash 2 bekannt, bei welchen sich aus der Bearbeitungszeit spezifischer falscher Schlüssel Rückschlüsse auf die tatsächlichen Schlüssel ergeben. Mittels handelsüblicher Rechenleistung können somit teilweise in Minuten Entschlüsselungen ohne Kenntnisse der Schlüssel erreicht werden.

---

[12] Ein Hashwert ist eine mathematische Prüfsumme, die durch Anwendung einer Hashfunktion (kryptographischer Algorithmus, bei dem Nachrichten beliebiger Länge auf einen Hashwert fester Länge abgebildet werden) 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. /BSI20w01/

Der letzte dargestellte Fall stellt hierbei eine Besonderheit dar. Es wird angenommen, dass herkömmliche Verschlüsselungen basierend auf Primfaktorzerlegungen mit dem Aufkommen von leistungsfähigen Quantencomputern innerhalb kurzer Zeit durch Brute-Force-Angriffe entschlüsselt werden können. Um vorab Verschlüsselungen sicherer zu machen, werden daher neue Verschlüsselungsalgorithmen entwickelt, die z. B. auf Kristallstrukturen oder anderen komplexen Berechnungen basieren, bei welchen Quantencomputer ebenso wie reguläre Computer mit aktueller Leistungsfähigkeit Jahrzehnte oder länger zur Entschlüsselung benötigen.

Grundsätzlich ist die Entschlüsselung von verschlüsselten Daten für Cyberangreifer aufgrund der geschützten Daten hochinteressant. Gleichzeitig sind die meisten Verschlüsselungsalgorithmen wie TLS oder RSALib enorm weit verbreitet, sodass eine einzelne Schwachstelle sofort die Entschlüsselung oder das Auslesen von Daten auf einer hohen Anzahl an Geräten ermöglicht. Bei bekanntgewordenen Schwachstellen werden zwar zumeist sehr schnell Updates veröffentlicht, diese können jedoch nur für erneut verschlüsselte Daten und nur für neu erstellte Schlüssel Relevanz entfalten, sodass zumeist trotz bereitgestelltem Update eine große Menge Daten angreifbar bleibt. Daher sind Schwachstellen in Verschlüsselungsalgorithmen und Software von erheblichem Interesse für Angreifer und führen zu spürbaren Auswirkungen für die Anwender von Verschlüsselungen.

2.5 Cyberangriffe auf Fahrzeuge

In modernen Fahrzeugen werden zunehmend IT-Systeme eingesetzt, um den Fahrkomfort und die Fahrsicherheit zu erhöhen. Gemäß einer EU-Verordnung wurden in den Jahren 2022 und 2024 zahlreiche Fahrzeugsicherheitssysteme in Neuwagen verpflichtend, um die Sicherheit der Fahrzeuginsassen und anderer Verkehrsteilnehmer zu erhöhen. Beispiele für gesetzlich vorgeschriebene Fahrzeugsicherheitssysteme sind Notbremsassistenzsystem, Notfall-Spurhalteassistent, intelligenter Geschwindigkeitsassistent, Warnsystem bei Müdigkeit, Abbiegeassistenzsystem oder Kollisionswarnsystem. Ab dem Jahr 2026 werden weitere Systeme in Neuwagen rechtsverbindlich /BMD24r01/. Neben diesen Systemen bieten die Fahrzeughersteller auch immer umfangreichere Systeme für den Fahrkomfort wie beispielsweise Online-Navigationssysteme, Einparkhilfe, umfangreiche Multimediafunktionen oder WLAN-Hotspot.

Viele dieser Systeme für die Fahrzeugsicherheit und den Fahrkomfort nutzen Sensoren, wie Ultraschall, Kamera, Radar, Lidar etc. und sind untereinander vernetzt. Aufgrund der Vielzahl der vernetzten Steuergeräte erfolgt die Kommunikation der Systeme nicht durch Kabelbäume, sondern mit sogenannten Bussystemen. Im Kraftfahrzeug hat sich der CAN-Bus (Controller Area Network) als Standard-Bus-System zur Datenübertragung zwischen den verschiedenen Komponenten durchgesetzt. Dabei besteht der CAN-Bus aus zwei miteinander verdrillten Drähten CAN-low (CAN-L) und CAN-high (CAN-H). Die einzelnen Steuergeräte (CAN-Stationen) sind an der Hauptleitung mit Stichleitungen verbunden, hören den Bus kontinuierlich ab und erkennen, welche Daten für sie relevant sind. In einem Fahrzeug sind mehrere CAN-Busse miteinander verbunden, entweder direkt mit Steckverbindungen oder digital über einen Gateway-Computer. Der Einsatz dieser zahlreichen IT-Systeme bietet eine Vielzahl potenzieller Ziele für Cyberangriffe. Dabei wird ein Zugriff auf den CAN-Bus als besonders schwerwiegend angesehen, da dadurch auf das interne Netzwerk des Fahrzeugs zugegriffen wird und eine Manipulation aller wichtigen Komponenten wie Motor, Getriebe, Sensoren und fast aller elektronisch kontrollierten Teile ermöglicht wird.

Cyberangriffe aus der Ferne, mit dem Ziel einer physischen Kontrolle des Fahrzeugs, erfordern in der Regel drei Schritte. Zuerst verschafft sich der Angreifer einen Remote Access zu einem internen Fahrzeug-Netzwerk, beispielsweise über das Multimediasystem. Nach dem Erstzugriff kann der Angreifer Nachrichten in das Fahrzeug-Netzwerk einspeisen und ein ausgewähltes elektronisches Steuergerät (ECU, Electronic Control Unit) direkt oder indirekt steuern. In den meisten Fahrzeug-Designs ist ein aus der Ferne kompromittiertes Steuergerät jedoch nicht in der Lage, direkt Nachrichten an ein sicherheitskritisches Steuergerät zu senden, d. h. das Auto kann nicht physisch manipuliert werden. Bei manchen Fahrzeugen kann das kompromittierte Steuergerät jedoch Signale empfangen und verarbeiten. Dann muss der Angreifer im zweiten Schritt einen Weg finden, diese Kommunikationslücke vom Netzwerk des kompromittierten Steuergerätes zum anvisierten Netzwerk des sicherheitskritischen Steuergerätes zu überbrücken. Wie dieser Schritt gelingen kann, ist stark abhängig von der Architektur, die der Hersteller in seinem Fahrzeug verwendet. Wenn es dem Angreifer gelingt, Nachrichten an das gewünschte Steuergerät zu senden, ist eine Kommunikation mit dem sicherheitskritischen Steuergerät möglich. Der dritte und letzte Schritt besteht dann darin, das anvisierte Steuergerät so zu manipulieren, dass die Fahrzeugsicherheit kompromittiert wird. Dazu bedarf es Reverse Engineering der Nachrichten im Netzwerk, um das genaue Datenformat für die Durchführung einer physischen Aktion herauszufinden.

Der Prozess des Reverse Engineering ist sehr aufwendig, da jeder Hersteller und evtl. jedes Model unterschiedliche Daten in den Nachrichten des Busses verwendet /CHA15r01/.

Ein weiteres elektronisches System, das für eine Manipulation durch Angreifer anfällig ist, ist das sogenannte Keyless-System, ein Komfort-Schließsystem für Fahrzeuge. Es ermöglicht die Türen bzw. das Lenkradschloss ohne aktive Nutzung eines Autoschlüssels zu ent- bzw. verriegeln, sobald sich der Fahrer dem Fahrzeug nähert bzw. es verlässt. Das Keyless-System arbeitet passiv, d. h. der Fahrer muss keine Taste mehr drücken, um das Fahrzeug zu ent- bzw. verriegeln. Sobald sich der Funkschlüssel in der Nähe befindet, wird das Fahrzeug automatisch entriegelt, wenn der Fahrer die Türgriffe berührt. Das Fahrzeug lässt sich dann durch Betätigen des Startknopfes oder durch einen Tritt auf die Bremse (bei Elektroautos) starten. Beim Verlassen erfolgt dann eine automatische Verriegelung. Die Keyless-Technologie ent- bzw. verriegelt das Fahrzeug dabei über Funksignale eines Transponders, den der Fahrzeughalter mit sich führt. Den Befehl zum Entsperren gibt ein Empfänger im Auto. Diese Technologie ist über das Mithören des Codes angreifbar.. Eine Schwachstelle ist die permanente Messung der Signalstärke, da sichergestellt werden soll, dass die Türen öffnen, wenn der Schlüssel nah genug am Auto ist. Daher sendet der Fahrzeugschlüssel permanent Funksignale. Angreifer können diese Schwachstelle des Keyless-Systems ausnutzen und durch einen sogenannten Relay-Angriff (relay attack) Autos stehlen. Ein Relay-Angriff (auch als two-thief attack, d. h. Zwei-Diebe-Angriff bezeichnet) funktioniert ähnlich wie ein Man-in-The-Middle-Angriff[13]. Während bei einem Man-in-The-Middle-Angriff ein einzelner Angreifer die Kommunikation zwischen zwei Parteien abfängt und manipuliert, wird bei einem Relay-Angriff die Kommunikation mit beiden Parteien von zwei Angreifern abgefangen. Die Nachrichten zwischen den beiden Parteien werden dann weitergeleitet, ohne sie zu manipulieren oder gar zu lesen. Für den Fahrzeugdiebstahl verwenden die Angreifer sogenannte Relay-Stationen, die Funksignale im Frequenzbereich des Keyless-Systems empfangen und aufzeichnen können. Die Relay-Stationen agieren dabei als „Mittelsmänner“, indem sie die Signale, die zwischen dem Fahrzeugschlüssel (Transponder) und dem Auto ausgetauscht werden aufzeichnen und weiterleiten. Der erste Täter empfängt mit einer Relay-Station das Signal des Fahrzeugschlüssels in einiger Entfernung

[13] 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. /BSI20w01/

vom Schlüssel (beispielsweise vor einem Haus). Dieses Signal wird dann an einen zweiten Mittäter mit einer Relay-Station weitergeleitet, der sich in der Nähe des Zielautos befindet, so dass dem Auto ein in der Nähe befindlicher Schlüssel vorgetäuscht wird und es entriegelt wird. Um die Reichweite des Funksignals zur Übertragung zu erhöhen, setzen die Angreifer spezielle Verstärker ein. Je nach verwendeter Verstärkertechnologie können sie auch erfolgreiche Relay-Angriffe durchführen, wenn sich der Fahrzeugschlüssel in beträchtlicher Entfernung vom Auto, beispielsweise im Haus des Besitzers, befindet.

Cyberangriffe auf Fahrzeuge werden als hochgradig problematisch angesehen, da sie den Straßenverkehr gefährden und potenziell lebensgefährlich für die Fahrzeuginsassen und andere Verkehrsteilnehmer sein können. Zudem liegt die Cybersicherheit von Autos auch im besonderen Interesse der Hersteller, da Fahrzeug-Hacks zu technischen Nachbesserungen, Softwareupdates und damit verbundenen Rückrufaktionen führen. Daraus können finanzielle Verluste und Rufschädigung resultieren, die die Hersteller vermeiden möchten. Seit Sommer 2024 gilt für die Hersteller von Neufahrzeugen in der EU die Vorschrift UNECE R155[14]. Darin werden die Hersteller dazu verpflichtet ein Cybersecurity Management System (CSMC) zur Risikoerkennung und Risikominimierung aufzubauen. Dazu gehören auch Bedrohungsanalysen und regelmäßige Risikobewertungen (Threat Analysis and Risk Assessment, TARA), sowie ein Monitoring von neuen Schwachstellen und bekannten Angriffen, um darauf mit Updates reagieren zu können. Die Cybersicherheit in der Automobilindustrie wird seit dem Jahr 2010 auch verstärkt in der Forschung untersucht. Dabei nutzen Sicherheitsforscher Schwachstellen in der Software, die vom Hersteller nicht erkannt wurden, um sicherheitstechnische Einschränkungen zu umgehen. Diese Schwachstellen sind besonders kritisch, wenn sie einen Fernzugriff auf das Fahrzeug ermöglichen, ohne das ein physischer Zugang notwendig ist. Angreifer können sich dann unbemerkt lateral im Netzwerk des Autos bewegen und Systeme manipulieren. Selbst wenn dabei keine sicherheitskritischen Systeme betroffen sind, kann ein solcher Cyberangriff fatale Auswirkungen auf die Fahrtauglichkeit eines Fahrers haben, wenn dieser beispielsweise durch unerwartete Aktionen erschrickt. Erstmals gelang es im Jahr 2010 Sicherheitsforschern aus den USA, mit dem CAN-Bus eines Autos zu kommunizieren und so eine physische Manipulation am Auto vorzunehmen, u. a. durch die Steuerung der Tachometeranzeige, das Abschalten des Motors und die Beeinflussung

[14] UN Regulation No. 155 - Cyber security and cyber security management system

der Bremsen. Sie benötigten dazu allerdings physischen Zugang zum Fahrzeug /KOS10j01/. Im Jahr 2011 gelang diesen Forschern auch ein solcher Zugriff auch über einen Remote Access /CHE11j01/.

Zusammenfassend lässt sich sagen, dass aufgrund der Vielzahl von IT-Systemen die Netzwerkarchitekturen der Fahrzeuge deutlich komplexer geworden sind. Zudem gibt es viel Technik für die drahtlose Kommunikation, wie beispielsweise Keyless-Systeme, Bluetooth, WLAN, AM/FM/XM-Radio etc., wodurch auch die Angriffsoberfläche für Angriffe aus der Ferne erhöht wird. Und es gibt eine Vielzahl von cyber-physischen Systemen, bei denen Elektronik, Software und Netzwerkkommunikation dazu benutzt werden, einen physikalisch-technischen Prozess zu steuern, wie beispielsweise adaptive Geschwindigkeitsregelung, Einparkhilfe oder Spurhaltassistent. Eine Manipulation dieser Systeme ist als besonders kritisch zu erachten.

Nachfolgend werden einige ausgewählte Cyberangriffe auf Fahrzeuge beschrieben:

- Im Jahr 2015 gelang es Sicherheitsforschern, einen Jeep Cherokee über einen Remote Access zu hacken /CHA15r01/. Der Erstzugriff erfolgte über einen WLAN-Hotspot des Multimedia-Systems, den Fahrzeughalter abonnieren können. Aufgrund einer Schwachstelle bei der Generierung des automatisch erstellten WLAN-Passworts, konnte dieses gehackt werden. Durch eine weitere Schwachstelle gelang es, das Multimedia-System zu manipulieren und Zugriff auf den Musikplayer, das Radio, die Heizung und die Klimaanlage zu erlangen. Zudem entdeckten die Forscher, dass es möglich ist, die GPS-Koordinaten des Jeeps abzufragen und abzurufen und das Auto über sein GPS-Navigationssystem zu verfolgen. Da nicht alle Fahrzeuginhaber einen WLAN-Hotspot abonniert haben und die Reichweite des WLANs beschränkt ist, suchten die Forscher auch nach alternativen Möglichkeiten für einen Erstzugriff. Aufgrund einer weiteren Sicherheitslücke gelang es den Forschern, sich mit einer Femtozelle, einer Miniatur-Mobilfunk Basisstation, über das Mobilfunknetz in das Fahrzeug einzuhacken. Über einen Massen-Scan konnten sie hunderttausend Chrysler Fahrzeuge finden, die die beschriebenen Sicherheitslücken in ihrem Multimediasystem aufwiesen. Obwohl das Multimediasystem nicht direkt mit dem CAN-Bus verbunden ist, entdeckten sie einen Controller, der zumindest CAN-Bus Signale empfangen konnte. Durch Reverse Engineering und einem Update des Controllers mit manipulierter Firmware gelang es ihnen schließlich, eine Kommunikation mit dem CAN-Bus herzustellen. Dadurch konnten sie die cyber-physikalischen Systeme des Autos manipulieren, wie beispielsweise das Lenkrad, den

Motor, das Getriebe und das Bremssystem. Aufgrund dieses Hacks musste Fiat Chrysler im Jahr 2015 rund 1,4 Millionen Fahrzeuge in die Werkstätten zurückrufen, um die Sicherheitslücken durch Softwareupdates zu schließen /CHA15r01/.

- Im Jahr 2022 gelang es einem Angreifer mit einem sogenannten „CAN-Bus-Injection“-Angriff, einen Toyota RAV4 zu stehlen. Für den Erstzugriff verschaffte sich der Angreifer Zugang zum Kabel des CAN-Bus, das mit dem Steuergerät des Lichtes verbunden ist, indem er die Außenverkleidung am Vorderlicht demontierte. Durch Anschließen eines manipulierten Bluetooth Lautsprechers an den CAN-Bus konnte er in das CAN-Bus Netzwerk eindringen. Dort wurde mittels einem im CAN-Injector verbauten CAN-Transceiver die CAN-Bus Kommunikation des Fahrzeugs gestört und daraufhin das Bussignal, das bei einem in der Nähe befindlichen Schlüssel gesendet wird, vorgetäuscht. Durch weitere Manipulationen gelangte dieses Signal auf den CAN-Bus für die Antriebssteuerung, so dass die Wegfahrsperre entriegelt wurde. Mittels des CAN-Bus-Injectors wurde dann noch eine gefälschte Nachricht an das Türsteuergerät gesendet, in der ein gültiger Schlüssel und damit das Signal für die Entriegelung vortäuscht wurde. Die Angreifer konnten damit schließlich die Türen öffnen und das Auto entwenden. /TIN23w02/

2.6 Cyberangriffe auf den Energiesektor

Cyberangriffe auf den Energiesektor können zu Stromausfällen führen und regionale bis internationale Auswirkungen haben. In diesem Zusammenhang muss nicht der Energieversorger zwingend das eigentliche Ziel des Angriffs sein. Es genügt bereits, wenn Geräte eines Herstellers, die von einem Angriff betroffen sind, in ICS-Systemen von Energieanlagen eingesetzt werden und zusätzlich eine unzureichende Trennung zwischen Büro-Netzwerken und ICS-Systemen vorliegt. Schadsoftware, die über Verbindungen zwischen den Büro-Netzwerken und dem Internet eingeschleust wurde, kann sich dann auf die ICS-Systeme ausbreiten und den Anlagenbetrieb stören und im schlimmsten Fall zum Ausfall der Anlage führen. Darüber hinaus gibt es weitere Möglichkeiten, Schadsoftware in ICS-Systemen einzuschleusen, z. B. über einen Innentäter, der ein kompromittiertes Gerät über eine Schnittstelle mit dem ICS-System verbindet. Seit dem russischen IT-Angriff mit der Schadsoftware BlackEnergy3 auf das ukrainische Stromnetz im Jahr 2015 /CIS16i01, ITB16r01/, sind verstärkt gezielte Angriffe auf den Energiesektor zu beobachten. Vor allem mutmaßlich russischen APT-Gruppierungen hat die Ukraine dabei regelrecht als Versuchslabor gedient. Bereits ein Jahr nach dem Angriff mit BlackEnergy3 kam es im Jahr 2016 zu einem Stromausfall, nachdem ein Umspannwerk

in Kiew mit der Schadsoftware Crashoverride/Industroyer angegriffen worden war /DRA20r01, ESE17r01/. Bei Crashoverride/Industroyer handelt es sich um die erste Schadsoftware, mit der ICS-Systeme von Umspannwerken und anderen elektrischen Einrichtungen gezielt manipuliert werden können. Darüber hinaus gibt es eine Vielzahl weiterer IT-Angriffe auf den Energiesektor, bei denen die ICS-Systeme und deren Manipulation, bis hin zu physischen Schäden, nicht im Vordergrund stehen. Im März 2019 kam es zum ersten dokumentierten IT-Angriff auf einen Betreiber von Windkraft- und Solaranlagen in den USA, der daraufhin die datentechnische Verbindung zu seinen energieerzeugenden Anlagen verlor /NER19r01, SEA19w01/. Es werden vermehrt IT-Angriffe, darunter Ransomware-Angriffe, beobachtet, bei denen sensible Daten entwendet und unter Umständen im Darknet zum Verkauf angeboten werden. Diese Daten können dann für die Planung und Vorbereitung späterer Angriffe auf den Energiesektor genutzt werden. Als Beispiel ist hier die seit dem Jahr 2015 andauernde Angriffswelle der APT-Gruppierung Dragonfly /THA20f01, SYM17r01/ gegen Unternehmen des Energiesektors zu nennen. Dabei sammeln die Angreifer gezielt Informationen zu industriellen Steuerungssystemen und deren Bedienung. Auch IT-Angriffe, die nicht primär auf den Energiesektor abzielen, können sich indirekt auf diesen auswirken. Beim russischen Einmarsch in die Ukraine im Februar 2022 erfolgte ein IT-Angriff auf den Kommunikationssatelliten KA-SAT, woraufhin dieser ausfiel /GOL22w01/. Dies hatte Auswirkungen auf Windkraftanlagen des deutschen Energieanbieters Euroskypark. Im Falle eines Fehlers war eine Entstörung aus der Ferne durch den Ausfall der Kommunikationsverbindung nicht mehr möglich.

Diese sowie weitere IT-Angriffe auf Anlagen und Einrichtungen zur Stromerzeugung und -übertragung werden im Folgenden kurz beschrieben:

- Am 23.12.2015 ereignete sich ein IT-Angriff der russischen APT-Gruppierung Sandworm mit der Schadsoftware BlackEnergy3, auch als BlackEnergy Lite bezeichnet, auf das ukrainische Stromnetz /CIS16i01, ITB16r01/. Es wurden insgesamt drei Energieversorgungsunternehmen erfolgreich angegriffen, was zu einem mehrstündigen Stromausfall führte, von dem etwa 225.000 Kunden betroffen waren. Drei weitere Unternehmen wurden ebenfalls angegriffen, ihr Betrieb konnte aber aufrechterhalten werden. Die Schadsoftware BlackEnergy3 beinhaltet Plugins und Funktionen, die im Wesentlichen auf die Auskundschaftung von Netzwerken ausgerichtet sind, sowie zusätzlich eine KillDisk-Komponente zur Datenlöschung. Eine spätere, abgewandelte Version der Schadsoftware bietet zusätzlich die Möglichkeit, ICS-Systeme zu manipulieren. Die IT-Angreifer erhielten über Remote-Zugänge

Zugriff auf die Büro-IT und die Leittechniksysteme. Über die KillDisk-Komponente wurden anschließend für den Betrieb erforderliche Daten gelöscht. Darüber hinaus wurde die unterbrechungsfreie Stromversorgung für die Server angegriffen. Es wird davon ausgegangen, dass BlackEnergy3 bei dem Angriff hauptsächlich eine unterstützende Rolle spielte, um Zugriff auf die IT-Netzwerke der Anlagen zu erhalten.

- Ende des Jahres 2015 erfolgte ein IT-Angriff mit der Schadsoftware GreyEnergy auf ein Energieversorgungsunternehmen in Polen /ESE18r01/. Danach fanden weitere IT-Angriffe mit der Schadsoftware gegen Ziele aus dem Bereich der kritischen Infrastrukturen in Zentral- und Osteuropa statt. Der Schwerpunkt lag dabei auf Organisationen in der Ukraine. Die Schadsoftware ist modular aufgebaut und dient im Wesentlichen dazu, Netzwerke auszukundschaften und Zugangsrechte zu erhalten. Sie ist nicht in der Lage, ICS-Systeme direkt zu beeinflussen. Die APT-Gruppierung, die die Schadsoftware entwickelt hat, wird ebenfalls als GreyEnergy bezeichnet.

- Ab dem Jahr 2015 führte die APT-Gruppierung Dragonfly /THA20f01, SYM17r01/ eine Angriffswelle gegen Unternehmen im Energiesektor einschließlich der kerntechnischen Industrie sowie der Öl- und Gasindustrie durch. Die Angriffe erreichten im Jahr 2017 einen vorläufigen Höhepunkt, dauern aber nach wie vor an und konzentrieren sich auf Unternehmen in Europa, darunter auch Unternehmen in Deutschland, sowie auf Unternehmen in den USA und in einigen asiatischen Ländern. Häufig greifen die Angreifer die anvisierten Ziele nicht direkt an, sondern kompromittieren zunächst geeignete Zwischenziele in der Lieferkette. Endgültig ins Zielnetzwerk eingedrungen, sammeln sie Informationen zu den industriellen Steuerungssystemen wie Konfigurations- und Zugriffsinformationen sowie Informationen zu deren Bedienung einschließlich der Erfassung von Screenshots während des Betriebs. Mindestens ein Angriff erfolgte auf eine kerntechnische Anlage, das US-amerikanische Kernkraftwerk Wolf Creek. In einer ersten Reaktion gab die Anlage an, die möglichen Auswirkungen des Angriffs seien auf die administrativen und geschäftlichen Teile des Anlagennetzwerks beschränkt, die Untersuchungen seien aber noch nicht abgeschlossen.

- Im Dezember 2016 führte die russische APT-Gruppierung ELECTRUM, welche in direkter Verbindung zur Gruppierung Sandworm steht, einen weiteren Angriff auf das ukrainische Stromnetz aus /DRA20r01, ESE17r01/. Von dem IT-Angriff war ein Umspannwerk in Kiew betroffen, was zu einem Stromausfall führte, der über eine Stunde andauerte. Die Angreifer setzten dabei die Schadsoftware Crashoverride, auch Industroyer genannt, ein. Sie bietet die Möglichkeit, die ICS-Systeme von

Umspannwerken und anderen elektrischen Einrichtungen direkt zu manipulieren und Schalter zu kontrollieren. Die Schadsoftware Crashoverride/Industroyer ist modular aufgebaut und kann durch zusätzliche Module erweitert werden, so dass weitere Angriffsmöglichkeiten denkbar sind. Bei dem genannten Angriff wurden die Handlungsoptionen, die die Schadsoftware bietet, nicht voll ausgeschöpft. Daher handelte es sich bei diesem Vorfall vermutlich um einen Test der Schadsoftware. Hierfür spricht auch, dass der Angriff nach etwa einer Stunde von Angreiferseite beendet wurde.

- In der ersten Hälfte des Jahres 2019 wurde die Wiper[15]-Schadsoftware ZeroCleare bei mehreren Angriffen auf den Energiesektor im Mittleren Osten eingesetzt /IBM20i01/. IT-Sicherheitsanalysten von IBM Security haben die Schadsoftware entdeckt. Der Wiper versucht auf den infizierten Systemen so viele Daten wie möglich zu löschen. Für Windows-basierte Systeme bedeutet das, dass ZeroCleare versucht, den Master Boot Record (MBR) zu überschreiben und Partitionen zu beschädigen. Nach eingehender Untersuchung der Schadsoftware äußerte IBM die Vermutung, dass die Angriffe von iranischen, staatlich geförderten Angreifern durchgeführt wurden. Die Rede ist hierbei von APT34, auch OilRig genannt, sowie von mindestens einer weiteren Gruppierung.

- Im März 2019 kam es zum ersten dokumentierten Fall eines IT-Angriffs auf einen Erzeuger erneuerbarer Energien in den USA /SEA19w01/. Bei diesem IT-Angriff verlor der betroffene Energieversorger die datentechnische Verbindung zu seinen energieerzeugenden Windkraft- und Solaranlagen. Der Betreiber sPower wurde hierbei Opfer eines IT-Angriffes auf Firewalls des Herstellers Cisco. Der Angriff erfolgte über eine bekannte Schwachstelle in der Software der Cisco Firewalls. Die zugehörige Hardware der Firewall wurde durch den Vorfall überlastet, sodass der Netzwerkverkehr von sPower zu seinen Anlagen nicht mehr weitergeleitet wurde. Hierbei handelte es sich nach bisherigen Berichten nicht um einen zielgenauen IT-Angriff auf den Energieerzeuger, sondern um Flächenangriffe. Es kam zu keinen Folgeangriffen auf die technische Infrastruktur von sPower.

- Im Oktober 2020 kam es in Mumbai zu einem Stromausfall, von dem 20 Millionen Menschen betroffen waren /ECT21w01/. Vermutlich war der Stromausfall die Folge

[15] 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.

eines IT-Angriffs einer mutmaßlich chinesischen Angreifergruppierung auf ein nahe gelegenes Stromlastmanagementzentrum. Dem Ereignis waren politische Spannungen zwischen Indien und China vorrausgegangen. Bis heute ist nicht vollständig klar, ob es sich bei dem Stromausfall um einen IT-Angriff oder um technisches bzw. menschliches Versagen gehandelt hat. Analysten gehen von einem IT-Angriff aus, was von offizieller, indischer Seite aber bestritten wird.

- Im Februar 2021 kam es zu einem IT-Sicherheitsvorfall im brasilianischen Kernkraftwerk Angra /REU21r01/. Dabei wurde von den Angreifern die Ransomware Darkside eingesetzt. Neben dem Kernkraftwerk wurden auch dessen Betreiber Eletrobras und der Energiekonzern Copel mit der Schadsoftware angegriffen und Informationen von Copel wurden entwendet. Der IT-Sicherheitsvorfall hatte keinen Einfluss auf den Betrieb des Kernkraftwerks.

- Ab Februar 2022 kam es unter Ausnutzung der Schwachstelle Log4Shell in der Software VMWare Horizon zu IT-Angriffen durch die nordkoreanische APT-Gruppierung APT 38, auch Lazarus genannt, auf Energieunternehmen in den USA, Kanada und Japan /CSD22w01, CIS22r05, SYM22r01/. Über die Schwachstelle erlangten die Angreifer Zugriff auf über das Internet erreichbare Server und über diese auch auf die Daten und Netzwerke der betroffenen Energieunternehmen. Sie nutzten drei unterschiedliche Schadsoftwaren für den Aufbau eines langfristigen Zugriffs und das Auslesen von Zugangsdaten und weiteren für die Angreifer relevanten Datensätzen. Die langfristigen Ziele der Angriffe scheinen insbesondere das Auslesen von Zugriffsdaten, die Etablierung innerhalb des Netzwerks der angegriffenen Unternehmen und der allgemeine Abfluss von Daten gewesen zu sein.

- Im Februar 2022 begann Russland mit der Invasion der Ukraine /GOL22w01/. Parallel zu den physischen Kampfhandlungen wurden auch IT-Angriffe gegen die Ukraine durchgeführt. Am 08.04.2022 sollten offenbar durch den Einsatz der Schadsoftware Industroyer 2 industrielle Steuerungssysteme in Hochspannungsumspannwerken sabotiert und so ein Blackout hervorgerufen werden, von dem etwa zwei Millionen Menschen betroffen gewesen wären. Der Angriff, der der APT-Gruppierung Sandworm zugeschrieben wird, wurde jedoch rechtzeitig erkannt und ein Stromausfall konnte verhindert werden. Die Schadsoftware Industroyer 2 basiert auf der Schadsoftware Industroyer bzw. Crashoverride, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert.

- Bei KA-SAT (KASAT Viasat) handelt es sich um einen Kommunikationssatelliten der US-amerikanischen Firma Viasat. Mit 82 Spotbeams erreicht er eine europaweite Abdeckung. Am 24.02.2022, um 4 Uhr UTC kam es in Folge eines IT-Angriffs mit der Wiper-Schadsoftware AcidRain zu einem Ausfall der Kommunikation über den KA-SAT-Satelliten /GOL22w01, SEN22w02/. Dieser erfolgte nahezu zeitgleich mit dem Angriff durch russische Streitkräfte auf die Ukraine. Hierbei wird ein Zusammenhang vermutet. Beweise hierzu liegen bisher allerdings nicht vor. Der Ausfall des Satelliten hatte auch Auswirkungen auf Windkraftanlagen des deutschen Energieanbieters Euroskypark. Zwar laufen die Anlagen autark weiter und ihre Steuerung ist weiterhin gewährleistet, aber eine Entstörung im Falle eines Fehlers ist aus der Ferne bei einem Ausfall der KA-SAT-Verbindung nicht möglich.

- Im Oktober 2022 führte ein Cyberangriff durch die APT-Gruppierung Sandworm zu einem ungeplanten Stromausfall in der Ukraine /MAN23r02/. Die Angreifer erlangten ab Juni 2022 Zugriff auf die IT-Systeme des angegriffenen Energieunternehmens und anschließend ohne den Einsatz von weiterer Schadsoftware Zugriff auf die OT-Systeme. Am 10. Oktober 2022 nutzten die IT-Angreifer ihre erlangten Zugriffe und führten native Befehle des SCADA Systems (Typ MicroSCADA) aus, wodurch es zum Schalten der Leistungsschalter der Anlage und im Anschluss zum Ausfall der Anlage kam. Der Angriff erfolgte im Kontext der zu diesem Zeitpunkt stattfindenden Angriffskampagne Russlands gegen das ukrainische Strom- und Wärmenetz im Rahmen des russisch-ukrainischen Krieges.

- Um den Schutz kritischer Infrastrukturen in den USA zu verbessern, hat das FBI im Jahr 1996 das InfraGard-Programm ins Leben gerufen. IT-Angreifer, die sich selbst als „USDoD“ bezeichnen und das Siegel des U.S. Department of Defense verwenden, haben sich im InfraGard-Programm angemeldet und konnten die Datenbank wichtiger Schlüsselpersonen aus dem Bereich kritischer Infrastrukturen kopieren /RHP22w01/. Die Datenbank dient dazu, ein Vernetzen der Schlüsselpersonen zu ermöglichen. Die Angreifer haben die abgegriffenen Daten seit dem 10.12.2022 in einem Darknet-Forum zum Verkauf angeboten. Offenbar betrifft der Datendiebstahl die Informationen von mehreren zehntausend Menschen, zu denen auch Mitarbeiter von Energieversorgern und Kernenergieunternehmen gehören.

- Im Mai 2023 wurden insgesamt 22 dänische Unternehmen im Bereich der Energieversorgung Opfer eines großflächigen Cyberangriffs /SEC23r01, ZYX23w01/, der in zwei Wellen erfolgte. Die Cyberangriffe zielten auf eine zuvor bekannt gewordene Schwachstelle in Firewalls des Herstellers Zyxel ab, welche sich mit einfachen

Netzwerkbefehlen auf die Firewall ohne eine Authentifizierung ausnutzen lässt. Die Firewalls wurden von den betroffenen Energieunternehmen in Dänemark als Schnittstelle und zur Sicherung von leittechnischen Umgebungen von anderweitigem Netzwerkverkehr und zur Kontrolle des Datenverkehrs aus dem Internet in die leittechnischen Umgebungen eingesetzt. Die RCE-Schwachstelle ermöglicht die Kontrollübernahme über die eingesetzten Firewalls. /ZYX23w01, SEC23r01/

Darüber hinaus erfolgten IT-Angriffe mit Ransomware auf den Energiesektor, die das Ziel hatten, sensible Daten zu stehlen und/oder zu verschlüsseln, um anschließend eine Lösegeldforderung für die Nicht-Veröffentlichung und/oder die Entschlüsselung der Daten zu stellen. Am 19.11.2021 wurde ein IT-Angriff auf Vestas Wind Systems A/S, einem der weltweit größten Hersteller von Windenergieanlagen mit Hauptsitz in Dänemark, entdeckt /ITD21w01/ und am 31.03.2022 wurde festgestellt, dass es zu einem IT-Angriff auf Nordex, einem der weltweit größten Hersteller und Service Provider von Windenergieanlagen mit Niederlassungen in mehr als 30 Ländern und Hauptsitz in Deutschland, gekommen ist /BLE22w04, NOR22w01, SEC22w04/. Die APT-Gruppierung Black Basta führte am 11.04.2022 einen IT-Angriff auf die Deutsche Windtechnik durch /BLE22w02, SEC22w03/. Am 22. Juli 2022 erfolgte ein IT-Angriff der APT-Gruppierung BlackCat auf den luxemburgischen Netzbetreiber Creos und den luxemburgischen Energieversorger Enovos, die beide zur Encevo-Gruppe gehören und eine Gaspipeline sowie die Stromversorgung in Luxemburg betreiben /FBI22l02, SEC22w02/. Am 19.08.2022 erfolgte ein IT-Angriff der APT-Gruppierung Ragnar Locker auf den griechischen Gasnetzbetreiber Desfa /CSO22w03, SEC22w14, SEC22w15/. In allen Fällen waren die ICS-Systeme von den Angriffen nicht betroffen, da diese in der Regel vom Büro-IT-Netzwerk isoliert sind und nur letzteres eine Verbindung zum Internet besitzt. Aber da von den Unternehmen kein Lösegeld gezahlt wurde, wurden die gestohlenen sensiblen Daten veröffentlicht. Diese umfassen unter anderem personenbezogene Daten von Mitarbeitern (z. B. Ausweiskopien, E-Mails, Daten zu Bankkonten) und Vertragsdaten.

Cyberangriffe auf den Energiesektor stellen eine wachsende Bedrohung dar. Der Einsatz von speziell ausgelegter Schadsoftware wie Crashoverride/Industroyer zeigt, dass eine Spezialisierung von APT-Gruppierungen auf ICS-Systeme erfolgt, die im Bereich der Energieversorgung eingesetzt werden. Die Angreifer verfügen über das technische Verständnis, die Mittel und die Fähigkeiten, ICS-Systeme elektrischer Einrichtungen gezielt zu manipulieren. Um die Auswirkungen solcher Angriffe zu verhindern oder wenigstens zu minimieren, sind umfassende Sicherungsmaßnahmen u. a. zur rechtzeitigen

Detektion eines IT-Angriffs auf die IT-Systeme in den elektrischen Einrichtungen und zur umgehenden Reaktion darauf, wie beispielsweise im Fall des IT-Angriffs mit Industroyer 2, ausschlaggebend.

2.7 Cyberangriffe in politischen Spannungsfeldern

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

Das Spannungsfeld Russland-Ukraine bzw. Russland-NATO stellt im Moment zwar eines der sichtbarsten, aber bei Weitem nicht das einzige politische Spannungsfeld dar, in dem Cyberangriffe eine bedeutende Rolle spielen. Ein zentraler Punkt hierbei ist, dass solche Spannungsfelder nicht losgelöst vom restlichen Weltgeschehen existieren, sondern sich häufig gegenseitig beeinflussen. So hat der Krieg in der Ukraine auch Auswirkungen auf Cyberangriffe und Angreiferaktivitäten in weiteren Spannungsfeldern. Eine Reihe von APT-Gruppierungen, die dem chinesischen, nordkoreanischen oder iranischen Nexus zugeordnet werden, nutzten beispielsweise die Situation in der Ukraine oder auch die EU-Sanktionen gegen Russland für ihre Zwecke.

Krieg in der Ukraine

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

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

- So kam es bereits in den Jahren 2015 und 2016 zu gezielten Cyberangriffen auf das ukrainische Stromnetz. Im Dezember 2015 wurden mehrere ukrainische Energieversorgungsunternehmen unter Einsatz der Schadsoftware Black Energy 3 /CIS16i01, ITB16r01/ angegriffen. Einige der angegriffenen Unternehmen konnten den Betrieb aufrechterhalten, dennoch waren die physischen Auswirkungen so groß, dass es zu einem mehrstündigen Stromausfall für ca. 225.000 Kunden kam.

- Im Dezember 2016 wurde unter Einsatz der Schadsoftware Crashoverride/Industroyer /DRA20r01, ESE17r01/ ein Umspannwerk in Kiew angegriffen, wodurch es zu einem einstündigen Stromausfall im Großraum Kiew kam. Während beide Cyberangriffe von ihrem Effekt her der Demonstration von Fähigkeiten und dem Aufbau einer Drohkulisse zugeordnet werden können, erfüllte der Cyberangriff im Jahr 2016 offenbar noch einen weiteren Zweck. So wurde dieser Angriff nach etwa einer Stunde von den Angreifern selbst beendet, was stark für einen Testcharakter des Angriffs spricht.

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

ukrainische Regierungseinrichtungen und Einrichtungen im IT-, Energie- und Finanzsektor. Zusätzlich wurden auch DDoS-Angriffe in diesen Bereichen durchgeführt:

- Besonders hervorzuheben ist hierbei die Schadsoftware WhisperGate, die den Berichten /REC22w02/ zufolge vornehmlich gegen Ziele in der Ukraine – darunter Regierungseinrichtungen, Non-profit-Organisationen und IT-Organisationen – eingesetzt wurde. Dabei handelt es sich um einen Wiper, der unter dem Deckmantel eines Ransomware-Angriffs den Master Boot Record des angegriffenen Systems zerstört.

Seit Kriegsbeginn hat sich die Situation weiter verschärft:

- Direkt mit Kriegsbeginn, nahezu zeitgleich mit dem Beginn des Angriffs russischer Streitkräfte auf die Ukraine, am Morgen des 24. Februar 2022, erfuhr die Kommunikation über den Kommunikationssatelliten KA-SAT eine Unterbrechung, welche einen teilweisen Ausfall der Dienste des KA-SAT-Satellitennetzwerks über Europa nach sich zog /GOL22w01/. Über KA-SAT wurde zu diesem Zeitpunkt auch die Satellitenkommunikation für die ukrainische Polizei und das ukrainische Militär bereitgestellt, deren Störung das eigentliche Ziel des Cyberangriffs gewesen sein dürfte.

- Zwischen Februar und Mai 2023 hat die pro-russische APT-Gruppierung Shuckworm (auch bekannt als Gamaredon, Actinium, Primitive Bear, Trident Ursa, UAC-0010 oder Armageddon) nach Angaben des IT-Sicherheitsunternehmens Symantec Schadsoftware über USB-Geräte auf ukrainische Einrichtungen wie das Militär, Nachrichtendienste und Regierungsorganisationen verteilt. Ziel der Angriffe war offenbar das Sammeln sensibler Informationen, darunter Berichte über Personen des ukrainischen Militärs, feindliche Aktivitäten, Luftangriffe, Arsenalinventar und Militärübungen /CYH23w01, INF23w01, SEC23w09/.

- In Zusammenhang mit dem Ukrainekrieg hat die APT-Gruppierung APT28, die zu Russlands militärischem Geheimdienst gehört, diverse Phishing-Kampagnen durchgeführt /BIT23w02, SEC23w07/. Im Mai 2023 berichtete das CERT (Computer Emergency Response Team) der Ukraine „CERT-UA“ über eine laufende Phishing-Kampagne auf staatliche Regierungsbehörden in der Ukraine, die im April 2023 erfolgte. Bei dieser Kampagne wurden Mails an staatliche Regierungsbehörden in der Ukraine geschickt, die Anweisungen für die Durchführung eines vorgeblichen Windows-Updates zum Schutz vor IT-Angriffen gaben. Dabei täuschten die E-Mails als Absender den Systemadministrator der jeweiligen Behörde mit real existierendem Mitarbeiternamen vor. Die E-Mails wollten den Empfänger dazu verleiten, ein

angebliches Windows-Update zu installieren und dafür ein entsprechendes Power-Shell-Skript herunterzuladen und auszuführen. Wird das Skript vom Empfänger geöffnet, dann simuliert dieses einen Aktualisierungsprozess des Betriebssystems, lädt aber im Hintergrund ein weiteres, maliziöses Power-Shell-Skript herunter. Es ist davon auszugehen, dass APT28 mit den Angriffen beabsichtigt, sensible Daten von den infiltrierten Systemen zu stehlen und vermutlich die Arbeit der ukrainischen Regierungsbehörden zu behindern. Mit einer weiteren Phishing-Kampagne im Juni 2023 wurden laut CERT-UA E-Mail-Server ukrainischer Behörden und Regierungsstellen kompromittiert. Die Kampagne lief bereits seit November 2021, wurde aber erst im Juni 2023 in Zusammenarbeit zwischen der Insikt Group von Recorded Future und dem Computer Emergency Response Team der Ukraine (CERT-UA) entdeckt. Von dieser Phishing-Kampagne betroffen waren u. a. ein regionales Büro der Staatsanwaltschaft, eine zentrale Regierungseinheit und verschiedene Regierungsstellen, sowie eine Organisation, die sich mit der Instandhaltung militärischer Infrastruktur im Bereich Luftfahrt beschäftigt. Hauptziel dieser Kampagne war offenbar das Erlangen von militärischen Informationen, um die russische Invasion in der Ukraine zu unterstützen. Im Dezember 2023 erfolgte eine weitere Phishing-Kampagne gegen Regierungsbehörden in der Ukraine und polnische Organisationen. Etwa 60% aller Phishing-E-Mails, die im ersten Viertel des Jahres 2023 auf die Ukraine abzielten, stammten aus Russland.

- Seit Beginn des russischen Angriffskrieges gegen die Ukraine hat der Sicherheitsdienst der Ukraine (Security Service of Ukraine (SSU)) den Zugriff auf etwa 10.000 Kameras blockiert /HEI24w04, INM24w01, SSU24w01/. Kurz nach einem russischen Luftangriff mit Drohnen und Raketen am 02.01.2024 auf Kiew wurden vom SSU die IP-Adressen von zwei kompromittierten Kameras identifiziert, die den Einsatz der ukrainischen Luftverteidigung und kritische Infrastrukturen aufgezeichnet haben. Für Personen, die die Internetverbindung ihrer Kameras nicht abschalten, drohen bis zu zwölf Jahre Haft.

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

- Unter anderem gab es einen versuchten Cyberangriff auf die ukrainische Stromversorgung mit der Schadsoftware Industroyer 2 in der ersten Aprilhälfte 2022, der ukrainischen Angaben zufolge rechtzeitig erkannt und vereitelt wurde /ESE22w01/.

- Am 10. Oktober 2022 führte ein Cyberangriff durch Sandworm zu einem ungeplanten Stromausfall in der Ukraine. Der Angriffe wurde erst im November 2023 bekannt. Die Angreifer erlangten ab Juni 2022 Zugriffe auf die IT-Systeme des angegriffenen Energieunternehmens und anschließend ohne den Einsatz von weiterer Schadsoftware Zugriff auf die OT-Systeme. Am 10. Oktober 2022 nutzten die IT-Angreifer ihre erlangten Zugriffe und führten Native Befehle des SCADA-Systems (Typ MicroSCADA) aus, wodurch es zum Schalten der Leistungsschalter der Anlage und im Anschluss zum Ausfall der Anlage kam. Der Angriff erfolgte im Kontext der zu diesem Zeitpunkt stattfindenden Angriffskampagne Russlands gegen das ukrainische Strom- und Wärmenetz im Rahmen des russisch-ukrainischen Krieges /MAN23r03/.

- Am 19.04.2024 veröffentlichte das Computer Emergency Response Team der Ukraine (CERT-UA) einen umfassenden Bericht zu einer Cyberangriffskampagne auf insgesamt 20 Unternehmen der kritischen Infrastrukturen Energie, Wasser und Wärme in 10 Regionen der Ukraine /INF24r01/. Die der APT-Gruppierung Sandworm (APT44) zugeschriebene Kampagne nutze hierbei eine Vielzahl an unterschiedlichen Schadsoftwares für langfristige Zugriffe auf unterschiedliche Betriebssysteme und industrielle Steuerungen.

Die Ukraine zeigt sich jedoch nicht nur in Bezug auf konventionelle militärische Aktionen als äußerst wehrhaft. Auch in Bezug auf Cyberangriffe ist der Ukraine nach eigenen Angaben ein bedeutender Gegenschlag gelungen:

- Im März 2024 soll der ukrainische Militärnachrichtendienst GUR nach eigenen Angaben einen erfolgreichen Cyberangriff auf das russische Verteidigungsministerium durchgeführt haben /GUR24i01/. Dabei sollen Dokumente gestohlen worden sein, die Aufschluss über die Strukturen und den vollständigen Aufbau des russischen Ministeriums geben, sowie die Software, die das russische Ministerium für die Verschlüsselung seiner Daten verwendet.

Neben Cyberangriffen durch mutmaßlich von staatlichen russischen Stellen unterstützte Angreifergruppierungen auf die Ukraine ist seit Beginn des Krieges auch die Entfaltung zahlreicher weiterer, kriegsbegleitender Cyberangriffe festzustellen. Dies gilt sowohl in Bezug auf Angreifer, welche mit ihren Aktivitäten die ukrainische Seite unterstützen wollen, als auch in Bezug auf Angreifer, die ihre Unterstützung für die russische Seite erklärt haben.

Bereits vor Ausbruch der physischen Kriegshandlungen, aber verstärkt seit dem russischen Angriff auf die Ukraine, ist nicht nur die Ukraine das Ziel von Cyberangriffen von russischen Angreifergruppierungen geworden, sondern vermehrt auch Länder, die sich unterstützend gegenüber der Ukraine zeigen oder sich gegen den russischen Angriffskrieg aussprechen. Beispielsweise wurden nahezu alle Mitgliedsstaaten der NATO seit dem Jahr 2022 Opfer von Cyberangriffen, die in Zusammenhang mit dem Angriff auf die Ukraine stehen. Zudem ist zu erwähnen, dass auch weltweite Partner-Länder der NATO Ziel solcher Cyberangriffe waren. Die beobachteten Cyberangriffe werden von verschiedenen Angreifergruppierungen wie beispielsweise Killnet oder NoName057(16) durchgeführt.

In den Jahren 2022 und 2023 waren zahlreiche europäische NATO-Mitgliedsstaaten von politisch motivierten Cyberangriffen im Zusammenhang mit dem Krieg in der Ukraine betroffen. Darunter befanden sich beispielsweise Albanien /FOR23w01/, Belgien /CPO23w01, BLO23w01, SAK23w01/, Bulgarien /UKR23w01, SAK23w01/, Dänemark /REU23w02, DER23w01, SAK23w01/, Deutschland /SPI23w01, SAK23w01, SYS22w01/, Estland /SAK23w01, SYS22w01/, Finnland /DAI23w03, SAK23w01/, Frankreich /REC23w01, SAK23w01/, Griechenland /MIM23w01, SAK23w01/, Großbritannien /COM23w01, SAK23w01/, Island /EUR23w02/, Italien /REC23w01, SAK23w01, SYS22w01/, Lettland /BIT23w01, SAK23w01, SYS22w01/, Litauen /LRT23w01, SAK23w01/, Luxemburg /LUX23w01/, Niederlande /REC23w01, SAK23w01/, Nord-Mazedonien /NAT23w01/, Norwegen /COM23w01/, Polen /FOC23w01, SAK23w01, SYS22w01/, Portugal /EUR23w01/, Rumänien /SYS22w01/, Slowakei /UKR23w02/, Spanien /REC23w01, SAK23w01/, Tschechien /EXP23w01, SAK23w01, SYS22w01/ und die Türkei /MIC22w01/.

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

Äußerungen gegen den russischen Angriffskrieg waren in der Vergangenheit ausreichend, um Ziel eines Cyberangriffes seitens prorussischer Angreifer zu werden.

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

- Im August 2023 kam es zu zwei Cyberangriffen auf die polnische Bahn, bei denen es aufgrund eines unbefugten Sendens eines Nothalt-Signals zum Anhalten von Zügen kam. Hierbei wurde der Bahnverkehr in den nordwestlichen, südwestlichen und nördlichen Provinzen von Polen beeinflusst. Bei den Cyberangriffen wurde eine lang bekannte Schwachstelle des analogen Funksystems ausgenutzt. Beide Male kam es zu physischen Auswirkungen /WIN23w01, HEI23w01, WIR23w01/.
- Ebenfalls im August 2023 wurden mehrere deutsche Webseiten Ziel eines Cyberangriffs, darunter befanden sich deutsche Versicherungskonzerne und die Webseite des Bundesfinanzministeriums (BMF). Dieser Cyberangriff war Teil des DDoSia-Projektes, welches durch die Angreifergruppierung NoName057(16) ins Leben gerufen wurde. Jeder Hacker kann Teil dieses Projektes werden und Cyberangriffe auf vorzugsweise östliche und westliche NATO-Länder, wie Litauen, Polen, Italien, Frankreich oder Deutschland durchführen /SAK23w01, GOL23w02, THN23w01/.
- Im Fokus einer Phishing-Kampagne, die zwischen März und Mai 2023 durchgeführt wurde, standen auch zahlreiche osteuropäische Mitgliedsstaaten. Die Infizierung der Opfer erfolgte mit einer neuen Backdoor namens Graphical Proton, ausgeführt wurden die Angriffe von der APT-Gruppierung APT29 /SEC23w10/.

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

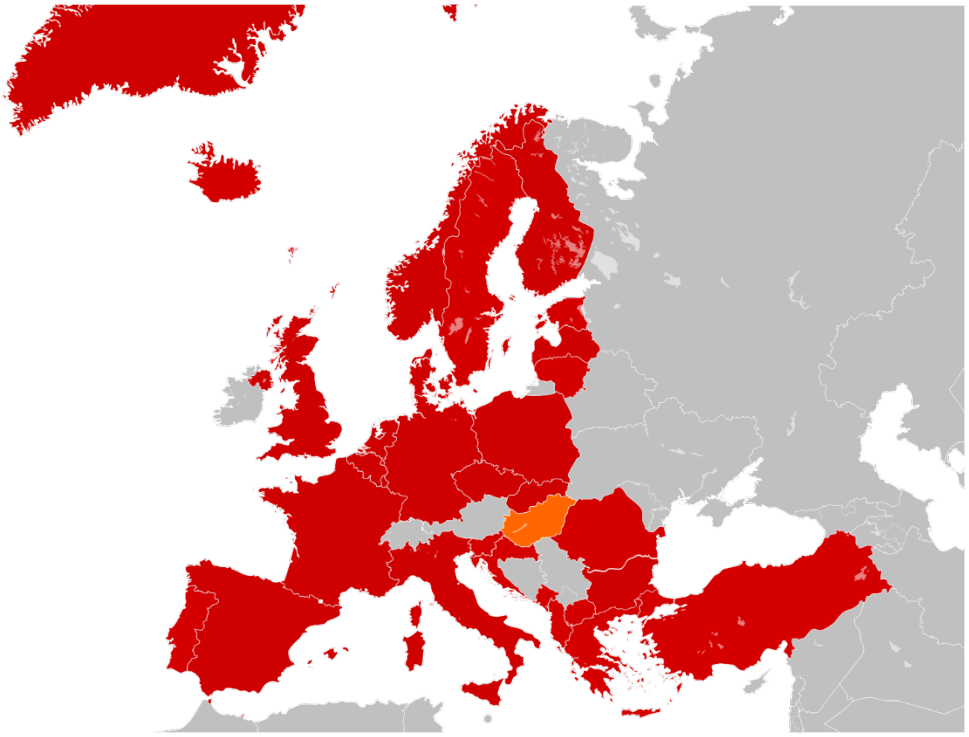

Abb. 2.1 Europäische NATO-Mitgliedsstaaten, die seit Ausbruch des Krieges in der Ukraine Opfer eines Cyberangriffs wurden

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

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

Es ist zudem anzumerken, dass nicht nur europäische Mitgliedsstaaten der NATO bereits das Ziel von Cyberangriffen von prorussischen Angreifergruppierungen geworden sind, sondern auch die nicht-europäischen NATO-Mitgliedsstaaten USA /SAK23w01, SYS22w01/ und Kanada /REU23w03/, sowie NATO-Partnerstaaten, wie Österreich /BLE22w09/, die Schweiz /SWI23w01/, Japan /TAS23w01/ und Australien /ABC23w01/.

Insgesamt ist im Zusammenhang mit dem Krieg in der Ukraine bereits vor Beginn der Kampfhandlungen eine deutliche Zunahme an Cyberangriffen bekannt geworden. Seit Beginn der Kampfhandlungen wurde darüber hinaus ein deutlicher Anstieg bei den

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

China-Japan

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

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

Beispiele für Angriffe, die chinesischen Angreifergruppierungen zugeschrieben werden, sind der Supply Chain Angriff auf E-Mail Security Gateway-Geräte des Herstellers Barracuda, bei dem unter Ausnutzung einer Zero-Day-Schwachstelle Backdoors auf kompromittierten Systemen installiert wurden /NVD23i06/ und die Angriffskampagne mit Volt

Typhoon zur Ausspähung kritischer Infrastrukturen in den USA. Bei letzterem wurden von mutmaßlich chinesischen Angreifern vornehmlich Ziele aus den Bereichen Kommunikation, Transport, Herstellung und IT angegriffen, sowie militärnahe Einrichtungen auf der Pazifikinsel Guam, auf der sich ein wichtiger US-Luftwaffenstützpunkt befindet.

Nordkorea-Südkorea

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

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

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

Iran-Israel

Seit Jahren werden im politischen Spannungsfeld Iran-Israel von beiden Seiten Cyberangriffe durchgeführt. Ein eindrückliches Beispiel aus dem Juni 2022 ist der Cyberangriff auf ein iranisches Stahlwerk. Die Cyberangriffe sind insgesamt sehr zahlreich und nehmen sowohl an Häufigkeit als auch an Komplexität zu. Bei den Angriffen von iranischen Angreifergruppierungen auf Ziele in rivalisierenden oder verfeindeten Staaten wie Israel zeichnet sich inzwischen ein Shift von überwiegend disruptiven Angriffen hin zu Angriffen zu Spionagezwecken ab. Im vergangenen Jahr wurden u. a. hochentwickelte Spionageangriffe auf Verteidigungs- und Nachrichtendienste in Israel, Saudi-Arabien und Jordanien beobachtet, die alle iranischen Angreifern zugeschrieben werden. Hierbei wurden jeweils nicht nur E-Mail-Kommunikationsdaten ausgeschleust, sondern auch zentrale Informationen über die Cyber-Infrastruktur. Verschiedene Gruppierungen, welche dem Nexus des Iran zugerechnet werden, verüben zudem seit mehr als einem Jahrzehnt umfangreiche Cyberangriffe. Bereits 2010 wurde von den islamischen Revolutionsgarden (IRGC) des Iran die Rolle des „Soft Wars“ und der Nutzung von psychologischen Operationen („PSYOPS“) zur Stärkung des eigenen Regimes und Schwächung wahrgenommener Feinde offiziell festgeschrieben. Im Verlauf der Entwicklung des iranischen Cyberprogramms wurde daher verstärkt auf Social Engineering Maßnahmen gesetzt. Diese Angriffsmethoden dienen dazu, die Angegriffenen durch die Vorspiegelung falscher Tatsachen und das Ausnutzen menschlicher Verhaltensweisen zur Preisgabe von Zugangsrechten, Passwörtern und anderen wertvollen Details zu bewegen. Social Engineering Angriffe seitens iranischer Angreifer werden inzwischen fortwährend geführt und dabei immer wieder der momentanen Zielsetzung angepasst. Neben Angriffen auf Menschenrechtsaktivisten, Dissidenten und militärische Gegenspieler sind auch Angriffe auf Ziele aus den Bereichen Finanzen, Medizin, Forschung und Entwicklung sowie IT bekannt geworden. Die APT-Gruppierung CyberAv3ngers ist vermutlich dem Korps der Islamischen Revolutionsgarde (IRGC) angeschlossen. Die CyberAv3ngers sind nachweislich seit mindestens dem Jahr 2020 aktiv und haben umstrittene und falsche Behauptungen über Angriffe auf kritische Infrastrukturen in Israel aufgestellt. Im Zusammenhang mit dem Angriff der Hamas auf Israel am 07.10.2023 wurde ein Anstieg an Cyberoperationen beobachtet. Laut Analysen von Microsoft wurde eine Beteiligung von iranischen Gruppierungen (Islamische Revolutionsgarde und Ministerium für Nachrichtenwesen) im Cyberbereich erst ab dem 18.10.2023 beobachtet.

Am 17. September 2024 ereigneten sich im gesamten Libanon sowie in Damaskus in Syrien mehrere tausend kleinere Explosionen, als Funkmeldeempfänger (kurz Pager), welche zur Kommunikation eingesetzt wurden, unmittelbar explodierten und dabei mehrere tausend Personen verletzten und mehrere Todesopfer forderten. Am darauffolgenden Tag explodierten im Libanon Handfunkgeräte mit einer erhöhten Explosionsstärke, welche wiederum zu zahlreichen Verletzen und Todesopfern führten. Seit Jahrzehnten stehen sich der Staat Israel sowie die von der EU als Terrororganisation eingestufte libanesische Partei und Miliz Hizbullah verfeindet gegenüber, wobei wiederkehrend kriegerische Akte beiderseitig ausgeführt werden. Die Spannungen zwischen Israel und der Hizbullah nahmen in der Konsequenz des 07.10.2023 und den darauffolgenden Militäraktionen Israels im Gazastreifen stark zu. Am 17.09.2024 gegen 15:30 Uhr Ortszeit erhielten tausende Mitglieder der Hizbullah zeitgleich eine Nachricht auf ihren zur Kommunikation eingesetzten Pagern, wenige Sekunden später explodierten die Pager und führten zu mehreren Todesopfern und mehreren tausend hauptsächlich im Gesicht, den Händen und dem Beckenbereich verletzten Personen. Am 18.09.2024 gegen 15:00 Uhr Ortszeit folgten weitere Explosionen im Libanon, bei welchen Handfunkgeräte mit größerer Explosionskraft explodierten und zu mehreren hundert Verletzten und dutzenden Todesopfern führten. Über die folgenden Tage verdichteten sich die Indizien, dass es sich um komplexe Lieferkettenangriffe handelte. Dabei wurden im Rahmen mehrjähriger Operationen staatlicher Geheimdienste und unter dem Einsatz von Tarnfirmen die Geräte mit dem Sprengstoff PETN innerhalb der internen Batterien der Geräte an die Hizbullah verkauft und von dieser aufgrund der Sorge vor dem Einsatz von Smartphones als Kommunikationsmittel an ihre Mitglieder ausgegeben. /BBC24r01, TOI24r01, REU24r01/

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

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

2.8 Physische Angriffe auf IT-Systeme und IT-Angriffe mit physischen Auswirkungen

IT-Systeme können nicht nur durch Cyberangriffe, sondern auch durch physische Angriffe in Mitleidenschaft gezogen werden. Bei einem physischen Angriff auf ein IT-System wird eine gezielte, physische Attacke ausgeführt. Das Ziel einer solchen Attacke kann es beispielsweise sein, Teile eines IT-Systems oder das ganze System zu sabotieren, zu beschädigen oder zu zerstören. Dies kann beispielsweise durch Brandstiftung, Sprengstoffanschläge, Zerstörung einzelner Komponenten oder das Einbringen von Schadstoffen geschehen. Weitere Ziele physischer Angriffe können beispielsweise die Unterbrechung von Betriebsabläufen (z. B. durch Stören der Stromversorgung oder der Kommunikation) oder der Diebstahl sensibler Daten (z. B. durch Einbrecher) sein. Der physische Angriff kann dabei verschiedene Formen annehmen, wie z. B. Einbruch, Vandalismus, Sabotage oder Terroranschläge.

Um sich vor physischen Angriffen gegen IT-Systeme zu schützen, können diverse Maßnahmen eingeführt werden. Dazu zählen z. B. Zugangskontrollen, um nur einem gewünschten Personenkreis Zutritt zum IT-System zu gewähren und unbefugten Zutritt zu verhindern sowie das Vier-Augen-Prinzip, welches beinhaltet, dass für einen Zutritt zwei Personen erforderlich sind. Weitere mögliche Maßnahmen sind die Überwachung der Umgebung eines IT-Systems mittels Überwachungskameras oder Sicherheitspersonal oder der Einsatz von Perimeterschutz wie Zäunen, Barrieren oder anderen Schutzvorrichtungen wie Alarmanlagen. Ebenfalls relevant ist das Verhalten im Falle eines physischen Angriffs, beispielsweise durch die Ausarbeitung und regelmäßige Überprüfung von Notfallplänen für verschiedene Angriffsszenarien oder die Schulung von Mitarbeitern für das richtige Verhalten im Falle eines Angriffs oder bei Erkennen verdächtiger Aktivitäten.

Für kritische Infrastrukturen muss der Blick auf die physische Sicherheit ein essenzieller Bestandteil der Schutzmaßnahmen sein. Der alleinige Blick auf die Cybersicherheit reicht nicht aus, um IT-Systeme umfassend gegen eine wachsende Bedrohungslage zu schützen. Trotz der unterschiedlichen Schwerpunkte zwischen physischer Sicherheit (z. B. Schutz vor Einbrüchen, Vandalismus und anderen physischen Bedrohungen) und

Cybersicherheit (z. B. Schutz vor Malware, Phishing und anderen digitalen Bedrohungen) gibt es Überschneidungen zwischen den beiden Bereichen. Beispielsweise können IT-Systeme auch durch physische Sicherheitsmaßnahmen geschützt werden, während Überwachungssysteme zum Schutz der physischen Sicherheit durch Maßnahmen zur Cybersicherheit geschützt werden können. Ohne die Einrichtung physischer Schutzmaßnahmen können kritische Infrastrukturen nicht umfassend geschützt werden, da die alleinige Einrichtung von Maßnahmen gegen Cyberangriffe keinen effektiven Schutz gegen Angreifer mit direktem physischem Zugang liefert.

Ein Beispiel für einen physischen Angriff auf ein IT-System ist die Beschädigung von Glasfaserkabeln. Durch solche Angriffe kam es in der Vergangenheit z. B. zum Ausfall von Internetanbindungen sowohl von Unternehmen als auch von Privatpersonen. Durch den Diebstahl von Kupferkabeln kommt es immer wieder zu Betriebsstörungen bei der Bahn. Weitere Beispiele für physische Angriffe auf IT-Systeme sind Beschädigungen von Unterseekabeln. In den vergangenen Jahren kam es mehrmals zur Beschädigung von Unterseekabeln, beispielsweise im Oktober 2022, als drei Unterseekabel vor Südfrankreich beschädigt wurden und es dadurch zu Engpässen im Datenverkehr zwischen den USA und Europa kam. Im Februar 2023 kam es zur Beschädigung von Unterseekabeln vor Taiwan und als Folge davon zu Internetausfällen. Vier Unterseekabel im Roten Meer wurden im Februar 2024 beschädigt, wodurch bis zu 70 % des Datenverkehrs zwischen Europa und Asien unterbrochen wurden /AGE24w01, AGE24w02, HAN24w01/. Die immer weitere Verbreitung der Angriffe auf Unterseekabel im Rahmen von Sabotageakten zeigt eine Ende 2023, von zwei Gruppierungen (Houthi und Lebanese Hizbullah) getätigte Aussage, dass Unterseekabel strategische Ziele für Angriffe seien. Im November 2024 kam es zur Beschädigung von zwei Unterseekabeln in der Ostsee, wobei es sich um ein Kabel zwischen Finnland und Deutschland und ein Kabel zwischen Litauen und Schweden handelte. In einer gemeinsamen Erklärung der Außenminister von Finnland und Deutschland zu diesem Fall hieß es: *„Die europäische Sicherheit ist nicht nur durch Russlands Angriffskrieg gegen die Ukraine bedroht, sondern auch durch hybride Kriegsführung böswilliger Akteure.“* /FOC24w01/.

Ein weiteres Beispiel für einen physischen Angriff auf ein IT-System, in diesem Fall ein kombinierter Angriff mittels einer vorweggehenden physischen Manipulation und der letztendlichen Auslösung des Angriffes durch einen IT-Angriff, ist die in Abschnitt 2.7 bereits diskutierte Explosion von Pagern und Handfunkgeräten im Libanon. Im September 2024 ereigneten sich im Libanon sowie in Damaskus mehrere tausend Explosionen

von Handfunkgeräten und Pagern, welche zur Kommunikation eingesetzt wurden. Die Handfunkgeräte und Pager wurden von der als Terrororganisation eingestuften libanesischen Partei und Miliz Hizbullah als Kommunikationsmittel aufgrund der rein unidirektionalen Kommunikation als Ersatz für gut zu trackende Mobilfunkgeräte eingeführt. Seit Jahrzehnten stehen sich der Staat Israel und die Hizbullah verfeindet gegenüber, wobei die Spannungen nach den Angriffen auf Israel im Oktober 2023 stark zunahmen. Zu den Explosionen der Pager kam es aufgrund der Remote-Auslösung der Explosionen des in den Pagern verbauten Sprengstoffs durch ein gezieltes, direkt aufeinander folgendes Triggern zweier verschiedener Auslösemechanismen. Zunächst erfolgte das Versenden einer verschlüsselten Nachricht mit spezifischem Code, der die Explosion triggerte und zu deren Empfang beide Hände zum Drücken zweier Knöpfe benötigt wurden. Kurz darauf erfolgte das Versenden einer weiteren Nachricht mit spezifischem Code, der die Pager ohne User-Interaktion zur Explosion brachte. Bei den Angriffen handelte es sich um komplexe Lieferkettenangriffe, bei denen über Jahre hinweg die Lieferketten manipuliert wurden, um die Geräte mit dem Sprengstoff zu manipulieren. Insgesamt hatten die Angriffe, bei denen es sich um kombinierte Angriffe auf digitale Kommunikationsmedien durch physische Manipulation sowie Manipulation der eingebetteten Software handelte, mindestens 42 Tote und über 3000 Verwundete zur Folge. /BBC24r01, TOI24r01, REU24r01/

Unter IT-Angriffen mit physischen Auswirkungen sind IT-Angriffe zu verstehen, die gezielt Schäden in der physischen Welt verursachen. Darunter fallen beispielsweise gezielte Beschädigungen oder Zerstörungen verfahrenstechnischer Komponenten. Beispiele für solche IT-Angriffe sind die Angriffe mit den verschiedenen Varianten der Schadsoftware Stuxnet /SYM13r01, SYM11r01/, durch die es zur Beschädigung von zahlreichen Zentrifugen zur Urananreicherung gekommen ist, als auch der Angriff auf ein deutsches Stahlwerk im Jahr 2014 /SAN14r01/, bei dem ein Hochofen beschädigt wurde.

Als weiteres Beispiel für IT-Angriffe mit physischen Auswirkungen können Ransomware-Angriffe genannt werden. Bei Ransomware handelt es sich um Schadsoftwarekomponenten, welche von IT-Angreifern zu Zwecken von Lösegelderpressung eingesetzt werden. Dabei werden die Dateien des Opfers extrahiert und verschlüsselt und anschließend wird eine Lösegeldforderung gestellt, um die Dateien wieder zu entschlüsseln und die gestohlenen, möglicherweise sensiblen Dateien nicht zu veröffentlichen. Ransomware-Angriffe sind oftmals äußerst destruktiv und enden nicht selten mit der

unwiderruflichen Zerstörung des Dateisystems der Opfer. Neben dem Diebstahl sensibler Daten können Ransomware-Angriffe auch dazu führen, dass Teile von IT-Systemen betroffener Unternehmen abgeschaltet werden müssen, um eine weitere Ausbreitung der Schadsoftware zu verhindern, oder dass die IT-Systeme selbst von der Attacke betroffen sind. Dies kann zu zum Teil erheblichen physischen Auswirkungen führen, wie z. B. Produktionsausfälle oder Beschädigungen. Im Februar 2024 kam es beispielsweise zu einem Ransomware-Angriff auf rumänische Krankenhäuser, bei dem die Ausbreitung der Schadsoftware über die Lieferkette erfolgte, da ein gemeinsamer Service-Provider für die in den Krankenhäusern eingesetzte Management-Software betroffen war. Über 100 Einrichtungen des rumänischen Gesundheitswesens, in denen die kompromittierte Software des Service-Providers genutzt wurde, waren durch den Angriff betroffen. Darunter waren 26 Krankenhäuser, in denen tatsächlich Systeme verschlüsselt wurden, und 79 weitere, vorsorglich vom Internet abgekoppelte Einrichtungen. Die Angriffe hatten den Ausfall des Gesundheitsmanagementsystems zur Folge, hatten aber auch Auswirkungen auf Untersuchungen von Patienten. Um zumindest eine eingeschränkte Patientenversorgung aufrecht erhalten zu können, wurden die Arbeiten auf Papierbasis durchgeführt. /CSO24w01, DNS24w01/

Der Einsatz von Abschaltvorrichtungen in polnischen Zügen kann als weiteres Beispiel für IT-Angriffe mit physischen Auswirkungen, in diesem Fall der Ausfall diverser Züge, gesehen werden. Im Frühjahr 2022 kam es an Zügen des Typs Impuls vom Hersteller Newag nach Wartungen zu dem Phänomen, dass sich die Züge nicht mehr starten ließen. Die vorhergehenden Wartungen wurden dabei nach Auslaufen des Wartungsvertrages nicht mehr von Newag selbst, sondern von anderen Wartungsfirmen durchgeführt. Die Auswertung der Steuerungstechnik betroffener Züge des Typs Impuls hat ergeben, dass die Software geokoordinatenbezogene Abfragen enthielt, welche sich auf polnische Wartungswerke für Züge der Größe des Typs Impuls bezog. Eine dahinter liegende Logik schaltete die Fähigkeit zur Anschaltung der Züge ab, wenn diese sich mehr als 10 Tage am Stück innerhalb dieser Koordinaten befanden. Einzige Ausnahme, bei welcher die Abschaltvorrichtung nicht aktiviert wurde, war ein Aufenthalt in einem Wartungswerk der Firma Newag. /BAD23r01, DRA23w02, ZAU23r01/

Hinsichtlich physischer Angriffe auf IT-Systeme zeigt sich, dass die Berücksichtigung der physischen Sicherheit ein integraler Bestandteil einer Cybersicherheitsstrategie sein muss. Dies erfordert eine Harmonisierung von Maßnahmen zur Cybersicherheit mit Maßnahmen zur physischen Sicherheit, um IT-Systeme effektiv vor Angriffen zu

schützen. Hinsichtlich IT-Angriffen mit physischen Auswirkungen zeigt sich, dass diese, abgesehen von Ransomware-Angriffen, die in der Regel nicht die physischen Auswirkungen als prioritäres Ziel haben, nach wie vor recht selten sind. Allerdings gewinnen sie insbesondere vor dem Hintergrund einer verschärften allgemeinen Bedrohungslage und einer erhöhten Wahrscheinlichkeit für die Sabotage kritischer Infrastruktur durch Dritte stark an Bedeutung.

3 Zusammenfassung und Fazit

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

Auch im Jahr 2024 waren Cyberangriffe auf und über die Lieferkette für die Gewährleistung der Cybersicherheit eine der größten Herausforderungen. In Anbetracht der zunehmenden Digitalisierung und Globalisierung in nahezu allen Bereichen inklusive der Lieferketten von IT-Systemen und industriellen Steuerungssystemen wird dies voraussichtlich auch auf absehbare Zeit so bleiben. Solche Supply-Chain-Angriffe haben ein hohes Gefährdungspotenzial, da sie auf die in Bezug auf Sicherungsmaßnahmen schwächeren Glieder in der Lieferkette zielen und damit letztlich die Sicherungsmaßnahmen der eigentlich anvisierten Ziele, die selbst meist besser gegen Cyberangriffe geschützt sind, umgehen. Supply-Chain-Angriffe haben daher eine Art Bypasswirkung an den Sicherungsmaßnahmen der eigentlichen Angriffsziele vorbei. Neben gezielten Supply-Chain-Angriffen auf ausgewählte Kunden kommt Angriffen auf IT-Dienstleister eine besondere Bedeutung zu. Diese weisen aufgrund des Kundenkreises derartiger Unternehmen, die aufgrund eines Angriffs auf den Dienstleister ebenfalls betroffen sind,

potenziell eine Vielzahl möglicher Opfer auf. Besonders kritisch sind IT-Angriffe über die Lieferkette dann, wenn davon weit verbreitete Software betroffen ist, die auf IT-Systemen, auf denen sie installiert ist, mit weitreichenden Rechten ausgestattet ist, wie beispielsweise Überwachungs-, Management- oder Antiviren-Software. Gleiches gilt für Cyberangriffe auf Dienstleister wie Software-as-a-Service-Anbieter oder Security Operation Centres. Typischerweise reduzieren sich die Möglichkeiten, die der Endkunde zur Detektion von schadsoftwarebehafteten Produkten hat, je früher im Entwicklungsprozess der Soft- oder Hardware die Angreifer ihre Manipulationen vorgenommen haben. Auch sind die Detektionschancen für eine vorliegende Infektion mit Schadsoftware typischerweise geringer, wenn die Schadsoftware über die Lieferkette eingebracht wurde, da so der Fußabdruck beim eigentlichen Angriffsziel kleiner bleibt. Daher sind die Erfolgsaussichten bei Supply-Chain-Angriffen auf gut geschützte Ziele meist deutlich höher als bei direkten Cyberangriffen von außen. Daher muss gerade bei Anlagen und Einrichtungen, die ein hohes Sicherungsniveau in Bezug auf die Cybersicherheit umgesetzt haben, potenziellen Supply-Chain-Angriffen besondere Aufmerksamkeit gewidmet werden. Besonders kritisch sind Cyberangriffe auf Systeme, die zur Überwachung des Netzwerkverkehrs eingesetzt werden. Eine Kompromittierung solcher Systeme ermöglicht es den Angreifern beispielsweise, weitere Angriffsschritte im Netzwerk unbemerkt auszuführen oder Überwachungsmechanismen zu manipulieren. Da solche Systeme typsicherweise Zugriff auf viele Bereiche mit entsprechenden Zugriffsrechten besitzen, können sich aus solchen Angriffen ernstzunehmende Bedrohungen entwickeln. Insgesamt ist festzustellen, dass die Angriffsoberfläche einer konkreten Anlage oder Einrichtung durch die verzweigten Lieferketten, Abhängigkeiten in Softwareprodukten und die Auslagerung von sensiblen Informationen und Diensten an externe Anbieter zum einen größer und zum anderen diffuser und für die einzelne Anlage schlechter abgrenzbar wird. Zu berücksichtigen ist auch, dass sich das Feld der Supply-Chain-Angriffe nicht auf direkte Cyberangriffe auf die Lieferketten von Softwareprodukten oder IT-Systemen beschränkt, sondern deutlich breiter ist. Beobachtete Angriffe auf Ziele innerhalb der Lieferkette von Lieferanten unterstreichen den zuvor erwähnten Aspekt der Diffusität der Angriffsoberfläche noch einmal.

Die bereits erwähnte Reduzierung der Möglichkeiten, die der Endanwender zur Detektion schadsoftwarebehafteter Produkte hat, je früher im Entwicklungsprozess die Angreifer ihre Manipulationen vorgenommen haben, zeigt sich auch bei der Thematik der Angreifbarkeit in der Softwareentwicklung. Bereits während der Softwareentwicklung vorgenommene Manipulationen führen dazu, dass diese später durch den Endanwender

nur schwer zu erkennen und zu entfernen sind. Insbesondere der Fall, dass die Manipulationen während der Softwareentwicklung vom Hersteller unbemerkt ablaufen und der Hersteller ein manipuliertes Softwareprodukt offiziell freigibt und zertifiziert, birgt erhebliche Gefahren und umgeht viele Sicherungsmaßnahmen zur Detektion der Manipulation. Für den Endanwender ist eine solche Manipulation häufig gar nicht oder nur indirekt detektierbar, z. B. wenn die Schadsoftware tatsächlich zu arbeiten beginnt. Auch der im Vergleich zu einem Angriff auf bereits entwickelte Software deutlich größere Aufwand, den Angreifer betreiben müssen, um einen Angriff in der Softwareentwicklung durchzuführen, findet aus Angreifersicht seine Rechtfertigung. Bereits in der Softwareentwicklung eingebrachte Manipulationen erreichen häufig eine sehr große Verteilung und somit viele mögliche Angriffsziele, wobei diese Angriffsziele die Manipulation nur sehr schwer detektieren können. Aber nicht nur gezielte Angriffe in der Softwareentwicklung können zu weitreichenden Auswirkungen führen. Auch zufällig im Rahmen der Softwareentwicklung eingebrachte und nicht entdeckte Fehler können erhebliche IT-Sicherheitsvorfälle hervorrufen oder von Angreifern bei deren Bekanntwerden im Rahmen von Angriffen ausgenutzt werden. Ebenfalls Einfluss auf die Angreifbarkeit von Softwareprodukten haben nicht-sicherheitsgerichtete menschliche Entscheidungen im Verlauf des Softwareentwicklungsprozesses, wie der Umgang mit noch nicht öffentlich bekannten Schwachstellen, die Vergabe von Zugriffsrechten oder das Outsourcing von Teilen der Softwareentwicklung. Insgesamt zeigt sich, dass die Berücksichtigung von Angriffsmöglichkeiten bereits während des Softwareentwicklungsprozesses immer stärkere Bedeutung gewinnt. Aufgrund der zunehmenden Komplexität der Produkte und der zunehmenden Verlagerung des Entwicklungsprozesses in die Cloud wird sich diese Situation in den kommenden Jahren vermutlich noch verschärfen.

Ein weiterer Trend der vergangenen Jahre ist der Fortschritt von Anwendungen künstlicher Intelligenz bezüglich deren Fähigkeiten und Anwendungsmöglichkeiten. Es wurden neuere und leistungsfähigere KI-Modelle veröffentlicht, wobei sich dieser Trend in den kommenden Jahren vermutlich weiter verstärken wird. Die wachsenden Fähigkeiten und Funktionen von KI-Modellen können auch für Cyberangriffe genutzt werden. Ein Anwendungsbereich von KI im Rahmen von Cyberangriffen betrifft das Social Engineering. Durch die KI-basierte Generierung von täuschend echt wirkenden Dokumenten, synthetischen Stimmen oder Videos kann die Glaubhaftigkeit hochspezifizierter Social Engineering Angriffe massiv gesteigert werden. Auf Basis kurzer Sprachproben und einzelner Fotos ist es mittlerweile möglich, nahezu täuschend echte Teilnehmer an Videotelefonaten KI-basiert zu erzeugen. Es ist zu erwarten, dass der Einsatz von KI es künftig noch

leichter machen wird, relevante Personen zu unwissentlichen Innentätern bei einem Cyberangriff zu machen, da Social Engineering ausgefeilter und stärker auf einzelne Personen zugeschnitten wird und gleichzeitig Täuschungen schwerer zu erkennen sind. Ein weiteres Einsatzgebiet von künstlicher Intelligenz im Rahmen von Cyberangriffen ist die Möglichkeit, KI-Modelle zu nutzen, um große Datenmengen, die im Rahmen eines Angriffs gestohlen wurden, in kürzester Zeit nach spezifischen Informationen zu durchsuchen. Zudem können KI-Modelle direkt zur Entwicklung von Schadsoftware eingesetzt werden. Bereits heute sind diese in der Lage, Code mit begrenztem Funktionsumfang zu erzeugen. Diese Fähigkeit wird sich sicherlich in den kommenden Jahren weiter verbessern, was dazu genutzt werden kann, effizienter nach Schwachstellen zu suchen oder Exploits für diese Schwachstellen zu entwickeln. Außerdem ist zu erwähnen, dass der Einsatz von künstlicher Intelligenz dazu führen kann, dass auch Gruppierungen, die mit weniger Ressourcen und weniger Fähigkeiten ausgestattet sind als APT-Gruppierungen, in der Lage sein werden, hochkomplexe Angriffe unter Ausnutzung komplexer Schadsoftware auszuführen. Somit wird der Einsatz von KI es solchen Gruppierungen erheblich erleichtern, Angriffe durchzuführen, was zu einer höheren Anzahl potenzieller Angreifer führen wird.

Kryptografische Verfahren zum Schutz sensibler Daten vor unbefugten Zugriffen und Manipulationen sind ebenfalls Ziel von Cyberangreifern. Dabei sind insbesondere Schwachstellen in der Programmierung und Etablierung von Verschlüsselungen im Fokus der Angreifer. Aber auch die geheimen Schlüssel sind beliebte Angriffsziele, da Angreifer durch diese direkt in der Lage sind, die verschlüsselten Daten zu entschlüsseln. Schwachstellen bei der Verschlüsselung basieren einerseits auf Schwachstellen in der Erzeugung und Verbreitung von Schlüsseln, andererseits in der Programmierung der Programme zur Verschlüsselung. Angriffe auf Schwachstellen in der Erzeugung von Schlüsseln zielen beispielsweise darauf ab, dass der Erzeugungsalgorithmus keine ausreichende Zufälligkeit erreicht und damit vorhersehbar ist. Schwachstellen in den Programmen zur Verschlüsselung ermöglichen es Angreifern z. B. trotz Verschlüsselung Daten unverschlüsselt auszulesen. Eine weitere Gefahr bildet der potenzielle Einsatz von Quantencomputern zum Knacken von Verschlüsselungen. Es wird angenommen, dass herkömmliche Verschlüsselungen mit dem Aufkommen leistungsfähiger Quantencomputer, mit dem in den kommenden Jahren gerechnet wird, innerhalb kürzester Zeit zu entschlüsseln sind. Daher werden bereits heute neue Verschlüsselungsalgorithmen entwickelt, die quantensicher sind. Aufgrund der enormen Verbreitung der meisten Verschlüsselungsalgorithmen kann das Bekanntwerden einer einzelnen Schwachstelle

erhebliche Auswirkungen haben. Daher sind kryptografische Verfahren von erheblichem Interesse für Angreifer und bekanntgewordene Schwachstellen führen zu spürbaren Auswirkungen für die Anwender von Verschlüsselungen.

Aufgrund des vermehrten Einsatzes von IT-Systemen in modernen Fahrzeugen, die diverse, untereinander vernetzte Sensoren wie Ultraschall, Kamera, Radar oder Lidar nutzen, sind auch Fahrzeuge ein Ziel von Cyberangreifern. Ein Angriff auf den sogenannten CAN-Bus (Controller Area Network), der als Standard-Bus-System zur Datenübertragung zwischen den verschiedenen Komponenten im Fahrzeug genutzt wird, wird dabei als besonders schwerwiegend angesehen. Durch einen solchen Angriff kann auf das interne Netzwerk des Fahrzeugs zugegriffen werden, womit Manipulationen wichtiger Komponenten wie Motor, Getriebe, Sensoren und sonstigen elektronisch kontrollieren Teilen möglich sind. Auch Angriffe aus der Ferne, bei dem über einen Remote Access auf das interne Fahrzeug-Netzwerk eine Kommunikation mit dem CAN-Bus hergestellt wurde und physikalische Systeme des Fahrzeugs wie Lenkrad, Motor, Getriebe und Bremsen manipuliert wurden, sind bereits durchgeführt worden. Ein weiteres System, was Cyberangriffen bereits zum Opfer gefallen ist, ist das Keyless-System zur Ermöglichung der Ent- bzw. Verriegelung der Türen ohne aktive Nutzung eines Schlüssels. Dabei wurden die vom System versendeten Funksignale von den Angreifern mitgehört und die Signale anschließend zum Diebstahl des Fahrzeugs verwendet. Cyberangriffe auf Fahrzeuge sind von besonderer Bedeutung, da sie den Straßenverkehr gefährden und potenziell lebensgefährlich für Verkehrsteilnehmer sein können. Aufgrund der Vielzahl von IT-Systemen sind die Netzwerkarchitekturen der Fahrzeuge deutlich komplexer geworden, was neben der Etablierung drahtloser Kommunikation die Angriffsoberfläche auf Fahrzeuge in den letzten Jahren deutlich erhöht hat.

In Bezug auf Cyberangriffe auf den Energiesektor ist festzuhalten, dass die eigentlichen Angriffszwecke und vermutlich auch die Motivation der Angreifer sehr breit gefächert sind. Zum einen gibt es immer wieder Cyberangriffe, die auf direkte physische Auswirkungen abzielen, beispielsweise auf die Hervorrufung von Stromausfällen. Zudem gibt es eine große Anzahl an Angriffen, bei denen Informationsdiebstahl und Spionage im Vordergrund stehen. Ebenfalls beobachtet werden Cyberangriffe, die eher vorbereitenden Charakter für spätere Angriffsschritte oder den Zweck einer geeigneten Positionierung für spätere Angriffe zu haben scheinen. Zusätzlich zu diesen eher strategisch, politisch oder ideologisch motivierten Cyberangriffen gibt es aber auch Cyberangriffe mit deutlich finanzieller Motivation, wobei Erpressung und der Handel mit gestohlenen Daten

im Vordergrund stehen. Eine Problematik, die in den vergangenen Monaten und Jahren wiederkehrend zutage getreten ist, ist der Einsatz alter Kommunikationsprotokolle. Diese Protokolle wurden in einer Zeit entwickelt, in welcher der Fokus ausschließlich auf der Bereitstellung von Funktionalitäten lag und zu der die Berücksichtigung von Aspekten der Cybersicherheit noch nicht üblich war. Erfolgreiche Angriffe auf die elektrische Energieversorgung sind generell mit deutlichen Auswirkungen verbunden. Die Verursachung physischer Schäden hat hierbei häufig weitreichende Folgen wie beispielsweise flächendeckende Stromausfälle und dadurch Kollateralschäden in von der elektrischen Energieversorgung abhängigen Bereichen. Dies gilt insbesondere für Angriffe, die zu länger andauernden Stromausfällen führen.

Geopolitische Spannungsfelder begünstigen traditionell die Entwicklung defensiver und offensiver Fähigkeiten und den Aufbau entsprechender Ressourcen. Hierbei stellen Cyberangriffe keine Ausnahme dar. Gerade in Zusammenhang mit dem russischen Angriffskrieg in der Ukraine ist es in den vergangenen Jahren zu zahlreichen Cyberangriffen gekommen. Bereits vor Beginn der Kampfhandlungen war hier eine deutliche Zunahme an Cyberangriffen zu verzeichnen. Seit Beginn der Kampfhandlungen wurde darüber hinaus ein weiterer Anstieg bei den bekannt gewordenen Cyberangriffen festgestellt. Hierzu zählen Cyberangriffe auf kritische Infrastrukturen und Kommunikationskanäle, aber insbesondere auch strategisch und politisch motivierte Cyberangriffe, die nicht nur Russland und die Ukraine, sondern darüber hinaus beispielsweise auch die NATO Partner und weitere Staaten, die eine offizielle Form der Unterstützung für die Ukraine signalisiert haben, betreffen. Ähnliches gilt für die meisten geopolitischen Spannungsfelder. Cyberangriffe kommen heutzutage in praktisch allen geopolitischen Spannungsfeldern zum Einsatz. Dies schließt Cyberangriffe verschiedenster Komplexität von einfachen disruptiven Angriffen bis hin zu hochausgereifter Schadsoftware und langandauernden Angriffskampagnen ein. Hierbei stehen meist strategische Motive, Spionage, politische Meinungsäußerung und psychologische Effekte wie Destabilisierung und Demoralisierung im Vordergrund. Insgesamt wird deutlich, dass eine Abgrenzung geopolitischer Spannungsfelder nur oberflächlich möglich ist. Auf einer tiefer liegenden Ebene sind konkrete Spannungsfelder zwischen einzelnen Staaten meist nur Ausprägungen von deutlich breiter gefächerten Spannungsfeldern, an denen typischerweise nicht nur zwei Staaten beteiligt sind. Dies schlägt sich auch in den entsprechenden Cyberangriffen nieder.

Die letzten Jahre haben gezeigt, dass IT-Systeme nicht nur durch Cyberangriffe, sondern auch durch physische Angriffe in Mitleidenschaft gezogen werden können. Dabei

werden gezielte physische Attacken auf IT-Systeme durchgeführt mit dem Ziel, diese zu beschädigen oder zu zerstören. Daher reicht insbesondere für kritische Infrastrukturen der Blick auf die Cybersicherheit allein nicht aus, sondern auch die physische Sicherheit muss ein essentieller Bestandteil der Schutzmaßnahmen sein, um IT-Systeme gegen die wachsende Bedrohungslage zu schützen. Ohne die Einrichtung effektiver physischer Schutzmaßnahmen kann kein Schutz gegen Angreifer mit direktem physischem Zugang aufgebaut werden. Einen anderen Blickwinkel liefert die Betrachtung von IT-Angriffen mit physischen Auswirkungen. Darunter sind IT-Angriffe zu verstehen, die gezielt Schäden in der physischen Welt verursachen. IT-Angriffe mit gezielten physischen Auswirkungen sind zwar noch relativ selten, gewinnen aber insbesondere vor dem Hintergrund der verschärften allgemeinen Bedrohungslage und der erhöhten Wahrscheinlichkeit von Sabotage zunehmend an Bedeutung. Dies zeigen beispielsweise diverse, mutmaßlich gezielt herbeigeführte Beschädigungen von Unterseekabeln.

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

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

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

Sowohl aus dem Blickwinkel der IT-Bedrohungslage als auch ausgehend von der individuell vorhandenen Angriffsoberfläche zählen prinzipiell auch alle deutschen kerntechnischen Anlagen und Einrichtungen zu potenziellen Angriffszielen für Cyberangriffe. Grundsätzlich bietet die korrekte und vollständige Umsetzung der SEWD Richtlinie IT /BMU13n03/ aus Sicht der GRS weitreichenden Schutz vor den Gefahren von Cyberangriffen. Aus Sicht der GRS ist zunächst davon auszugehen, dass in Anlagen, die ihre IT-Systeme konsequent gemäß SEWD Richtlinie IT schützen, die Hürden für die Kompromittierung eines sicherheitstechnisch relevanten Systems deutlich höher sind als in vielen anderen kritischen Infrastrukturen. Insgesamt ist allerdings zu beachten, dass auch die korrekte und vollständige Umsetzung der SEWD Richtlinie IT – oder eines beliebigen anderen Regelwerks zur Cybersicherheit – zwar einen weitreichenden, aber keinen vollumfänglichen Schutz vor den Gefahren eines langfristig angelegten Cyberangriffs durch eine Angreifer-Gruppierung mit den entsprechenden zeitlichen, finanziellen und personellen Ressourcen bieten kann. Die hier beschriebenen IT-Sicherheitsvorfälle und weiteren Aktivitäten der Angreifer verdeutlichen, dass Strategien zur frühzeitigen Detektion solcher Cyberangriffe und angemessene Maßnahmen zur Reaktion auf entsprechende IT-Sicherheitsvorfälle in diesem Zusammenhang von zentraler Bedeutung für die Sicherheit und Sicherung deutscher kerntechnischer Anlagen sind. Dies wird noch

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

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

Abkürzungsverzeichnis

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

Abbildungsverzeichnis

Quellen

/ABC23w01/ ABC News, Tran, D., Russian hackers claim responsibility for theft of data from Australian bond broker FIIG, 12.06.2023, https://www.abc.net.au/, [abgerufen am 19.09.2023]

/ADE23w01/ adesso, "Aktuelle Informationen zum Cyber-Angriff auf adesso", 26.04.2023, www.adesso.de [abgerufen am 13.10.2023]

/AGE24w01/ Agenzianova, Medienberichten zufolge beschaedigten die Huthi vier Unterwasserkabel im Roten Meer, 26. Februar 2024, https://www.agenzianova.com/de/news/, [abgerufen am 24.09.2024]

/AGE24w02/ Agenzianova, Rotes Meer: Die Houthis bestreiten Schaeden an drei Unterseekabeln, 27. Februar 2024, https://www.agenzianova.com/de/news/, [abgerufen am 24.09.2024]

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

/BAD23r01/ BadCyber: Dieselgate, but for trains - some heavyweight hardware hacking, December 2023

/BBC24r01/ The BBC: What we know about the Hezbollah device explosions, by Matt Murphy and Joe Tidy, 21.09.2024

/BIT23w01/ Bitedefender, Killnet: Hacker greifen europaeische Krankenhaeuser an, 17.02.2023, https://www.bitdefender.de/, [abgerufen am 18.09.2023]

/BIT23w02/ Bitdefender, Vlad Constantinescu, Russian Cyber Group APT28 Targets Ukraine Government with Fake Windows Update Emails, 03. Mai 2023, https://www.bitdefender.com, [abgerufen am 07.05.2024]

/BLE22w02/ Bleeping Computer, New Black Basta ransomware springs into action with a dozen breaches, 27. April 2022, www.bleepingcomputer.com [abgerufen am 28.06.2022]

/BLE22w04/ Bleeping Computer, Wind turbine firm Nordex hit by Conti ransomware attack, 14. April 2022, www.bleepingcomputer.com [abgerufen am 29.06.2022]

/BLE22w09/ Bleeping Computer, Toulas, B., Russian hackers perform reconnaissance against Austria, Estonia, 23.05.2022, https://www.bleepingcomputer.com/, [abgerufen am 27.11.2023]

/BLO23w01/ Blockzeit, Munene, V., Ein Hackerkollektiv unter der Fuehrung von Killnet greift das SWIFT-Netzwerk innerhalb der naechsten 48 Stunden an, 16.06.2023, https://blockzeit.com/, [abgerufen am 07.09.2023]

/BMD24r01/ Bundesministerium für Verkehr, Neue Fahrzeugsicherheitssysteme, https://www.bmv.de/SharedDocs/DE/Artikel/StV/Strassenverkehr/neue-fahrzeugsicherheitssysteme.html, 2024

/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

/BTB23w01/ B2B Cyber Security News, Alphv veroeffentlicht Daten von Ziegler, 25.04.2023, https://b2b-cyber-security.de/alphv-veroeffentlicht-daten-von-ziegler-feuerwehrfahrzeuge/ [abgerufen am 28.09.2023]

/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]

/CHA15r01/ Dr. Charlie Miller, Chris Valasek, Remote Exploitation of an Unaltered Passenger Vehicle, 2015

/CHE11j01/ Stephen Checkoway et al., Comprehensive Experimental Analyses of Automotive Attack Surfaces, 2011

/CNN24w01/ CNN Buisness by Juliana Liu and Hassan Tayir: China claims it has cracked Apple AirDrop's encryption to identify senders

/CIO21w01/ CIO, Großer Hacker-Angriff trifft hunderte Unternehmen, 04.07.2021, https://www.cio.de/ [abgerufen am 20.05.2022]

/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]

/CIS22r05/ CISCO TALOS: Lazarus and the tale of three RATs, by Asheer Malhotra, Vitor Ventura and Jungsoo An, 08. September 2023

/CLO23r01/ CloudSEK: Compromising Google Accounts:Malwares Exploiting Undocumented OAuth2 Functionality for session hijacking, December 2023

/COM23w01/ Computer Weekly, Russian DDoS hacktivist seen targeting western hospitals, 31.01.2023, https://www.computerweekly.com/, [abgerufen am 07.09.2023]

/CPO23w01/ CPO Magazine, Hope, A., Russian Hackers Killnet Executed a Cyber Attack on European Air TRaffic Control Agency Eurocontrol, 01.05.2023, https://www.cpomagazine.com/, [abgerufen am 07.09.2023]

/CRO24w01/ Crowwdstrike Blog, "Technical Details: Falcon Content Update for Windows Hosts", 20.07.2024, www.crowdstrike.com [abgerufen am 20.08.2024]

/CSD22w01/ CyberSecurity Dive: Energy providers hit by North Korea-linked Lazarus exploiting Log4j VMware vulnerabilities, Matt Kapko, 13. September 2022

/CSO22w03/ CSO, Energieversorger ignoriert Erpresser, 24.08.2022, https://www.csoonline.com/de/a/energieversorger-ignoriert-erpresser,3674116 [abgerufen am 25.09.2023]

/CSO24w01/ CSO, Hackerangriff legt 21 rumaenische Krankenhaeuser lahm, 13.02.2024, https://www.csoonline.com/ [abgerufen am 16.05.2024]

/CYH23w01/ Cybersecurity Help, Gamaredon cyber spies use new PowerShell script to drop backdoors, 15 June 2023, https://www.cybersecurity-help.cz/blog/3347.html, [abgerufen am 01.10.2024]

/DAI23w03/ Daily Finland, Russian cyber-attacks against Finland become more frequent, 22.04.2023, https://www.dailyfinland.fi/, [abgerufen am 19.09.2023]

/DNS24w01/ DNSC, UPDATE: Un atac cibernetic de tip ransomware a afectat spitale din Romania, 16.02.2024, https://dnsc.ro/ [abgerufen am 16.05.2024]

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

/DRA23w02/ Dragon Sector Webseite [abgerufen am 22.12.2023]

/ECT21w01/ The Economic Times, Is the Mumbai blackout last year connected to the Ladakh standoff?, 2. März 2021, https://economictimes.indiatimes.com, [abgerufen am 18.08.2022]

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

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

/ESE22w01/ ESET, Industroyer2: Industroyer reloaded, 12.04.2022, https://www.welivesecurity.com, [abgerufen am 04.05.2022]

/EUR23w01/ Euractiv, Dias, J., Portuguese company detects 961 pro-Russian cyber attacks in Western Europe, 22.09.2023, https://www.euractiv.com/, [abgerufen am 19.10.2023]

/EUR23w02/ Euractiv, Szumski, C., Cyberattacks target Icelandic official websites, tech companies, 14.06.2023, https://www.euractiv.com/. [abgerufen am 19.09.2023]

/EXP23w01/ Expats cz, More Russian attacks on Czech banks: Hackers call for end of support to Ukraine, 31.08.2023, https://www.expats.cz/, [abgerufen am 19.09.2023]

/FBI22l02/ Federal Bureau of Investigation, FBI Flash, BlackCat/ALPHV Ransomware Indicators of Compromise, 19. April 2022

/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]

/FOC23w01/ Focus online, Zwei Maenner nach Angriff auf Kommunikationsnetz der polnischen Bahn festgenommen, 27.08.2023, https://www.focus.de/, [abgerufen am 29.08.2023]

/FOC24w01/ Focus, Betroffene Länder gehen nach Kabelschäden in Ostsee von Sabotage aus, 20.11.2024

/FOR20w02/ FOR20w02Forbes, Peter Cohan, Pulse Secure Challenges Citrix In $7 Billion Secure Remote Access Market, June 2020

/FOR23w01/ Foreign Policy, Oghanna, A., How Albania Became a Target for Cyberattacks, 25.03.2023, https://foreignpolicy.com/, [abgerufen am 19.09.2023]

/FRE24r01/ Andres Freund, Backdoor in upstream xz/liblzma leading to ssh server compromise, Mail to oss-security at openwall, 29.3.2024, https://www.openwall.com/lists/oss-security/2024/03/29/4 [abgerufen am 14.05.2024]

/GOL22w01/ Golem.de, Satelliteninternet KA-SAT ausgefallen, 27.02.2022, https://www.golem.de [abgerufen am 01.03.2022]

/GOL23w02/ Golem, Stoeckel, M., Russische Hackergruppe waechst in 9 Monaten um Faktor 25, 01.07.2023, htpps://www.golem.de/, [abgerufen am 07.09.2023]

/GUR24i01/ Ukrainischer Militaernachrichtendienst GUR, Software, Ciphers, Secret Documents - DUI Cyber Specialists Hacked Russia's Defence Ministry, 04.03.2024, https://gur.gov.ua/en/content/, [abgerufen am 23.09.2024]

/HAN23w01/ Handelsblatt, Mueller, M. et al., Prorussische Hacker drohen mit Vergeltung fuer Leopard-Entscheidung, 25.01.2023, https://www.handelsblatt.com/, [abgerufen am 29.08.2023]

/HAN24w01/ Handelsblatt, Philipp Alvares de Souza Soares, Seekabel im Roten Meer durchtrennt - Bedrohung fuer das Internet in Europa waechst, 07.03.2024, https://www.handelsblatt.com/technik/it-internet/, [abgerufen am 24.09.2024]

/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]

/HEI21w06/ Heise online, Hacker-Angriff über IT-Dienstleister Kaseya trifft Hunderte Unternehmen, 05.07.2021, https://www.heise.de/ [abgerufen am 20.05.202]

/HEI22w08/ Heise Online, DDoS-Attacke: Israelische Regierungswebseiten vorübergehend nicht erreichbar, 15. März 2022, https://www.heise.de [abgerufen am 25.03.2022]

/HEI23w01/ Heise Online, Dennis Schirrmacher, Sicherheitsluecke in Moxa MXsecurity Series gefaehrdet kritische Infrastrukturen, 29.05.2023, https://www.heise.de/news/ [ab-gerufen am 03.07.2023]

/HEI24w04/ Heise online, Russland spaeht ukrainische Abwehr mit Webcams aus, Dirk Knop, 05.01.2024, https://www.heise.de/news/ [abgerufen am 18.01.2024]

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

/INF23w01/ Infosecurity Magazine, Alessandro Mascellino, Russia-affiliated Shuckworm Intensifies Cyber-Attacks on Ukraine, 16 June 2023, https://www.infosecurity-magazine.com/news/, [abgerufen am 29.08.2023]

/INF24r01/ Infosecurity Magazine: Russian Sandworm Group Hit 20 Ukrainian Energy and Water Sites, April 2024

/INM24w01/ Infosecurity Magazine, Russia Spies on Kyiv Defenses via Hacked Cameras Before Missile Strikes, James Coker, 03.01.2024, https://www.infosecurity-magazine.com [abgerufen am 17.07.2024]

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

/ITD21w01/ IT-daily.net, Vestas: Hacker haben personenbezogene Daten abgerufen, 09. Dezember 2021, https://www.it-daily.net/, [abgerufen am 25.08.2022]

/KAS24t01/ Securelist by Kaspersky, XZ backdoor story Initial analysis, 12 April 2024, https://securelist.com/xz-backdoor-story-part-1/112354/ [abgerufen am 14.05.2024]

/KOC18r01/ Kocher, P. et al., Spectre Attacks: Exploiting Speculative Execution, /KOS10j01/Karl Koscher et al., Experimental Security Analysis of a Modern Automobile, 2010

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

/LRT23w01/ Lithuanian National Radio and Television (LRT), Hackers stream anti-NATO broadcasts in Lithuania after cyber attacks, 10.07.2023, https://www.lrt.lt/, [abgerufen am 19.10.2023]

/LUX23w01/ Luxembourg Times, Lambert, Y., Hackers take down Luxembourg City council website, 19.09.2023, https://www.luxtimes.lu/, [abgerufen am 19.09.2023]

/MAL22w02/ Malwarebytes Labs, DDoS barrage against Israel described as the largest ever cyberattack its faced, 15. März 2022, https://blog.malwarebytes.com [abgerufen am 04.07.2022]

/MAN23r03/ Mandiant: Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology, November 2023

/MIC22w01/ Mircosoft, Smith, B., Defending Ukraine: Early Lessons from the Cyber War, 22.06.2022, https://www.microsoft.com/, [abgerufen am 19.10.2023]

/MIC23r02/ Microsoft Security Response Center: Results of Major Technical Investigations for STORM-0558 Key Acquistion, September 2023

/MIC24w01/ Microsoft, Weston, D., "Helping our customers through the CrowdStrike outage", 20.07.2024, www.blogs.microsoft.com [abgerufen am 20.08.2024]

/MIM23w01/ Michalis Michalos, An OSINT analysis of the Greek school exams site DDoS attack, 05.06.2023, https://www.michalos.net/, [abgerufen am 28.11.2023]

/NAT23w01/ NATO News, NATO team in North Macedonia to help against hybrid attacks, 07.03.2023, https://www.nato.int/, [abgerufen am 19.10.2023]

/NCS24r01/ National Cyber Security Centre: The near-term impact of AI on the cyber threat, January 2024

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

/NIS14n01/ National Vulnerability Database: CVE-2014-0160

/NIS17n02/ National Vulnerability Database: CVE-2017-15361

/NOR22w01/ Nordex, Nordex Group impacted by cyber security incident, https://www.nordex-online.com [abgerufen am 29.06.2022]

/NVD23i06/ National Vulnerabilty Database NVD, CVE-2023-2868 Detail, 24.05.2023, https://nvd.nist.gov/vuln/detail/CVE-2023-2868 [abgerufen am 19.10.2023]

/OKT22w01/ Okta, Bradbury, D., Updated Okta Statement on LAPSUS$, 22.03.2022, https://www.okta.com/ [abgerufen am 03.11.2022]

/OKT22w02/ Okta, Bradbury, D., Okta Concludes its Investigation Into the January 2022 Compromise, 19.04.2022, https://www.okta.com/ [abgerufen am 03.11.2022]

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

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

/REC23w01/ The Record, Antoniuk, D., Pro-Russian hackers claim attacks on French, Dutch websites, 09.08.2023, https://therecord.media/, [abgerufen am 31.08.2023]

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

/REU23w02/ Reuters, Denmark raises cyber risk alert level after Russian attacks, 31.01.2023, https://www.reuters.com/, [abgerufen am 19.09.2023]

/REU23w03/ Reuters, Russia-aligned hackers pose threat to Canada energy sector, spy agency says, 21.06.2023, https://www.reuters.com/, [abgerufen am 19.09.2023]

/REU24r01/ Reuters: Batteries of Lebanon walkie-talkies contained PETN explosive - Lebanese source, 20.09.2024

/RHP22w01/ Rheinische Post, Hacker erlangt offenbar Zugriff auf FBI-Datenbank, 15.12.2022, https://rp-online.de/panorama/ausland/fbi-datenbank-offenbar-von-hacker-geknackt_aid-81515043 [abgerufen am 18.09.2023]

/RSC24r01/ Russ Cox: Timeline of the xz open source attack, 03.04.2024

/SAK23w01/ Sekoia, Amaury, G. et al., Following NoName057(16) DDoSia Project's Targets, 29.06.2023, https://blog.sekoia.io/, [abgerufen am 21.09.2023]

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

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

/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]

/SEC22w02/ Security Week, Germany: 2 Oil Storage and Supply Firms Hit by Cyberattack, 01. Februar 2022, https://www.securityweek.com [abgerufen am 02.02.2022]

/SEC22w04/ Security Week, Conti Ransomware Gang Claims Cyberattack on Wind Tur-bine Giant Nordex, 15. April 2022, https://www.securityweek.com [abgerufen am 29.06.2022]

/SEC22w14/ SecNews, DESFA-Cyberangriff: Ransomware-Angriff oder Datenabfangen?, 20.08.2022, https://de.secnews.gr/415743/desfa-kivernoepithesi-ransomware-ipoklopi-dedomenon/ [abgerufen am 25.09.2023]

/SEC22w15/ Security Week, Ransomware Gang Leaks Data Allegedly Stolen From Greek Gas Supplier, 23.08.2022, https://www.securityweek.com/ransomware-gang-leaks-data-allegedly-stolen-greek-gas-supplier/ [abgerufen am 25.09.2023]

/SEC23r01/ Secureworks, Counter Threat Unit (CTU): Threat Intelligence Executive Report, Volume 2023, Number 3, 2023

/SEC23w07/ Security Affairs, Pierluigi Paganini, Russia-Linked APT28 Uses Fake Windows Update Instructions to Target Ukraine Govt Bodies, 30. April 2023, https://securityaffairs.com/145500/apt/spear-phishing-campaign-apt28.html, [abgerufen am 07.05.2024]

/SEC23w09/ Security Affairs, Pierluigi Paganini, Russia-linked APT Gamaredon update TTPs in recent attacks against Ukraine, June 15, 2023, https://securityaffairs.com/147497/apt/, [abgerufen am 01.10.2024]

/SEC23w10/ Security Affairs, Pierluigi Paganini ,Russian APT BlueBravo targets diplomatic entities with GraphicalProton backdoor, 23.07.2023 [abgerufen am 19.01.2026]

/SEC24w05/ Securityonline, Son, D., "CVE-2024-0692: SolarWinds Security Event Ma-nager Unauthenticated RCE Flaw", 01.03.2024, www.securityonline.info [abgerufen am 04.11.2024]

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

/SPI23w01/ Der Spiegel, Zahl der Cyberangriffe auf Verbuendete der Ukraine steigt, 29.03.2023, https://www.spiegel.de/, [abgerufen am 31.08.2023]

/SSU24w01/ Security Service of Ukraine (SSU), SSU blocks webcams that exposed air defence operation during russian missile attack on Kyiv on 2 January (video), 02.01.2024, https://ssu.gov.ua/en/novyny [abgerufen am 17.07.2024]

/SWI23w01/ Swissinfo, Political motives behind cyberattacks on Swiss government websites, 02.11.2023, https://www.swissinfo.ch/, [abgerufen am 27.11.2023]

/SYM11r01/ Symantec, Security Response, W32.Stuxnet Dossier, Version 1.4, February 2011

/SYM13r01/ Symantec, Security Response, Stuxnet 0.5: The missing link, Version 1.0, 26 February 2013

/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]

/SYM22r01/ Symantec by Broadcom Threat Intelligence: Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets, 27. April 2023

/SYS22w01/ Sysdig, Killnet cyber attacks against Italy and NATO countries, Alessandro Brucato, 18.05.2022 [abgerufen am 19.01.2026]

/TAG23w01/ Tagesschau, Cybermafia von Putins Gnaden?, 06.04.2023, https://www.tagesschau.de/, [abgerufen am 29.08.2023]

/TAS23w01/ The Asahi Shimbun, Nagoya Port cyberattack may become security wake-up call, 12.06.2023, https://www.asahi.com/, [abgerufen am 19.09.2023]

/TEC24r01/ TechMonitor: Implementation vulnerabilities reported for post-quantum encyrption algorithm, January 2024

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

/THN23w01/ The Hacker News, Lakshmanan, R., DDoSia attack tool with encryption, targeting multiple sectors, 04.07.2023, https://thehackernews.com/, [abgerufen am 21.09.2023]

/TIN23w02/ Dr. Ken Tindell, CAN Injection: keyless car theft, 2023

/TOI24r01/ The Times of Israel: Hezbollah was still distributing pagers hours before Tuesday blast, 20.09.2024

/TUD21r01/ Technische Universität Darmstadt: Apple AirDrop teilt nicht nur Daten

/UKR23w01/ Ukrainska Pravda, Russian hackers attack website of Bulgarian Parliament for assisting Ukraine, 16.07.2023, https://www.pravda.com.ua/, [abgerufen am 19.09.2023]

/UKR23w02/ Ukrainska Pravda, Russian hackers attack Slovak governmental websites after country supplies Mig-29s to Ukraine, 28.03.2023, https://www.pravda.com.ua/, [abgerufen am 19.09.2023]

/VAR21w01/ Varonis, Nemelka, K., REvil-Ransomware-Angriff auf Kaseya VSA: Was Sie wissen sollten, 16.07.2021, https://www.varonis.com/ [abgerufen am 03.11.2022]

/WIN23w01/ WinFuture, Kahle, C., Angriff auf Ukraine-Nachschub? - Funksignal bringt 20 Zuege zum Stehen, 28.08.2023, https://www.winfuture.de/, [abgerufen am 29.08.2023]

/WIR23w01/ Wired, Greenberg, A., The cheap radiohack that disrupted Poland's railway system, 27.08.2023, https://www.wired.com/, [abgerufen am 30.08.2023]

/ZAU23r01/ Zaufana Trzecia Strona: O trzech takich, co zhakowali prawdziwy pociag a nawet 30 pociagow (deutsch: Ueber drei, die einen echten Zug gehackt haben oder sogar 30 Zuege), December 2023

/ZDF23w02/ ZDF heute, Grossangelegter Hacker-Angriff auf Deutschland, 26.01.2023, https://www.zdf.de/, [abgerufen am 29.08.2023]

/ZYX23w01/ Zyxel security advisory for OS command injection vulnerability of firewalls, CVE-2023-28771, 2023

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-911727-43-3