IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand September 2022

GRS - 718

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen

Stand September 2022

Robert Arians
Christian Korn
Claudia Quester
Oliver Rest
Alexander Schug

November 2022

Anmerkung:

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

GRS - 718
ISBN 978-3-910548-09-1

Deskriptoren

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

Kurzfassung

Die IT-Bedrohungslage in Bezug auf kritische Infrastrukturen und industrielle Steuerungssysteme wird von der GRS kontinuierlich verfolgt, ausgewertet und in einem jährlichen Bericht dargestellt. Für das Jahr 2022 wurden insgesamt elf Themenschwerpunkte identifiziert. Diese gehen zum einen auf vielfach aufgetretene Arten von IT-Angriffen wie beispielsweise Ransomware-Angriffe und Supply-Chain-Angriffe sowie signifikante Schwachstellen beispielsweise in Komponenten zur datentechnischen Kommunikation ein. Zum anderen liegt der Fokus auf IT-Angriffen, die auf die Manipulation von industriellen Steuerungssystemen abzielen, physische Schäden hervorrufen oder auf den Energiesektor oder insbesondere kerntechnische Anlagen abzielen. Darüber hinaus werden Auswirkungen der Covid-19-Pandemie auf die IT-Sicherheit sowie IT-Angriffe in Zusammenhang mit dem Krieg in der Ukraine thematisiert. Einen weiteren Schwerpunkt bilden Kollateralschäden. Der Bericht beschäftigt sich zudem mit Advanced Persistent Threats. Dies umfasst sowohl einen Schwerpunkt zur Thematik „APT for hire“ als auch Abschnitte über einzelne, für den Energiesektor relevante APT-Gruppierungen. Die Anhänge stellen Informationen zu relevanten Schwachstellen, IT-Angriffswerkzeugen, IT-Sicherheitsvorfällen und IT-Angriffen bereit. Da es sich dabei um wachsende, lebende Anhänge handelt, umfassen sie im Gegensatz zum Hauptteil des Berichtes einen deutlich längeren Betrachtungszeitraum als nur das Jahr 2022.

Abstract

GRS continuously screens and analyses the cyber threat landscape, focusing on industrial control systems and critical infrastructures. This summary report for 2022 comprises eleven main topics including ransomware and supply chain attacks as well as vulnerabilities in communication components. Other main topics cover attacks aiming at ICS manipulation, entailing physical damage or targeting the energy or nuclear sector. Both, impacts of the Covid-19 pandemic on cyber security and cyberattacks connected to the war in Ukraine, are considered as well. Emphasis is also placed on collateral damage. Moreover, this report includes an overview concerning relevant advanced persistent threats, starting with APT for hire and then focusing on APTs active in the energy and nuclear sectors. The appendices summarize relevant vulnerabilities, cyber-attack tools, incidents and cyberattacks. As living appendices, they cover a much longer period than 2022 alone.

Inhaltsverzeichnis

1 Einleitung

Im Bereich der Informationstechnik führen kurze Produktentwicklungszyklen und eine immer höhere Leistungsfähigkeit zu schnellen technischen Veränderungen, welche schließlich aufgrund ihrer Potenziale und Verdrängungsprozesse auch in kerntechnischen Bereichen Einzug erhalten. Hierdurch wurden und werden viele ursprünglich festverdrahtet ausgeführte leittechnische Einrichtungen, Systeme und Komponenten in kerntechnischen Anlagen durch programmierbare oder rechnerbasierte Einrichtungen ersetzt. Darüber hinaus ist auch im Entwicklungs- und Herstellungsprozess sowie bei der Wartung dieser industriellen Steuerungssysteme ein immer stärkerer Einsatz von rechnerbasierten und programmierbaren Werkzeugen festzustellen. Diese Veränderungen führen zu immer neuen Möglichkeiten und Potenzialen im Bereich der Einflussnahme auf die Informationssicherheit durch Dritte. Aus dem Blickwinkel der Informationssicherheit ist es daher von großer Bedeutung, diese Möglichkeiten und Potenziale und die daraus resultierende IT-Bedrohungslage konstant zu erfassen und auszuwerten.

Die IT-Bedrohungslage entwickelt sich sehr dynamisch, beispielsweise

- durch das Bekanntwerden oder sogar die Ausnutzung neu erkannter oder bisher nicht geschlossener Schwachstellen in industriellen Steuerungssystemen bzw. in für kritische Infrastrukturen relevanten IT-Systemen,
- durch zunehmende, gezielte, technisch versierte und andauernde IT-Angriffe mit fortgeschrittenen Methoden, Schadsoftwarekomponenten und IT-Angriffswerkzeugen sowie
- durch die sich kontinuierlich weiterentwickelnden Techniken, Taktiken und Vorgehensweisen der IT-Angreifer, insbesondere vor dem Hintergrund der stetig wachsenden Angriffsoberfläche.

Auf nationaler und internationaler Ebene sind regelmäßig IT-Sicherheitsvorfälle mit sicherungstechnischer Bedeutung und potenziell auf kerntechnische Anlagen und Einrichtungen übertragbaren Aspekten zu verzeichnen, woraus sich Veränderungen der IT-Bedrohungslage ergeben. Angesichts der sich dynamisch verändernden IT-Bedrohungslage werden international die bestehenden Regelwerke und Richtlinien zur IT-Sicherheit (insbesondere von IAEO, IEC und ISO) und damit die Anforderungen an Sicherungsmaßnahmen ständig weiterentwickelt und erweitert. Beispiele hierfür sind die beiden Standards:

- IAEA NSS No. 17-T (Rev.1), Computer Security Techniques for Nuclear Facilities, September 2021 und
- IAEA NSS No. 42-G, Computer Security for Nuclear Security, July 2021.

Auch nationale Vorgaben zur IT-Sicherheit in Deutschland (BSI-Grundschutz, IT-SIG) und anderen Ländern (z. B. in GB, SF, USA) wurden in den letzten Jahren überarbeitet oder befinden sich gerade in Überarbeitung.

Für die IT-Sicherheit kommt damit der regelmäßigen Analyse der Bedrohungslage, aber auch der Bewertung des Standes von Wissenschaft, Technik und Erkenntnis zur Prävention und Detektion von sowie zur Reaktion auf IT-Angriffe eine besondere Bedeutung zu. Die GRS verfolgt daher die Entwicklung der IT-Bedrohungslage für industrielle Steuerungssysteme und kritische Infrastrukturen, relevante IT-Sicherheitsvorfälle, IT-Angriffe, Schwachstellen, IT-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 IT-Angriffswerkzeuge. Gleiches gilt bei Schwachstellen in industriellen Steuerungssystemen und weiteren relevanten IT-Systemen, und zwar sowohl für deren Ausnutzung und das Bekanntwerden entsprechender Exploits als auch für Patches und Updates zum Schließen oder Mitigieren der Schwachstellen. Dabei bedeutet die Entdeckung eines IT-Angriffs häufig nicht dessen Ende, sondern bietet den Angreifern lediglich Anlass, zunächst auf einzelne Angriffswege und Angriffswerkzeuge zu verzichten und diese im weiteren Verlauf anzupassen. So können sich – auch Jahre nach dem ersten Bekanntwerden – noch relevante, zusätzliche Aspekte ergeben, aufgrund derer Ersteinschätzungen immer wieder ergänzt,

angepasst oder vollständig überarbeitet werden müssen. Um dieser Dynamik gerecht zu werden, handelt es sich bei den im vorliegenden Bericht wiedergegebenen Beschreibungen (siehe Anhang) daher nicht um abschließende Bewertungen der jeweiligen Vorkommnisse, sondern um eine Momentaufnahme. Aufgrund dieser sich unter Umständen auch noch Jahre nach dem ersten Bekanntwerden ändernden Informationslage zu IT-Sicherheitsvorfällen, Angriffen und Schwachstellen müssen auch bisherige Auswertungen immer wieder auf ihre Aktualität geprüft und ggf. angepasst werden.

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

Zusätzlich zu den jeweils aktuell bekannt gewordenen IT-Sicherheitsvorfällen, IT-Angriffskampagnen 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 IT-Angriffswerkzeugen, werden auch Informationen zu den in diesem Zusammenhang aktuell relevantesten APT-Gruppierungen und deren Aktivitäten kontinuierlich verfolgt und zusammengetragen.

Nach einem kurzen Abschnitt zu grundlegenden Hintergrundinformationen zu industriellen Steuerungssystemen, werden anhand von Themenschwerpunkten verschiedene Aspekte der aktuellen IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen vorgestellt.

Die Themenschwerpunkte dieses Berichtes sind:

- **IT-Angriffe mit Einsatz von Ransomware** – Ransomware-Angriffe nehmen einen immer größeren Teil der IT-Angriffe insgesamt ein. Gleichzeitig kommt es auch immer häufiger zu Schein-Ransomware-Angriffen, die nur vorgeblich auf Erpressung ausgerichtet sind, in der Realität aber auf die Zerstörung von Daten setzen. Auch setzen die Angreifer hierbei immer stärkere Druckmittel ein, vor allem durch die indirekte Lahmlegung von industriellen Steuerungssystemen und verfahrenstechnischer Prozesse.

- **IT-Angriffe über die Lieferkette** – Supply-Chain-Angriffen kommt eine immer größere Bedeutung zu. Vor allem bei gut geschützten Angriffszielen wählen Angreifer diesen zwar aufwändigeren, aber gleichzeitig komfortableren Weg, um Sicherheitsmaß-nahmen und Barrieren zu umgehen.
- **Schwachstellen in Zusammenhang mit der datentechnischen Kommunikation** – Seit 2019 ist eine Vielzahl von Schwachstellen in TCP/IP Stacks und anderen Kommunikationskomponenten bekannt geworden.
- **ICS-spezifische Werkzeuge, Schwachstellen und Angriffe** – industrielle Steuerungs-systeme rücken immer stärker in den Fokus von Angreifern, während gleichzeitig in großem Umfang Schwachstellen in industriellen Steuerungssystemen bekannt wer-den.
- **IT-Sicherheitsvorfälle im Energiesektor** – immer wieder kommt es zu Angriffen auf Stromnetze und Energieerzeugungsanlagen.
- **IT-Sicherheitsvorfälle in kerntechnischen und radiologischen Anlagen und Einrichtungen** – auch kerntechnische und radiologische Anlagen und Einrichtungen sind immer wieder direkt oder indirekt von IT-Angriffen betroffen.
- **Auswirkungen der COVID-19 Pandemie auf die Informationssicherheit** – die Pandemiesituation hat auch in Bezug auf die Informationssicherheit einige Änderungen ge-bracht, nicht zuletzt durch die starke Zunahme an Remote-Zugriffen.
- **Hervorrufung physischer Schäden durch IT-Angriffe** – in den Jahren 2021 und 2022 sind gleich mehrere dieser nach wie vor seltenen Fälle aufgetreten.
- **IT-Angriffe in Zusammenhang mit dem Krieg in der Ukraine** – bereits vor dem Hintergrund der wachsenden Spannungen und noch einmal seit Kriegsausbruch ist es zu einem starken Anstieg der politisch und strategisch motivierten IT-Angriffe gekommen.
- **Kollateralschäden von gezielten IT-Angriffen** – häufig beschränken sich die Auswirkungen eines IT-Angriffs nicht auf das eigentliche Angriffsziel.
- **APT-for-hire** – gegen Bezahlung stehen erhebliche Ressourcen auch Angreifern mit entsprechender Intention aber ohne eigene Ressourcen und Fähigkeiten zur Verfügung.

2 Hintergrundinformationen

Industrielle, verfahrenstechnische Prozesse werden typischerweise durch industrielle Steuerungssysteme (ICS) geregelt, gesteuert und überwacht (siehe Abb. 2.1). Mittels ICS erfolgt auch die Erfassung von Felddaten und die Bedienung der Prozesse.

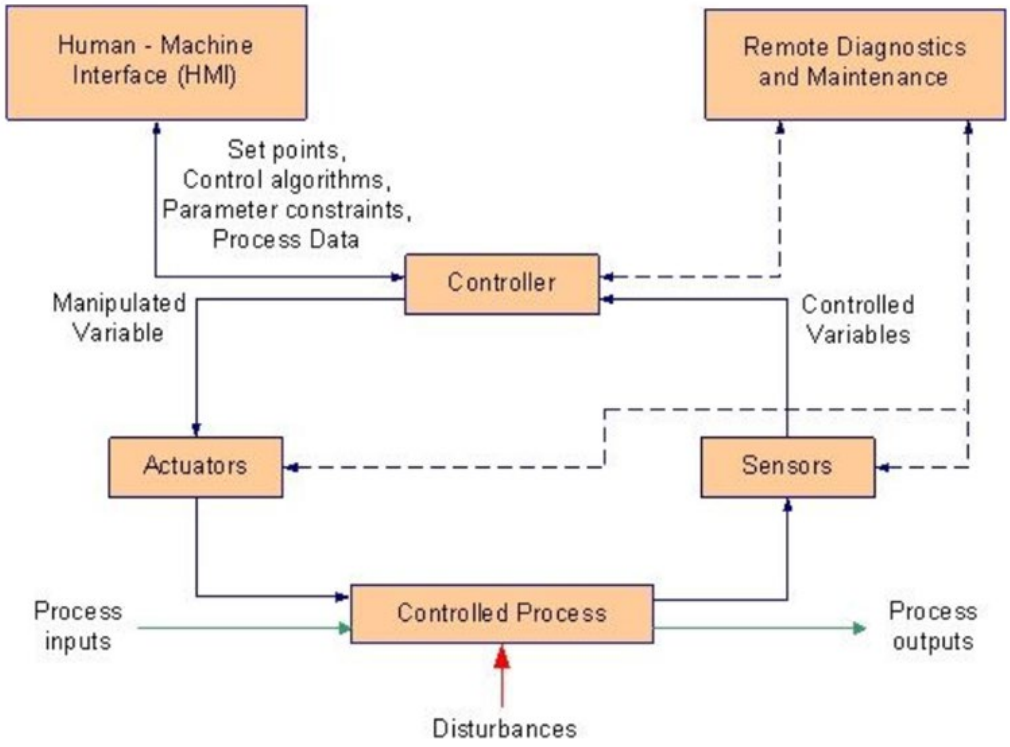

Figure 2-1. ICS Operation

Abb. 2.1 Übersicht über ein generisches industrielles Steuerungssystem

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

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

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

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

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

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

Ein generischer Aufbau für die IT- und leittechnische Architektur einer Anlage mit kritischen Sicherheits- und Steuerungssystemen ist beispielsweise der von FireEye erstellten Grafik zu entnehmen (Abb. 2.2). Dabei ist die IT der Anlage vom Internet durch eine oder mehrere Firewalls getrennt. Die sogenannte demilitarisierte Zone (DMZ), die sich zwischen der Anlagen-IT und den rechnerbasierten und programmierbaren leittechnischen Systemen und Komponenten befindet, ist beidseitig ebenfalls mit Firewalls geschützt. Die leittechnische Architektur teilt sich grob in die Systeme zur betrieblichen Steuerung und Regelung des verfahrenstechnischen Prozesses (hier DCS) und die Sicherheitssysteme zum Schutz vor potenziell gefährlichen Anlagenzuständen (SIS) auf

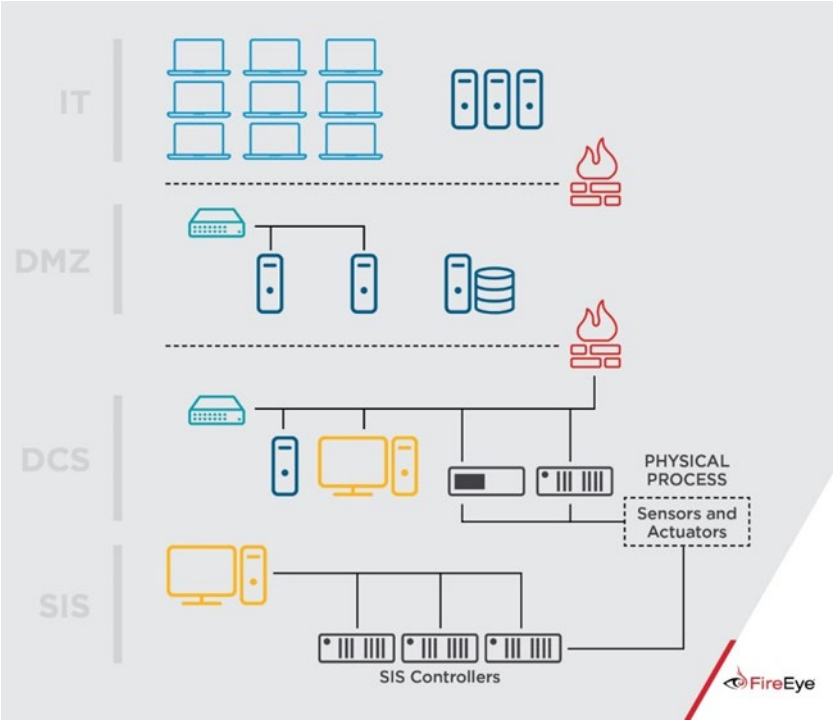

Abb. 2.2 Generischer Aufbau der IT- und leittechnischen Architektur einer Anlage mit kritischen Sicherheits- und Steuerungssystemen

Grafik unverändert übernommen aus /FIR17w01/

3 IT-Bedrohungslage

Die IT-Bedrohungslage für kritische Infrastrukturen und insbesondere kerntechnische Anlagen und Einrichtungen und ihre dynamische Entwicklung werden von der GRS fort-laufend verfolgt, erfasst und ausgewertet. Relevante Aspekte hierzu sind insbesondere bekanntgewordene

- Schwachstellen in industriellen Steuerungssystemen und in für kritische Infrastrukturen relevanten IT-Systemen (siehe Kapitel A im Anhang),
- IT-Angriffswerkzeuge, die unabhängig von IT-Angriffen bekannt werden (siehe Kapitel A im Anhang)
- IT-Sicherheitsvorfälle und IT-Angriffe einschließlich der dabei eingesetzten IT-Angriffswerkzeuge und Schadsoftwarekomponenten (s. Kapitel B im Anhang) sowie
- APT-Gruppierungen (Advanced Persistent Threat – fortgeschrittene andauernde Bedrohung) und ihre Aktivitäten (siehe Abschnitt 3.12).

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

- IT-Angriffe mit Einsatz von Ransomware
- IT-Angriffe über die Lieferkette
- Schwachstellen in Zusammenhang mit der datentechnischen Kommunikation
- ICS-spezifische Werkzeuge, Schwachstellen und Angriffe
- IT-Sicherheitsvorfälle im Energiesektor
- IT-Sicherheitsvorfälle in kerntechnischen und radiologischen Anlagen und Einrichtungen
- Auswirkungen der COVID-19 Pandemie auf die Informationssicherheit
- Hervorrufung physischer Schäden durch IT-Angriffe
- IT-Angriffe in Zusammenhang mit dem Krieg in der Ukraine
- Kollateralschäden von gezielten IT-Angriffen
- APT-for-hire

Diese Themenschwerpunkte werden in den folgenden Kapiteln 3.1 bis 3.11 vorgestellt.

3.1 Ransomware

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

Mittlerweile müssen Cyberkriminelle nicht mehr über Programmierkenntnisse verfügen, um Ransomware-Angriffe durchzuführen. APT-Gruppierungen wie z. B. REvil oder auch BlackMatter bieten Ransomware-as-a-Service (RaaS)-Lösungen an. Das bedeutet, dass sie eine für den jeweils beabsichtigten Angriff maßgeschneiderte Ransomware anderen Cyberkriminellen zum Kauf anbieten oder diese gegen eine Gewinnbeteiligung bei der Lösegelderpressung zur Verfügung stellen. Häufig streicht die APT-Gruppierung, welche die RaaS-Lösung bereitstellt, den Hauptteil des Lösegeldes ein. Da es sich bei den Lösegeldforderungen um Beträge im fünf- bis achtstelligen US-Dollar-Bereich handelt, ist die Inanspruchnahme dieser Dienste für Cyberkriminelle dennoch äußerst lukrativ.

Nicht zuletzt aufgrund der erzielbaren hohen Lösegeldbeträge und der Möglichkeit RaaS-Dienste in Anspruch nehmen zu können, nimmt die Zahl der Ransomware-Angriffe stetig zu.

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

- Bei REvil handelt es sich um eine vermutlich aus Russland heraus agierende APT-Gruppierung (siehe Abschnitt 3.12.10), welche weltweit Ransomware und RaaS sehr profitabel einsetzt und seit 2019 aktiv ist. Die von der Gruppierung bislang eingesetzte Schadsoftware fragt die Spracheinstellungen des infizierten Systems ab und wird bei Benutzern mit russischer Spracheinstellung nicht aktiv. Nach Verschlüsselung der Daten des angegriffenen Unternehmens durch die Schadsoftware wird von der Gruppierung eine entsprechende Lösegeldforderung gestellt mit der Drohung, während des Angriffs erbeutete, sensible Informationen bei Nichtzahlung zu veröffentlichen. Wenn das betroffene Unternehmen das Lösegeld nicht zahlt, führen die Angreifer einen Distributed-Denial-of-Service-Angriff (DDoS[1]) auf die Kunden und Geschäftspartner des Unternehmens durch. Zu den Angriffszielen von REvil gehören verschiedene Industriebereiche, u. a. im Bereich der Fertigung und Dienstleistung. Beispielsweise IT-Dienstleister oder das Gesundheitswesen - vor allem aber Unternehmen - von denen sich die APT-Gruppierung hohe Lösegelderträge verspricht.

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

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

zwei Organisationen des US-amerikanischen Lebensmittel- und Landwirtschaftssektors.

Sensible Daten von Unternehmen, die im Zuge von Ransomware-Angriffen gestohlen wurden, werden bei Zahlungsunwilligkeit der Angriffsopfer häufig auf Leak-Webseiten veröffentlicht. Diese Informationen können dann wiederum von anderen Cyberkriminellen genutzt werden, um weitere Angriffe zu planen. Befinden sich unter den gestohlenen Daten Informationen zu Lieferkettenstrukturen, sind zusätzlich zu den bereits attackierten Opfern, alle Lieferanten und Kunden des betroffenen Unternehmens potentielle Opfer von Datenlecks und somit das Ziel von IT-Angriffen.

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

- Eine mutmaßlich russische APT-Gruppierung kompromittierte mit Hilfe der Cuba-Ransomware Einrichtungen im Bereich der kritischen Infrastrukturen und erbeutete dabei Lösegeld für die angebliche Wiederherstellung der von ihnen verschlüsselten Daten (siehe Kapitel B.13.14 im Anhang). Bei den Angriffen wurde eine Vielzahl von Schadsoftware-Komponenten und Angriffstechniken eingesetzt. Die Cuba-Ransomware erhielt ihren Namen dadurch, dass sie die Endung der von ihr verschlüsselten Dateien in *.cuba* umbenannte. Seit Beginn des Jahres 2021 betreibt die APT-Gruppierung eine Leak-Webseite, auf der sie gestohlene Daten

veröffentlicht, sollte das Lösegeld nicht gezahlt werden. Einige der gestohlenen Daten wurden von den Angreifern verkauft. Zu den Angriffszielen gehören der Finanzsektor, Behörden und Regierungen, Gesundheitsorganisationen sowie Produktions- und Informationstechnikunternehmen in den USA, Südamerika und Europa.

- Am 23.01.2021 erfolgte ein Ransomware-Angriff auf WestRock, den zweitgrößten Hersteller von Verpackungen in den USA (s. Kapitel B.13.13 im Anhang). Der IT-Angriff hatte sowohl Auswirkungen auf das Büronetzwerk als auch auf das OT-Netzwerk. Mehrere Produktionsprozesse wurden bei dem Angriff unterbrochen. WestRock schaltete daraufhin verschiedene Systeme proaktiv ab, um eine weitere Ausbreitung der Schadsoftware zu verhindern. Mehr als zwei Wochen nach dem Angriff konnten immer noch nicht alle Systeme wiederhergestellt werden

- Im November 2021 führte die APT-Gruppierung BlackCat weltweit Ransomware-Angriffe auf Unternehmen aus dem Bereich der kritischen Infrastrukturen in Europa, Afrika, Asien und den USA durch (siehe die Kapitel B.14.16 und B.14.19 im Anhang). In Deutschland waren von den Angriffen zwei Unternehmen betroffen, die in der Lagerung und Lieferung von Öl und Mineralöl-Produkten tätig sind. Die Versorgungslage in Deutschland war allerdings nicht gefährdet, da andere Unternehmen aus dem Bereich der Tanklagerlogistik die Ausfälle kompensieren konnten. Am 22. Juli 2022 griff BlackCat den Netzbetreiber Creos und den Energieversorger Enovos an, die beide zur Encevo-Gruppe gehören und eine Gaspipeline sowie die Stromversorgung in Luxemburg betreiben. Nach der Datenverschlüsselung wurde das von den Angreifern geforderte Lösegeld allerdings nicht gezahlt. Daraufhin wurden einige der gestohlenen Daten von BlackCat veröffentlicht.

- Im Februar 2021 kam es zu einem IT-Sicherheitsvorfall im brasilianischen Kernkraftwerk Angra, bei dem die Ransomware DarkSide eingesetzt wurde (siehe Kapitel B.13.2 im Anhang). Allerdings wurde der Anlagenbetrieb davon nicht beeinflusst. Neben Angra wurden auch der Kernkraftwerksbetreiber Eletrobras selbst und der Energiekonzern Copel angegriffen. Dabei wurden Daten von Copel entwendet. Im Mai 2021 wurde der US-amerikanische Pipeline-Betreiber Colonial das Ziel eines IT-Angriffs von DarkSide (siehe Kapitel B.13.5 im Anhang). Die Colonial-Pipeline ist die größte Pipeline für Erdölderivate in den USA. Um eine weitere Ausbreitung der Schadsoftware zu verhindern, wurde der Betrieb der Pipeline durch den Betreiber innerhalb von wenigen Stunden nach Erkennung des Angriffs eingestellt. Dies führte beispielsweise zu Lieferengpässen und Treibstoffknappheit im Flugverkehr und bei Tankstellen. So konnte der Flugbetrieb an manchen Flughäfen nicht aufrecht

erhalten bleiben. Desweiteren bildeten sich vor zahlreichen Tankstellen aufgrund nicht verfügbarer Kraftstoffe lange Warteschlangen. Für die betroffenen Gebiete wurde der Notstand ausgerufen.

- Die russische APT-Gruppierung Conti verschafft sich üblicherweise durch Phishing-E-Mails Zugang zu den IT-Systemen ihrer Opfer. Am 14.05.2021 griff Conti mit der gleichnamigen Ransomware den irischen Gesundheitsdienst HSE (Health Service Executive) an (siehe Kapitel B.13.11 im Anhang). Daraufhin schaltete HSE sein gesamtes Computersystem ab, infolgedessen der Betrieb von zahlreichen Krankenhäusern eingeschränkt werden musste. Bei dem IT-Angriff wurden Daten sowohl verschlüsselt als auch gestohlen. Die Angreifer forderten ein Lösegeld für die Entschlüsselung und Nicht-Veröffentlichung der Daten. Da kein Lösegeld gezahlt wurde, folgte sodann die Veröffentlichung vertraulicher medizinischer Daten von Patienten sowie Unternehmensdokumenten im Internet durch die Angreifer. Es dauerte über 4 Monate, bis Ende September 2021, bis nahezu alle Systeme wieder in Betrieb genommen werden konnten. Am 08.11.2021 griff Conti das Unternehmen ONTEC Automation GmbH an, welches im Maschinen- und Anlagenbau tätig ist (siehe Kapitel B.13.15 im Anhang). Das Unternehmen ist auf den Bau von Automatisierungssystemen und Sondermaschinen für die industrielle Produktion spezialisiert und stellt somit ICS-Systeme her. Obwohl ONTEC zur Beschränkung der Auswirkungen des Angriffs IT-Systeme abschaltete, wurden weite Teile der IT-Infrastruktur verschlüsselt. Im April 2022 wurden mehrere Regierungsstellen in Costa Rica Opfer von Conti (siehe Kapitel B.14.8 im Anhang), betroffen waren dabei Finanz-, Zoll--- und Steuerbehörden, das Ministerium für Arbeit und Soziales sowie eine Universität. Der Angriff führte zu Ausfällen bei wichtigen Teilen von Behörden und Regierungsstellen, so dass der nationale Cyber-Notstand ausgerufen wurde. Es war das erste Mal, dass die Regierung eines Landes das Ziel einer Ransomware-Gruppe wurde. Der internationale Handel Costa Ricas kam zum Erliegen, wodurch ein Schaden in Millionenhöhe entstand. Am 31.03.2022 griff Conti den weltweit größten Hersteller und Service-Provider von Windenergieanlagen Nordex an (siehe Kapitel B.14.17 im Anhang). Als Vorsichtsmaßnahme schaltete das Unternehmen IT-Systeme an mehreren Standorten ab, um eine weitere Ausbreitung der Schadsoftware zu verhindern. Die von Nordex betreuten Windenergieanlagen blieben jedoch ohne Beeinträchtigung in Betrieb.

Weitere Ransomware-Angriffe werden im Anhang beschrieben (siehe beispielsweise Kapitel B.13.8, B.14.17, B.13.20 und B.14.13 im Anhang).

Zusammenfassend ist festzuhalten, dass Ransomware-Angriffe aufgrund der finanziellen Motivation durch die zu erzielenden hohen Lösegeldbeträge und der gleichzeitig immer einfacheren Möglichkeit, dies durch Inanspruchnahme von RaaS-Lösungen auch ohne eigene Fachkenntnisse zu erreichen, eine stetig wachsende Bedrohung darstellen. Dabei steht inzwischen nicht mehr nur die zeitweise Verschlüsselung der Daten des Opfers im Vordergrund sondern vermehrt auch der Einsatz von Schadsoftwarekomponenten, die nur vorgeblich Ransomwarekomponenten sind, aber keine Funktionalität für die Entschlüsselung der Daten besitzen und so betroffene Daten dauerhaft zerstören. Auch ist eine Beschränkung der Verschlüsselung auf reine Büro-IT, wie zu Beginn der Ransomware-Angriffe üblich, nicht mehr gegeben. Im Zuge der bei den Angriffen erfolgenden Datenverschlüsselung werden auch immer häufiger ICS-Systeme in Mitleidenschaft gezogen. Dies führt zu Produktionsausfällen, Lieferengpässen und in Verbindung mit der Lösegeldforderung der Angreifer für die Datenentschlüsselung zu einem immensen finanziellen Schaden. Auch ist die Wiedererlangung der verschlüsselten Daten längst nicht mehr der einzig maßgebliche Aspekt der Erpressung. Die Angreifer drohen neben dem Datenverlust zumeist auch mit der Veröffentlichung von im Zuge des Angriffs gestohlenen, sensiblen Daten. Auch geben die Angreifer in manchen Fällen durch eine Ausweitung der Drohungen und mögliche Angriffe auf den Kundenstamm eines Unternehmens ihren Forderungen noch stärkeres Gewicht. Ein in den letzten Monaten verstärkt beobachteter Trend zeigt zudem, dass besonders erfolgreiche Angreifergruppierungen mehr und mehr auch durch die Hervorrufung von Ausfällen bei verfahrenstechnischen Prozessen, den Druck auf die betroffenen Unternehmen noch deutlich erhöhen. Dieser Aspekt wiegt insbesondere bei Ransomware-Angriffen auf Organisationen im Bereich der kritischen Infrastrukturen besonders schwer.

3.2 Supply-Chain-Angriffe

In Anbetracht der fortschreitenden Digitalisierung und Globalisierung weltweit in nahezu sämtlichen Bereichen sind die Lieferketten (supply chain) im Bereich von IT-Systemen und industriellen Steuerungssystemen in den letzten Jahren zunehmend vielschichtig und komplex geworden. Die steigende Komplexität von Software, Hardware und IT-Dienstleistungen in diesem Zusammenhang bietet Angreifern vielfältige Möglichkeiten, insbesondere innerhalb der Lieferkette von Komponenten oder Diensten. Jüngste IT-Sicherheitsvorfälle wie die Supply-Chain-Angriffe auf international aufgestellte Unternehmen bzw. Produkte, die weltweit große Aufmerksamkeit erfuhren, verdeutlichen die potenziell verheerenden Folgen derartiger Angriffe.

Generell gab es in den vergangenen Jahren wiederholt 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 hohe Relevanz dieser Thematik für den Bereich der Cybersicherheit wird auch international zunehmend diskutiert und liegt im Fokus nationaler und internationaler Behörden und Organisationen weltweit.

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

Durch die Abhängigkeiten und Wechselwirkungen der einzelnen Schritte im Lebenszyklus eines IT-Systems, der Involvierung von in der Regel mehreren Zulieferern und der sich dadurch bietenden unterschiedlichen potenziellen 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 optimal ist und Informationen nur verspätet, nicht vollständig oder gar nicht weitergegeben werden. Für Betroffene ist eine gesicherte und stets aktuelle Informationslage essenziell, um Risiken für die eigene Organisation einschätzen und ggf. frühzeitig Maßnahmen ergreifen zu können, da auf Schwachstellen oder Sicherheitsrisiken nur reagiert werden kann, wenn diese bekannt sind. Insgesamt sind somit zur Vermeidung von IT-Sicherheitsvorfällen für Betreiber kritischer Infrastrukturen nicht nur das Sicherheitsmanagement und entsprechende Sicherheitsmaßnahmen vor Ort, sondern auch darüber hinausgehende 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.

Zahlreiche Angreifer haben in den vergangenen Jahren für ihre IT-Angriffe explizit auf bekannte bzw. zum Angriffszeitpunkt unbekannte Schwachstellen in der Lieferkette von IT-Systemen gesetzt, um ihre Ziele zu erreichen. Insbesondere kleinere oder mittelständische Hersteller oder IT-Dienstleister, die bezüglich IT-Sicherheitsmaßnahmen verglichen mit internationalen Großunternehmen lediglich eingeschränktere Möglichkeiten haben, stellen sich so oftmals als schwächstes Glied in der Lieferkette heraus, 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 Jahr 2021 wurden Informationen über schwerwiegende Sicherheitslücken bei Microsoft bekannt, welche von Angreifern dazu ausgenutzt werden können, um Microsoft Exchange Server, welche unter anderem für das weltweit verbreitete E-Mail und Organisations-Programm Outlook genutzt werden, vollständig zu kontrollieren (siehe Kapitel A.5.1 im Anhang). Zum Zeitpunkt des Bekanntwerdens wurde die Schwachstelle bereits aktiv von IT-Angreifern ausgenutzt, wodurch potenziell eine hohe Anzahl von Unternehmen, Behörden und Betreibern kritischer Infrastruktur betroffen war. Die Schwachstellen ermöglichen neben der Übernahme des gesamten Systems aus der Ferne durch IT-Angreifer auch Datendiebstahl und die Installation von Schadsoftware. In Deutschland waren Anfang 2021 von den Schwachstellen zehntausende Server potenziell betroffen.

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

- Bezüglich manipulierter, schadsoftwarebehafteter Solar-Winds-Produkte und Updates wurde im Dezember 2020 eine Angriffswelle von IT-Angriffen über die Lieferkette entdeckt (siehe Kapitel B.12.4 im Anhang). Betroffen hiervon war die Software-Plattform SolarWinds Orion, die unter anderem Monitoring und Management von IT-Netzwerken, -Systemen und -Anwendungen ermöglicht und von 33.000 SolarWinds Kunden genutzt wird. Bei diesem IT-Sicherheitsvorfall gelang es den Angreifern, unbemerkt eine Reihe von SolarWinds Orion Versionen mit einer Schadsoftwarekomponente zu infizieren, welche dann digital signiert und somit für Endkunden vom Hersteller zertifiziert ab März 2020 über den offiziellen Update-Server von SolarWinds verteilt wurden. Der 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 (bspw. die US-Departments of Homeland Security, Justice, Energy, Commerce und Treasury ebenso wie das US Department of State und die National Institutes of Health) sowie große, private IT-Unternehmen wie Microsoft oder Cisco und auf Analysen von IT-Angriffen spezialisierte Firmen wie FireEye.

- Weitere IT-Angriffe über die Lieferkette erfolgten auf die Software- bzw. IT-Dienstleistungsunternehmen Centreon (siehe Kapitel B.13.2), CodeCov (siehe Kapitel B.13.3), Ivanti (siehe Kapitel B.14.12) und Kisters AG (siehe Kapitel B.13.6). Obwohl IT-Angriffe über die Lieferkette nicht grundsätzlich auf Schwachstellen in der entsprechenden Software angewiesen sind, sind die potenziellen Folgen, wenn entsprechende Schwachstellen oder Zero-Day-Exploits vorliegen, oftmals verheerend. In diesem Zusammenhang verursachte das Bekanntwerden einer Schwachstelle in der Java Programmierbibliothek Log4j des amerikanischen Herstellers Apache im Dezember 2021 weltweit großes Aufsehen (siehe Kapitel A.5.12). Log4j ist Teil diverser Open-Source- und kommerzieller Softwareprodukte und hat sich zu einem De-Facto-Standard im Bereich des Loggings in Java entwickelt, der entsprechend weit verbreitet ist. Die Log4Shell genannte Schwachstelle ermöglicht es Angreifern bei einem IT-Angriff über Abhängigkeiten bzw. das Einbinden externer Java-Bibliotheken beliebigen Code auf dem angegriffenen System auszuführen und beispielsweise die vollständige Systemkontrolle zu übernehmen. Die Schwachstelle kann vollautomatisiert direkt über das Internet ausgenutzt werden. Weltweit wurden zahlreiche IT-Angriffe über die Schwachstelle registriert.

Insgesamt gilt nach wie vor, 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-Angriffe dar. Zum anderen reduzieren sich die Möglichkeiten, die der Endkunde zur Detektion von schadsoftwarebehafteten Produkten hat, je früher im Entwicklungsprozess der Soft- oder Hardware die Angreifer ihre Manipulationen vorgenommen haben. Auch sind die Detektionschancen für eine vorliegende Infektion mit Schadsoftware typischerweise geringer, wenn die Schadsoftware über die Lieferkette eingebracht wurde, da so der Footprint beim eigentlichen Angriffsziel kleiner

bleibt. Daher sind die Erfolgsaussichten bei Supply-Chain-Angriffen auf gut geschützte Ziele meist deutlich höher als bei direkten IT-Angriffen von außen.

3.3 Datentechnische Kommunikation

Als zentrale Schnittstelle zwischen IT-Systemen hat sich die Kommunikation in den letzten Jahren zu einem Schwerpunkt im Bereich der Informationssicherheit entwickelt. Die vermehrte Veröffentlichung von Forschungsarbeiten zu Schwachstellen in teilweise seit Jahrzehnten genutzten Kommunikationsprotokollen, vermehrte Angriffe auf die Kommunikationsverbindungen und der Bedeutungszuwachs der Kommunikation durch die COVID-19-Pandemie (siehe Kapitel 3.8) haben ein Bedrohungsumfeld geschaffen, in welchem der Kommunikation von IT-Systemen besondere Aufmerksamkeit zuteilwird.

Die meisten Kernaufgaben von IT-Systemen können ausschließlich mit datentechnischen Verbindungen zu anderen IT-Systemen realisiert werden. Ohne Verbindung zu datenverarbeitenden Servern oder zentral gespeicherten Datenbanken können innerhalb von Organisationen viele Aufgaben nicht realisiert werden. Leittechnische Systeme basieren auf der Kommunikation mit eigenen leittechnischen Servern oder Controllern und angesteuerten Feldgeräten. Sicherungstechniken wie Einbruchmeldesysteme sind als komplexe Verbünde aus Sensoren, Kameras, Alarmierungen, Servereinheiten und Bedieneinheiten aufgebaut. Jede dieser datentechnischen Verbindungen kann entsprechend dem „Open Systems Interconnection“-Modell kurz ISO/OSI-Referenzmodell, dargestellt werden. Dabei wird die Kommunikation über insgesamt bis zu 7 Schichten von der physischen Datenübertragung über die Adressierung und den Transport bis zur inhaltlichen Darstellung realisiert. Abseits der physischen Übertragungsebene ist für jede Datenübertragung ein Protokoll und damit eine Softwarelösung notwendig. Diese Softwarelösungen bearbeiten nicht nur sämtlichen durchgehenden Netzwerkverkehr, sondern besitzen zumeist auch tiefgreifende Systemzugriffe.

Mit der technologischen Entwicklung haben sich einige wenige Kommunikationsmethoden durchgesetzt. So ist die auf den Protokollen TCP und IP basierte Kommunikation zum zentralen Kommunikationsmittel in lokalen Netzwerken (LAN und WLAN), großen Netzwerken (WAN) und dem offenen Internet geworden. Im Bereich der industriellen Kommunikation haben sich insbesondere die zeitsensitiven Kommunikationsprotokolle Profibus und Modbus sowie auf TCP/IP basierende Protokolle wie Profinet durchgesetzt.

Die zur Verarbeitung der Kommunikation notwendigen Softwarelösungen werden, wenn sie mehrere Schichten des ISO/OSI-Referenzmodells abdecken, zumeist Protokolltürme (Stacks) genannt. Solche Stacks werden häufig Open Source oder kommerziell angeboten, wodurch einige Modelle eine milliardenfache Verbreitung gefunden haben, zum Teil ohne das Wissen der tatsächlichen Endnutzer. Entsprechend der in Kapitel 3.2 beschriebenen Lieferkettenproblematik, kann eine einzige erkannte Schwachstelle zur Betroffenheit von hunderten verschiedenen Produkttypen und Millionen von IT-Systemen führen. In den letzten Jahren haben insbesondere folgende Schwachstellen in der Netzwerkkommunikation verdeutlicht, wie groß das Angriffspotenzial auf die Kommunikation ist:

- **URGENT/11:** Im Jahr 2019 wurden 11 Schwachstellen im TCP/IP Stack IPnet entdeckt. IPnet wird insbesondere im leittechnischen Echtzeitbetriebssystem VxWorks verwendet, wodurch die Kommunikationsschwachstellen eine hohe Relevanz für leittechnische Systeme haben. 6 Schwachstellen ermöglichen als kritische[2] Schwachstelle bei Ausnutzung die vollständige Systemübernahme. Die Schwachstellen bestanden zum Teil mehr als 13 Jahre lang.

- **Ripple20:** Unter Ripple20 wurden im Jahr 2020 19 Schwachstellen im weit verbreiteten TCP/IP Stack ELMIC, auch bekannt als Net+ OS, Quadnet, GHNET v2 und Kwiknet, entdeckt. Die zum Teil kritischen Schwachstellen ermöglichen ebenfalls teilweise die vollständige Systemübernahme und betrafen leittechnische und IT-Systeme von Herstellern wie ABB, Aruba Networks, Cisco, HP, Miele, Mitsubishi Electric, Rockwell Automation, Schneider Electric und Xerox.

- **Amnesia:33:** Als Amnesia:33 wurden im Jahr 2020 insgesamt 33 bis dahin unbekannte zum Teil kritische Schwachstellen in vier verschiedenen TCP/IP Stacks bekannt. Die kritischen Schwachstellen betrafen die Open Source Stacks uIP, FNET, picoTC und Nut/Net, welche aufgrund des Open Source Charakters weit verbreitet sind.

[2] Kritische Schwachstellen sind solche Schwachstellen mit einem Common Vulnerability Scoring System (CVSS) Wert über 9 Punkten. CVSS hat sich international als De-Facto-Standard für die Bewertung von Schwachstellen etabliert. Mit dem CVSS Bewertungssystem wird Softwareschwachstellen eine Gefährdungszahl zwischen 1 (minimale Gefährdung) und 10 (maximale Gefährdung) zugeordnet. Sie dient der einfachen generellen Übersicht über die Gefährdung, welche von der entsprechenden Softwareschwachstelle ausgeht. Den CVSS Scores werden abgestuft nach dem berechneten Zahlenwert auch qualitative Schweregrade zugeordnet. So werden beispielsweise Schwachstellen mit CVSS Score 4.0 bis 6.9 als moderat bezeichnet, Schwachstellen mit CVSS Score 7.0 bis 8.9 als schwerwiegend und Schwachstellen mit CVSS Base Score von 9.0 bis 10.0 als kritisch.

- **INFRA:HALT**: Als INFRA:HALT wurde im Jahr 2021 eine Serie von 14 zum Teil kritischen Schwachstellen im TCP/IP Stack NicheStack bekannt. Dieser Stack wird insbesondere in leittechnischen Systemen eingesetzt.
- **NAME:WRECK:** 2021 wurden weiterhin 14 zum Teil kritische Schwachstellen in den TCP/IP Stacks FreeBSD, IPnet, NetX und Nucleus NET aufgefunden. Insbesondere IPnet zugehörig zum Echtzeitbetriebssystem VxWorks und Nucleus Net, der für das Nucleus Echtzeitbetriebssystem von Siemens verwendete TCP/IP Stack, erlangten dabei hohe Aufmerksamkeit aufgrund der potenziellen Betroffenheit von leittechnischen Systemen.
- **NUMBER:JACK:** Darüber hinaus wurden im Jahr 2021 unter dem Namen NUMBER:JACK weitere 9 moderate und schwerwiegende Schwachstellen in den TCP/IP Stacks Nut/Net, uC/TCP-IP, CycloneTCP, NDKTCPIP, FNET, uIP, Contiki, PicoTCP, MPLAB Net und Nucleus Net entdeckt.
- **Profinet:** Profinet ist ein Standard für die Echtzeitkommunikation von leittechnischen Systemen. 2020 veröffentlichte Siemens Hinweise zu insgesamt 14 im Zusammenhang mit dem Standard Profinet bestehenden Schwachstellen. Profinet wird von einer Vielzahl von Siemens Produktfamilien im leittechnischen Bereich unterstützt.

Den meisten dieser Schwachstellen ist gemein, dass für diese bei Bekanntwerden oder kurz darauf, Softwareupdates für die betroffenen TCP/IP Stacks bereitstanden. Die Verbreitung dieser Softwareupdates über die Lieferketten erwies sich jedoch als schleppend, sodass anzunehmen ist, dass in vielen der betroffenen Systeme auch aktuell noch die entsprechende Schwachstelle vorliegt.

Die offenen Schwachstellen bieten eine umfassende Angriffsoberfläche mit Einwirkungen auf betroffene Systeme. Darüber hinaus ist die Kommunikation jedoch ein zentrales Werkzeug zur Verbreitung von Schadsoftware und zur Durchführung von IT-Angriffen, sei es im Rahmen von Erstinfektionen oder Folgeinfektionen. Klassische Angriffe über die Kommunikation bzw. auf Kommunikation sind Denial-of-Service Angriffe, bei denen die Systeme durch spezifische Anfragen überfordert werden und damit Zustände erreicht werden, in welchen Angreifer die Kontrolle über die Systeme übernehmen können oder aber zumindest die Systeme zum Absturz bringen können. Des Weiteren kann die Kommunikation auch direkt angegriffen werden, in dem z. B. Kommunikationsdaten ausgelesen oder verändert werden. In Man-in-the-Middle Angriffen wird sich dies zu Nutze gemacht. Schwachstellen in den Kommunikationsprotokollen erleichtern solche Angriffe.

Daher werden für die Kommunikation von IT-Systemen mittlerweile umfassende Schutzmaßnahmen eingesetzt, wobei auch diese wiederum von Schwachstellen betroffen sein können und als Angriffsoberfläche dienen können. Ein Beispiel hierfür sind IT-Angriffe auf Firewalls von Routern der Marke WatchGuard (siehe Kapitel B.14.22 im Anhang). Hierbei wurden Firewalls mit Schadsoftware einer APT-Gruppierung angegriffen, wodurch der von den Geräten behandelte Netzwerkverkehr ausspioniert werden konnte und die Systeme selbst für Botnetaufgaben zur Verfügung standen. Im Rahmen des QuietExit Angriffs (siehe Kapitel B.14.20 im Anhang) wurde über einen langen Zeitraum Netzwerktechnik innerhalb des betroffenen Unternehmens angegriffen und durch die Angreifer übernommen. Ausgehend von den betroffenen Systemen der Netzwerktechnik, aber auch anderer, weniger beachteter vernetzter Systeme wie Kameras und Datenspeichersysteme, wurden die Angriffe dann weiter fortgeführt. Der Schutz der Kommunikation ist mittlerweile ein zentral zu beachtender Punkt beim Aufbau von Kommunikationsnetzwerken und stellt Anlagen immer wieder vor umfassende Herausforderungen, nicht nur in Bezug auf die Prävention, sondern auch langfristig im Rahmen der Detektion und Reaktion.

Weitere Angriffe auf die Kommunikation betreffen insbesondere Formen von Spoofing. Hierbei werden z. B. bei Angriffen auf das DNS (Domain Name System) System Anfragen auf unerwünschte Netzwerkadressen oder Webseiten umgeleitet. Weiteres Spoofing betrifft z. B. das aktuell in Europa auftretende Spoofing von Telefonnummern durch Betrüger im Rahmen der „Europol-Anruf“-Betrugsserie. Im Rahmen von mehreren IT-Angriffen auf den Kommunikationsdienstleister T-Mobile USA nutzten Angreifer die erbeuteten Daten, um sich Zugriff auf neu zugeschickte SIM-Karten der Nutzer zu verschaffen. In dessen Folge hatten diese Zugriff auf die Kommunikation, z. B. in Form von Authentifizierungs-SMS der Nutzer und damit auf zugangsbeschränkte Konten.

Durch die stetig wachsenden Angriffsmöglichkeiten wird die Kommunikation von IT-Systemen langfristig im Fokus von Angreifern bleiben. Schwachstellen in Softwarekomponenten, Protokollen oder Kommunikationssystemen wie Firewalls und Routern bieten eine große Angriffsoberfläche, gleichzeitig sind kontinuierlich oder temporär bestehende Datenverbindungen weiterhin der Hauptverbreitungsweg für Schadsoftwarekomponenten. Aus diesem Grund bleiben Sicherungsmaßnahmen, die zur Vermeidung sowie Detektion einer Verbreitung von Schadsoftwarekomponenten über solche datentechnischen Verbindungen dienen können, vor dem Hintergrund der aktuellen IT-Bedrohungslage essentiell.

3.4 ICS-spezifische Werkzeuge, Schwachstellen und Angriffe

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

Erste gezielte IT-Angriffe auf industrielle Steuerungssysteme wurden bereits vor über zehn Jahren beobachtet. In den öffentlichen, globalen Fokus gerieten derartige Angriffe erstmals durch das Bekanntwerden der speziell auf die Manipulation von speicherprogrammierbaren Steuerungen ausgerichtete Schadsoftware Stuxnet (siehe Kapitel B.1.1 im Anhang). Es handelt sich bei Stuxnet um eine hochkomplexe Schadsoftware, die zur Verbreitung mehrere Sicherheitslücken im Betriebssystem Microsoft Windows ausnutzt und nach der erfolgten Erstinfektion in der Lage ist, autonom und ohne mit den Angreifern zu interagieren, gezielt Manipulationen vorzunehmen. Diese Eigenschaften sind insbesondere für die Fähigkeit von Stuxnet relevant, Air Gaps bzw. weitere Sicherheitsmaßnahmen zu überwinden (z. B. durch die Verbreitung über mobile Datenträger wie USB-Sticks), die häufig genutzt werden, um IT-Systeme bzw. industrielle Steuerungssysteme vor IT-Angriffen zu schützen. Stuxnet sucht auf infizierten Systemen gezielt nach Prozesssteuerungssystemen, die SIMATIC WinCC oder SIMATIC PCS7 vom Hersteller Siemens einsetzen. Diese Siemens-Komponenten, die im Bereich ICS eingesetzt werden, wiesen in der Vergangenheit bereits diverse Schwachstellen auf (siehe hierzu beispielhaft Kapitel A.5.8 im Anhang). Die bei einem Angriff auf die Urananreicherungsanlage Natanz eingesetzten Versionen A, B und C von Stuxnet zielten auf die Manipulation von Frequenzumrichtern ab, um die Urananreicherung dort zu beeinflussen und physische Schäden an den eingesetzten Zentrifugen herbeizuführen (Kapitel B.3.1).

Innerhalb der letzten zehn Jahre wurden weitere IT-Sicherheitsvorfälle im Zusammenhang mit industriellen Steuerungssystemen beobachtet:

- Hierzu zählt beispielsweise eine von China unterstütze Spear-Phishing-Angriffswelle zwischen den Jahren 2011 und 2013 auf amerikanische Gaspipeline-Unternehmen, wobei die Angreifer unter anderem autorisierte Fernzugriffskanäle und darunter auch Systeme für den Datentransfer und Systeme mit Zugriff auf ICS kompromittierten (siehe Kapitel B.4.1 im Anhang). Dabei gelang es den Angreifern außerdem, auf die OT-Netzwerke betroffener Gaspipeline-Unternehmen zuzugreifen. Die CISA und das FBI gehen davon aus, dass der IT-Sicherheitsvorfall zur Vorbereitung möglicher IT-Angriffe auf die Pipeline-Infrastruktur der USA mit dem Ziel der Herbeiführung physischer Schäden bzw. weitreichender Störungen genutzt werden könnte.

- Ein weiterer IT-Angriff auf die kritische Infrastruktur der USA erfolgte im Februar 2021, wobei die Angreifer ebenfalls einen Fernwartungszugriff nutzten. Der IT-Angriff betraf eine Wasserwiederaufbereitungsanlage in Florida (siehe Kapitel B.13.1 im Anhang). Die Angreifer nutzten den Fernwartungszugriff, der von den Mitarbeitern insbesondere in der Covid-19-Pandemiezeit verwendet wurde, um einen Regler für die Steuerung des Anteils von Natriumhydroxid im Wasser zu manipulieren. Da der Angriff rechtzeitig erkannt wurde, ergaben sich keine weiteren Auswirkungen. Hätten die Angreifer Erfolg gehabt, hätten zwar Sicherheitssysteme abweichende Werte in der Wasserqualität detektiert, woraufhin die Verfügbarkeit der Wasserversorgung im weiteren Verlauf jedoch möglicherweise beeinträchtigt gewesen wäre.

- Mit der Schadsoftware Crashoverride bzw. Industroyer wurde mutmaßlich beim Angriff auf das ukrainische Stromnetz im Jahr 2016 erstmals eine Schadsoftware eingesetzt, die gezielt für IT-Angriffe auf elektrische Stromnetze entwickelt wurde (siehe Kapitel B.8.1 im Anhang). Dabei können mit Crashoverride gezielt industrielle Steuerungssysteme in Umspannwerken und anderen elektrischen Einrichtungen direkt manipuliert werden. Bei dem IT-Angriff wurde ein Umspannwerk in Kiew angegriffen, was zu einem über Stunden dauernden Stromausfall führte. Die Schadsoftware Crashoverride bietet u. a. die Möglichkeit, Schalter und Trennschalter in Umspannwerken zu kontrollieren, wodurch sich durch ihren modularen und erweiterbaren Aufbau auch weitere Angriffsmöglichkeiten ergeben. Weitere IT-Angriffe auf das ukrainische Stromnetz mit dem Fokus der Manipulation industrieller Steuerungssysteme, erfolgten unter anderem mit Hilfe der Schadsoftware BlackEnergy (siehe Kapitel B.7.1 im Anhang) und Industroyer-2 (siehe Kapitel B.8.1 im Anhang).

- Die Schadsoftware Triton/TriSIS wurde im Rahmen eines IT-Angriffs auf eine petrochemische Anlage in Saudi-Arabien im Jahr 2017 entdeckt, als es in Folge von Manipulationen von Steuerungen von Sicherheits- und Schutzsystemen der Anlage zu mehreren Schutzabschaltungen von sicherheitsrelevanten verfahrenstechnischen Prozessen kam (siehe Kapitel B.9.2 im Anhang). Die Schadsoftware wurde dabei im Image einer dem Safety Instrumented System (SIS) zugeordneten Engineering Workstation gefunden, wodurch sich die entsprechenden potenziellen Auswirkungen auf die Ausführung von Sicherheits-, Sicherungs- und Schutzfunktionen ergaben. Daneben war auch das industrielle Steuerungsnetz zur Steuerung verfahrenstechnischer Prozesse betroffen. Ähnlich wie Stuxnet, BlackEnergy und Crashoverride/Industroyer handelt es sich bei Triton/TriSIS um eine hochentwickelte, komplexe Schadsoftware, die auf industrielle Steuerungssysteme insbesondere kritischer Infrastrukturen ausgelegt ist und im Gegensatz zu diesen vor allem auf die Manipulation von Schutzfunktionen abzielt. Zusätzlich zu der potenziellen Beschädigung von Komponenten oder der Abschaltung/Störung von industriellen Prozessen und der expliziten Herbeiführung unsicherer Anlagenzustände ist mit Triton/TriSIS somit auch die Verhinderung von Schutzaktionen denkbar.

Neben den oben genannten gezielten IT-Angriffen auf industrielle Steuerungssysteme wurden in diesem Jahr mehrere Berichte über speziell auf ICS ausgelegte Angriffswerkzeuge bzw. entsprechende Schwachstellen veröffentlicht:

- Die CISA veröffentlichte in Zusammenarbeit mit dem FBI, das NSA und dem Department of Energy eine Warnmeldung zu einem ICS-Spezifischen Set aus IT-Angriffswerkzeugen, welches Incontroller bzw. Pipedream genannt wird (siehe Kapitel A.6.1 im Anhang). Dabei handelt es sich um ein hochkomplexes, maßgeschneidertes und vielfältig einsetzbares Set verschiedener Schadsoftwarekomponenten, die zum Einsatz gegen industrielle Steuerungssysteme mutmaßlich mit staatlicher Förderung durch unbekannte Angreifer entwickelt wurden und entsprechende Schwachstellen ausnutzen. Obwohl es bisher keine Informationen zu einem aktiven Einsatz von Incontroller/Pipedream gibt, erhöht aus Sicht des BSI *„die bloße Existenz von Incontroller/Pipedream das Bedrohungsszenario für ICS-Systeme“*. Betroffen von Incontroller/Pipedream sind speziell ausgewählte Controller und speicherprogrammierbare Steuerungen von Schneider Electric und Omron, wobei das Set modular aufgebaut ist und es Angreifern erlaubt, weitere Komponenten zu entwickeln und für andere leittechnischen Komponenten anzupassen. Hervorzuheben ist bei Incontroller/Pipedream, dass es Angreifern erlaubt, IT-Angriffe mit hohem

Automatisierungsgrad auf die anvisierten Controller durchzuführen, wodurch es prinzipiell auch von nicht fachkundigen Angreifern mit geringeren technischen Kenntnissen genutzt werden kann. Zu den denkbaren Szenarien beim Einsatz des Sets zählen unter anderem die Störung von Controllern in der betrieblichen Leittechnik zur Unterbrechung verfahrenstechnischer Prozesse, die Umprogrammierung von Controllern in der betrieblichen Leittechnik zur Sabotage verfahrenstechnischer Prozesse und die Deaktivierung von Controllern in der Sicherheitsleittechnik zur Hervorrufung physischer Schäden.

- Unter der Bezeichnung OT:ICEFALL veröffentlichten Forscher im Juni 2022 einen Bericht über 56 Schwachstellen verschiedener Geräte von zehn Anbietern, die Operational Technology (OT) betreffen (siehe Kapitel A.6.2 im Anhang). Die betroffenen Geräte von Herstellern wie Honeywell, Omron, Motorola und Siemens sind für ihren Einsatz in industriellen Anlagen, insbesondere auch in kritischen Infrastrukturen wie der Öl-, Gas-, Chemie- und Nuklearindustrie bekannt. Im Bericht wird die bisher im Bereich OT weniger ausgeprägte Sicherheitskultur thematisiert, die dazu führt, dass Geräte in diesem Bereich oftmals eine schlechte Allgemeinsicherheit bezogen auf IT- bzw. ICS-spezifische Angriffe aufweisen. Die im Bericht aufgeführten Angriffsmöglichkeiten hängen von den genauen anlagenspezifischen Umständen ab und umfassen unter anderem die Ausführung beliebigen Codes auf betroffen Geräten sowie Denial-of-Service-Angriffe, bei denen Angreifer zum Beispiel die Verfügbarkeit betroffener Geräte einschränken können.

Industrielle Steuerungssysteme geraten immer stärker in den Fokus von Angreifern. Dieser Fokus ist vielschichtig. Zum einen bieten potenzielle Produktionsausfälle und mögliche Schäden an verfahrenstechnischen Komponenten ein starkes Druckmittel im Rahmen von Ransomware-Angriffen (siehe Kapitel 3.1). Zum anderen lassen sich mit IT-Angriffen auf industrielle Steuerungssysteme Auswirkungen in der physischen Welt erreichen. Dies reicht von der Manipulation von Produkten und der Beeinflussung von Produktionsprozessen über den Ausfall, die Beschädigung und Zerstörung von Komponenten bis hin zu Auswirkungen auf Mensch und Umwelt. Insbesondere bei kritischen Infrastrukturen wie der Wasser- oder Energieversorgung lassen sich durch entsprechend ausgefeilte IT-Angriffe hier massive Auswirkungen erreichen, was sowohl im Rahmen von Drohgebärden oder der Demonstration von Fähigkeiten als auch zur Schwächung von Gegnern durchaus erwünscht ist. Vor dem Hintergrund der aktuellen, allgemeinen Bedrohungslage kommt ICS-spezifischen Schadsoftwarekomponenten und IT-Angriffen daher eine besondere Bedeutung zu.

3.5 IT-Angriffe mit physischen Schäden

Eine Untergruppe von ICS-spezifischen IT-Angriffen (siehe Abschnitt 3.4) bilden IT-Angriffe, die gezielt Schäden in der physischen Welt verursachen. Hierbei sind explizit keine vorübergehenden Ausfälle von verfahrenstechnischen Komponenten gemeint. Vielmehr zählen solche IT-Angriffe dazu, bei denen es zu einer gezielten Beschädigung oder Zerstörung von verfahrenstechnischen Komponenten kommt. Beispiele hierfür sind IT-Angriffe wie die Angriffe mit den verschiedenen Varianten der Schadsoftware Stuxnet (siehe Abschnitte B.1.1 und B.3.1 im Anhang), durch die es zur Beschädigung von zahlreichen Zentrifugen zur Urananreicherung gekommen ist, als auch der IT-Angriff auf ein deutsches Stahlwerk im Jahr 2014 (siehe Abschnitt B.6.2 im Anhang), bei dem ein Hochofen beschädigt wurde.

Im Juni 2022 ist es derzeitigen Informationen zufolge zu einem IT-Angriff auf die drei größten Stahlwerke des Iran gekommen, bei dem in mindestens einem der Stahlwerke verfahrenstechnische Komponenten beschädigt wurden (siehe Abschnitt B.14.6 im Anhang). Parallel zu den wachsenden Spannungen in der Region kommt es seit Monaten immer wieder zu Cyberangriffen auf israelischer oder iranischer Seite. Für einige der im Iran durchgeführten IT-Angriffe hat die Hackergruppierung Predatory Sparrow (Gonjeshke Darande) die Verantwortung übernommen. Hierzu zählen Angriffe auf die iranische Eisenbahn, den iranischen Rundfunk, zahlreiche Überwachungskameras und iranischen Tankstellen. Am 27.06.2022 gab die Gruppierung bekannt, die drei Firmen, welche sich das Monopol für die Stahlproduktion in Iran teilen, angegriffenen zu haben, und veröffentlichte einen mutmaßlichen Mitschnitt einer Überwachungskamera aus der Produktionshalle einer der Firmen. Darauf ist zunächst der normale Ablauf der Produktion zu sehen. Zudem ist sichtbar, wie das Personal nach und nach das Umfeld der Maschinen verlässt. Anschließend kommt es zu Störungen des Produktionsablaufes, bei dem nach wenigen Sekunden ein Feuer ausbricht. Das Video endet mit Beginn der Löscharbeiten. In den Tagen nach der Veröffentlichung dieses Videos sind weitere Videos aus der Anlage aufgetaucht, die dieselbe Szene aus teils anderen Blickwinkeln zeigen. Darin sind Rufe der Arbeiter nach der Feuerwehr sowie Ausrufe zu Schäden an Komponenten zu hören. Bislang wird das Bildmaterial von Analysten als authentisch eingestuft.

IT-Angriffe, die irreversible physische Schäden an verfahrenstechnischen Komponenten hervorrufen, sind nach wie vor recht selten. 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.

3.6 IT-Angriffe auf den Energiesektor

IT-Angriffe auf den Energiesektor können zu Stromausfällen führen und regionale bis hin zu länderübergreifende Auswirkungen haben. In diesem Zusammenhang muss nicht der Energieversorger zwingend das eigentliche Ziel des Angriffs sein. Es genügt bereits, wenn Geräte eines Herstellers, die von einem Angriff betroffen sind, in ICS-Systemen von Energieanlagen eingesetzt werden und zusätzlich eine unzureichende Trennung zwischen Büro-Netzwerken und ICS-Systemen vorliegt. Über die Verbindungen der Büro-Netzwerke mit dem Internet eingeschleuste Schadsoftware, kann sich dann auf die ICS-Systeme ausbreiten und den Anlagenbetrieb stören und im schlimmsten Fall zum Ausfall der Anlage führen. Seit dem russischen IT-Angriff mit der Schadsoftware BlackEnergy3 auf das ukrainische Stromnetz im Jahr 2015 (siehe Kapitel B.7.1 im Anhang), sind verstärkt gezielte Angriffe auf den Energiesektor zu beobachten. Vor allem mutmaßlich russischen Angreifergruppierungen hat die Ukraine dabei regelrecht als Versuchslabor gedient. Bereits ein Jahr nach dem Angriff mit BlackEnergy3 kam es im Jahr 2016 zu einem Stromausfall, nachdem ein Umspannwerk in Kiew mit der Schadsoftware Crashoverride/Industroyer angegriffen worden war (siehe Kapitel B.8.1 im Anhang). Bei Crashoverride/Industroyer handelt es sich um die erste Schadsoftware, mit der ICS-Systeme von Umspannwerken und anderen elektrischen Einrichtungen gezielt manipuliert werden können.

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 (siehe Kapitel B.7.1 im Anhang). Es wurden insgesamt drei Energieversorgungsunternehmen erfolgreich angegriffen, was zu einem mehrstündigen Stromausfall führte, von dem etwa 225.000 Kunden betroffen waren. Drei weitere Unternehmen wurden ebenfalls angegriffen, ihr Betrieb konnte aber aufrechterhalten werden. Die Schadsoftware BlackEnergy3 beinhaltet Plugins und Funktionen, die im Wesentlichen auf die Auskundschaftung von Netzwerken ausgerichtet sind sowie zusätzlich eine KillDisk-Komponente zur Datenlöschung. Eine spätere, abgewandelte Version der Schadsoftware bietet zusätzlich die Möglichkeit,

ICS-Systeme zu manipulieren. Die 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.

- Am 17.12.2016 führte die russische APT-Gruppierung ELECTRUM, welche in direkter Verbindung zur Gruppe Sandworm steht, einen weiteren Angriff auf das ukrainische Stromnetz aus (siehe Kapitel B.8.1 im Anhang). 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.

- Am 24.02.2022 begann Russland mit der Invasion der Ukraine (siehe Kapitel 3.9 sowie Kapitel B.14.5 im Anhang). Parallel zu den physischen Kampfhandlungen wurden auch IT-Angriffe gegen die Ukraine durchgeführt. Am 08.04.2022 sollten offenbar durch den Einsatz der Schadsoftware Industroyer2 industrielle Steuerungssysteme in Hochspannungsumspannwerken sabotiert und so ein Blackout hervorgerufen werden, von dem etwa zwei Millionen Menschen betroffen gewesen wären. Der Angriff, der der APT-Gruppierung Sandworm zugeschrieben wird, wurde jedoch rechtzeitig erkannt und ein Stromausfall konnte verhindert werden. Die Schadsoftware Industroyer2 basiert auf der Schadsoftware Industroyer bzw. Crashoverride, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert.

- Im März 2019 kam es zum ersten dokumentierten Fall eines IT-Angriffs auf einen Erzeuger erneuerbarer Energien in den USA (siehe Kapitel B.11.7 im Anhang). 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.

- Am 13. Oktober 2020 kam es in Mumbai zu einem Stromausfall, von dem 20 Millionen Menschen betroffen waren (siehe Kapitel B.12.3 im Anhang). Vermutlich war der Stromausfall die Folge 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 (siehe Kapitel B.13.2 im Anhang). Dabei wurde von den Angreifern die Ransomware Darkside eingesetzt. Neben dem Kernkraftwerk wurden auch dessen Betreiber Eletrobras und der Energiekonzern Copel mit der Schadsoftware angegriffen und Informationen von Copel wurden entwendet. Der IT-Sicherheitsvorfall hatte keinen Einfluss auf den Betrieb des Kernkraftwerks.

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

3.7 IT-Angriffe auf kerntechnische Anlagen und Anlagen mit radioaktiven Stoffen sowie auf Systemen zur Strahlungsüberwachung

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

Kerntechnischen Anlagen und Anlagen mit radioaktiven Stoffen sind aus gleich mehreren Perspektiven für Angreifende interessant. So sind Informationen über diese Anlagen und die darin eingesetzten verfahrenstechnischen Systeme und IT-Systeme sowie die Daten, die in diesen Anlagen erfasst, verarbeitet und ausgegeben werden, zum einen für Angreifergruppierungen, die staatlich beauftragt oder gefördert werden, im Rahmen der Spionage oder der potenziellen weiteren Angriffsvorbereitung direkt von Interesse. Ähnliches gilt auch für andere Gruppen, nicht zuletzt für politische Zwecke. Aufgrund der besonderen Bedeutung von kerntechnischen und radiologischen Anlagen, erfahren bekannt gewordene IT-Angriffe oder IT-Ereignisse mit kerntechnischem bzw. radiologischem Bezug hohe Aufmerksamkeit. Im Rahmen der Analyse der Bedrohungslage wurden dabei insbesondere IT-Angriffe auf die verwaltenden IT-Systeme von kerntechnischen und radiologischen Anlagen selbst, aber auch auf deren Zulieferer oder andere, im kerntechnischen Sektor agierenden Unternehmen verzeichnet. Zu den bekannt gewordenen IT-Angriffen auf kerntechnische Anlagen zählten neben dem bereits in Kapitel 3.6 erwähnten Angriff auf das Kernkraftwerk Angra unter anderem folgende Ereignisse:

- Mit dem indischen Kernkraftwerk Kudankulam wurde im Jahr 2019 ein direkter IT-Angriff auf ein sich im Betrieb befindliches Kernkraftwerk bekannt. Nach bisherigen Erkenntnissen wurden hierbei über mehrere Jahre Informationen zu Personen

im indischen zivilen nuklearen Sektor erforscht, um dann entsprechenden Personen und Unternehmen mit Schadcode behaftete Emails zu übersenden. Die Angreifenden gaben sich dabei als Mitarbeiter der indischen Regierung aus, was schließlich zur Infektion eines zentralen Servers des administrativen Netzwerks des Kernkraftwerks Kudankulam führte. Der Angriff wurde langfristig vorbereitet, erreichte tiefgehenden Systemzugriff im administrativen Teil, aber nicht im davon getrennten leittechnischen Teil des Anlagennetzes, und ermöglichte die Entwendung einer großen Menge an Daten. Der Angriff wird der APT Gruppe 38/Lazarus (siehe Kapitel 3.12.3) zugeordnet und wird in Kapitel B.11.2 im Anhang genauer beschrieben.

- Im Kernkraftwerk Südukraine kam es zu einem Zwischenfall durch die eigenen Mitarbeiter (siehe Kapitel B.11.1 im Anhang). Hierbei führten im August 2019 Mitarbeiter eigene IT-Systeme in den Verwaltungsbereich des Kraftwerks ein, mit dem Ziel Kryptowährungen wie Bitcoins auf diesen zu generieren. Da die hierfür notwendigen Hochleistungsgrafikkarten einen hohen Energiebedarf besitzen, wurde der Strom des Kernkraftwerks genutzt. Um Kryptowährungen zu erzeugen, ist eine permanente Internetverbindung notwendig, sodass die Mitarbeiter Teile des internen Netzwerks des Verwaltungstraktes entgegen den Vorgaben an das Internet anschlossen. Auch in den militärischen Kasernen der Nationalgarde wurde entsprechende Technik auf dem Kraftwerksgelände gefunden.

Dienstleister für kerntechnische Anlagen wurden in den letzten Jahren mehrmals Ziel von Angriffen auf deren informationstechnische Systeme. Hierzu zählt insbesondere der IT-Angriff auf den italienischen Konzern Sogin und der IT-Angriff auf den französischen Konzern Ingérop (siehe Kapitel B.13.19 und B.13.9 im Anhang):

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

- Sogin ist ein staatliches Unternehmen Italiens und ist für die Abwicklung des Rückbaus italienischer kerntechnischer Anlagen sowie die Entsorgung sonstiger radioaktiver Stoffe verantwortlich. Durch einen nicht näher dargestellten IT-Angriff wurden Ende 2020 umfassende Datensätze mit Informationen zu den Mitarbeitern, Passwörtern im Klartext, technischen Zeichnungen, Software- und Hardware-Updates,

weiteren betrieblichen Informationen sowie auch privaten Informationen gestohlen und im Darknet zum Verkauf angeboten. Es besteht aufgrund des Vorhandenseins privater Informationen unter den angebotenen Daten die Vermutung, dass durch eine private Nutzung von IT-Systemen eine Angriffsoberfläche für den Angriff auf Sogin entstanden ist.

Auch Anlagen mit radioaktiven Stoffen und Systeme zur Strahlungsüberwachung waren Ziel von IT-Angriffen:

- Im zweiten Quartal 2021 kam es zu einer Unterbrechung der Messung von Gammastrahlen in über 300 von insgesamt 800 in Spanien verteilten Messsystemen (siehe Kapitel B.14.25 im Anhang). Das RAR (Red de Alerta ala Radiactividad) genannte Überwachungs- und Warnsystem für Gammastrahlung wird von der staatlichen Generaldirektion für Katastrophenschutz und Notfälle (DGPCE) betrieben. Die Angreifer, welche sich als zwei frühere Mitarbeiter eines an der Entwicklung des RAR-Systems beteiligten Zulieferer herausstellten, griffen in einer ersten Phase auf die Computersysteme des DGPCE zu um anschließend die Messsysteme selbst anzugreifen und ihre Kommunikation mit der Zentrale zu unterbinden. Es handelt sich somit um eine direkte Innentäterschaft, deren Motive bisher nicht vollständig aufgeklärt werden konnten.

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

3.8 Auswirkungen der COVID-19-Pandemie auf die Informationssicherheit

Mit dem Auftreten der COVID-19 Pandemie kam es ab März 2020 zu zum Teil erheblichen Transformationsprozessen in der Arbeitswelt und dem sozialen Miteinander. Die durch den Infektionsschutz notwendig gewordenen bzw. vorgeschriebenen Maßnahmen umfassten zu einem großen Umfang die Arbeitswelt, welche in vielen Bereichen temporär zum Erliegen kam oder soweit möglich in Homeofficeumgebungen überführt wurde. Diese Transformation wurde durch Vorgaben von außen erzwungen. Viele Unternehmen waren hierauf nicht vorbereitet, sodass insbesondere 2020 und 2021 umfassende neue technische Lösungen für die Arbeitsumgebungen zuhause eingeführt werden mussten. Hierzu zählen Lösungen wie Fernzugriffe über VPNs und direkte Fernwartungen von Systemen, zu denen bis 2020 keine oder nur eingeschränkte Fernzugriffe möglich waren, aber auch der Ausbau von digitalen Speichermöglichkeiten, digitalen Versandmöglichkeiten und digitalen Bearbeitungsmöglichkeiten. Viele vorher in Präsenz durchgeführte Treffen wurden mit verschiedensten Softwarelösungen online durchgeführt, von kleineren Besprechungen bis zu großen Konferenzen. Im Unterschriftenwesen wurden teilweise Unterschriften auf Papier durch digitale Lösungen ersetzt, zum Teil mit dafür vorgesehenen Tools mit Sicherungsmaßnahmen, zum Teil durch das Einsetzen von eingescannten Unterschriften. Wo vorher die Informationssicherheit ausschließlich auf den IT-Systemen der Unternehmen sichergestellt werden musste, war mit Eintreten der COVID-19-Pandemie auch die Informationssicherheit vom Homeoffice bis zum Eingangsserver der Unternehmen, Behörden und anderen Einrichtungen notwendig zum Schutz vor IT-Angriffen. Da jedoch die COVID-19-Pandemie diese Transformationsprozesse erzwang, wurde häufig die Funktionalität und die Realisierungsgeschwindigkeit stärker als die Informationssicherheit priorisiert. In der Konsequenz kam es in Bereichen der Fernzugriffe und Fernwartungen zu einer Vergrößerung der Angriffsoberfläche und damit zu einer verstärkten Verwundbarkeit im Hinblick auf IT-Angriffe.

Angreifergruppierungen haben diese in der Breite angestoßenen Transformationsprozesse ebenfalls erkannt und immer wieder IT-Angriffe gezielt auf die Infrastruktur von Fernzugriffsprozessen wie VPN-Clients oder Router für Privatanwender ausgeführt:

- So wurde z. B. eine Wasserwiederaufbereitungsanlage in Tampa, Florida über die Fernwartung angegriffen. Die Angreifer griffen auf Steuerelemente der Wasseraufbereitung zu und versuchten über einen Regler, den vorgesehenen Anteil von Natriumhydroxid im Wasser von 100 ppm auf 11.000 ppm zu erhöhen. Einem

diensthabenden Mitarbeiter fiel der laufende Angriff auf, als sich das System selbstständig steuerte und er unterband den Angriff (siehe Kapitel B.13.1 im Anhang).

- Mittels eines nicht umfassend gesicherten VPN-Zugriffs erlangten Angreifende Zugriff auf die IT-Systeme des Colonial Pipeline Betreibers im Jahr 2021 und brachten Ransomware in das Netzwerk ein, wodurch der Pipelinebetrieb zum Erliegen kam.

Insbesondere Entwickler von VPN Clients und Fernwartungslösungen wurden seit 2020 vermehrt zum Ziel von IT-Angreifergruppierungen. So wurde zum Beispiel der VPN Client Pulse Connect Secure von Ivanti mehrfach angegriffen wie auch Kaseya, ein Entwickler für Remote-Monitoring and Management:

- Ivanti gab für das als besonders sicher beworbene Pulse Connect Secure im April 2021 eine kritische Schwachstelle bekannt, welche bereits zuvor von Angreifenden genutzt wurde. Die kritische Schwachstelle ermöglichte die vollständige Systemkontrolle der Pulse Connect Secure ausführenden IT-Systeme und führte zu IT-Angriffen auf Unternehmen wie den Telekommunikationskonzern Verizon oder die New Yorker U-Bahn, aber auch weitere Unternehmen der kritischen Infrastruktur, Telekommunikation und Verteidigung sowie Regierungsbehörden der USA. Zwei weitere Schwachstellen wurden im Verlauf des Jahres 2021 bzw. 2022 entdeckt. (siehe Kapitel B.14.12 im Anhang)
- Kaseya stellt seinen über 30.000 Kunden Lösungen für die Fernwartung mittels der Software VSA zur Verfügung. Diese Software wurde im Juli 2021 angegriffen, die IT-Angreifer nutzten hierbei Schwachstellen der Fernwartungssoftware, um die Kunden von Kaseya mit Ransomware anzugreifen. Betroffen waren mehr als 1.000 direkte Kunden sowie weitere Kunden, deren Partner, Zulieferer oder Dienstleister die Software VSA von Kaseya nutzten (siehe Kapitel B.13.4 im Anhang).

Klassische Netzwerksysteme wie Router waren auch bereits vor der COVID-19-Pandemie im Fokus von Angreifenden (siehe Kapitel 3.3). Mit der Pandemie wurden insbesondere jedoch Heimnetzwerke zu einem höherrangigen Ziel von IT-Angriffen, sodass neue und potente Schadsoftware für diese Ziele entwickelt und vertrieben wurde:

- Eine dieser Schadsoftware ist der Remote Access Trojaner ZuoRAT, welcher 2022 bekannt wurde. ZuoRAT ist eine komplexe Schadsoftware entwickelt für verschiedene Router von Heimnetzwerken und kleinen Unternehmen zur Installation eines dauerhaften Zugriffs auf die betroffenen Systeme durch die Angreifer. Hierbei nutzt

ZuoRAT Schwachstellen verschiedener Router von Herstellern wie ASUS, Cisco, DrayTek oder NETGEAR und installiert sich auf den entsprechenden Routern. Umfangreiche Routinen zur Analyse von Netzwerken ermöglichen ZuoRAT eine genauere Identifikation der Umgebung um anschließend fortgesetzte Angriffe auf angeschlossene IT-Systeme und den Datenverkehr im Netzwerk auszuführen. Routerangriffe waren vor der Pandemie bereits bekannt, so nutze das Mirai-Botnet seit vielen Jahren mit Schadsoftware infizierte Router. Durch den Trend zum Homeoffice infolge der Pandemie, kamen Router von Heimnetzwerken jedoch mehr in den Fokus. (Kapitel B.14.26)

Neben der Intensivierung von IT-Angriffen auf und über Fernzugriffe, VPNs und u. ä., verschoben sich auch teilweise die Aufgaben und Interessen von APT-Gruppen selbst. So nahm die APT-Gruppe Lazarus im Jahr 2020 Pharmaunternehmen ins Ziel ihrer Angriffe und erzielte mit einem Angriff auf den Hersteller eines COVID-1-Vakzins einen Erfolg in Form von Entwendung von Daten. Auch andere (medizinische) Forschungsunternehmen wurden während der Pandemie gezielt über die Informationstechnik angegriffen. Andere Gruppen nutzten die COVID-19-Pandemie als Aufhänger für ihre Angriffe. So verteilte eine Angreifergruppe Ransomware per postalisch zugestellten USB-Sticks. Manche der Sticks wurden in Geschenkboxen verteilt, andere wurden als Speichermedium für COVID-1-Leitlinien der Gesundheitsbehörden getarnt. (Kapitel B.14.15)

Die meisten Experten erwarten, dass Arbeiten im Homeoffice auch langfristig im Vergleich zum Jahr 2019 einen erheblichen Stellenwert behalten wird, unabhängig vom Verlauf der Pandemie. Damit einhergehend werden die Fernzugriffsmöglichkeiten sowie die Anzahl ausgeführter Fernzugriffe sowohl auf Büro-IT als auch auf leittechnische Systeme zwecks Datenzugriff bzw. Fernwartung langfristig weiter ansteigen. Schon heute werden solche Fernzugriffe auch für Systeme kerntechnischer Anlagen etabliert. Damit ist anzunehmen, dass nicht nur die Infrastruktur für Homeofficearbeiten sondern auch die für Fernzugriffe weiterhin ein Ziel von IT-Angriffen sein werden.

3.9 IT-Angriffe in Zusammenhang mit dem Krieg in der Ukraine

Im Zusammenhang mit dem Krieg in der Ukraine ist es bislang zu zahlreichen IT-Angriffen gekommen. Dies schließt sowohl kriegsbegleitende IT-Angriffe seit Ende Februar 2022 als auch kriegsvorbereitende IT-Angriffe mit ein.

Bereits in der zweiten Jahreshälfte 2021 wurde ein deutlicher Anstieg an IT-Sicherheitsvorfällen in der Ukraine verzeichnet. Seit Ausbruch des Krieges ist es zu einem weiteren, sprunghaften Anstieg gekommen.

Schon seit Jahren kommt es mutmaßlich von russischer Seite zu IT-Angriffen auf ukrainische Ziele. Besonders hervorzuheben sind hierbei IT-Angriffe auf kritische Infrastrukturen mit physischen Auswirkungen:

- So kam es bereits in den Jahren 2015 und 2016 zu gezielten IT-Angriffen auf das ukrainische Stromnetz. Im Dezember 2015 wurden mehrere ukrainische Energieversorgungsunternehmen unter Einsatz der Schadsoftware Black Energy 3 (siehe Kapitel B.7.1) im Anhang) angegriffen. Einige der angegriffenen Unternehmen konnten den Betrieb aufrechterhalten, dennoch waren die physischen Auswirkungen so groß, dass es zu einem mehrstündigen Stromausfall für ca. 225.000 Kunden kam.
- Im Dezember 2016 wurde unter Einsatz der Schadsoftware Crashoverride/Industroyer (siehe Kapitel B.8.1 im Anhang) ein Umspannwerk in Kiew angegriffen, wodurch es zu einem einstündigen Stromausfall im Großraum Kiew kam. Während beide IT-Angriffe von ihrem Effekt her der Demonstration von Fähigkeiten und dem Aufbau einer Drohkulisse zugeordnet werden können, erfüllte der IT-Angriff 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.

Auch in den Folgejahren kam es immer wieder zu IT-Angriffen auf ukrainische Ziele von Angreifern mit mutmaßlich russischem Hintergrund. In dem Jahr vor Beginn der Kriegshandlungen wurde allerdings verstärkt Angriffe festgestellt. So wurden ab März 2022 von ukrainischen Stellen zahlreiche IT-Angriffe 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 IT-Angriffe

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 IT-Angriffe hinaus auch zu IT-Angriffen mit Wipern und anderen destruktiven Schadsoftwarekomponenten auf ukrainische Regierungseinrichtungen und Einrichtungen im IT-, Energie- und Finanzsektor. Zusätzlich wurden auch DDoS-Angriffe in diesen Bereichen durchgeführt:

- Besonders hervorzuheben ist hierbei die Schadsoftware WhisperGate (siehe Kapitel B.14.1 im Anhang), die Berichten /REC22w02/ zufolge vornehmlich gegen Ziele in der Ukraine – darunter Regierungseinrichtungen, Non-profit-Organisationen und IT-Organisationen – eingesetzt wurde. Dabei handelt es sich um einen Wiper, der unter dem Deckmantel eines Ransomware-Angriffs den Master Boot Record des angegriffenen Systems zerstört.

Mit Kriegsbeginn hat sich die Situation weiter verschärft:

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

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

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

Neben IT-Angriffen durch mutmaßlich von staatlichen russischen Stellen unterstützte Angreifergruppierungen ist seit Beginn des Krieges auch die Entfaltung zahlreicher weiterer, kriegsbegleitender IT-Angriffe 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:

- Ein Beispiel ist die Hacktivisten-Gruppierung Killnet (siehe Kapitel B.14.3 im Anhang). Killnet formierte sich vor dem Hintergrund der wachsenden Spannungen zwischen Russland und der Ukraine und trat im Januar 2022 erstmalig in Erscheinung. Seit Beginn des Krieges in der Ukraine fällt die Gruppierung regelmäßig durch prorussisch motivierte IT-Angriffe vornehmlich in Europa auf. Dabei greift sie zumeist zu DDoS-Angriffen, mit denen sie Webseiten, häufig von Regierungseinrichtungen, lahmlegt. Von Killnet angegriffen wurden seit Beginn des Krieges in der Ukraine beispielsweise Ziele in Deutschland, Rumänien, Litauen und Norwegen.
- Umgekehrt hat das Hackerkollektiv Anonymus nach dem Angriff Russlands auf die Ukraine, der russischen Regierung mit Angriffen gedroht und seither diverse IT-Angriffe auf russische Einrichtungen durchgeführt, u. a. den Kreml, das russische Verteidigungsministerium, das Unterhaus der Duma, russische Banken und auch die deutsche Niederlassung des russischen Ölproduzenten Rosneft (siehe Kapitel B.14.4 im Anhang).

Insgesamt ist im Zusammenhang mit dem Krieg in der Ukraine bereits vor Beginn der Kampfhandlungen eine deutliche Zunahme an IT-Angriffen bekannt geworden. Seit Beginn der Kampfhandlungen wurde darüber hinaus ein deutlicher Anstieg bei den bekannt gewordenen IT-Angriffen festgestellt. Seit Kriegsausbruch haben insbesondere strategisch und politisch motivierte IT-Angriffe deutlich zugenommen. Grundsätzlich ist im Hinblick auf bekannt gewordene IT-Angriffe 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 IT-Angriffe, 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 IT-Angriffen bei gleichzeitig geringer werdender Informationslage auszugehen.

3.10 Kollateralschäden

Ein weiter wesentlicher Punkt, der zwar nicht neu ist, durch die Ereignisse im Zusammenhang mit dem Krieg in der Ukraine aber noch einmal deutlicher in den Vordergrund getreten ist, ist das Risiko von Kollateralschäden. Kollateralschäden im Rahmen von IT-Angriffen zeichnen sich analog zu Kollateralschäden bei physischen Angriffen insbesondere dadurch aus, dass neben den eigentlichen Angriffsopfern auch unbeteiligte Dritte Schäden erleiden oder durch Auswirkungen des Angriffs beeinträchtigt werden:

- So waren durch den IT-Angriff auf KA-Sat (siehe Kapitel B.14.2 im Anhang) in Deutschland auch kritische Infrastrukturen betroffen, deren Störung von den Angreifern nicht direkt beabsichtigt gewesen sein dürfte. So war bei tausenden Windkraftanlagen ein Fernzugriff, beispielsweise zu Wartungs- oder Entstörungszwecken nicht mehr möglich. Erst nach einigen Wochen konnte die Kommunikation über KA-Sat mit den Windkraftanlagen stückweise wieder hergestellt werden. Von der Störung betroffen waren teilweise auch Geräte der Gefahrenabwehr wie beispielsweise Satellitenkommunikationssysteme von Einsatzleitfahrzeugen der Feuerwehr, wo die Satellitenkommunikation über KA-Sat in manchen Fällen als Rückfallebene genutzt wird.

- Im kerntechnischen Bereich war beispielsweise das Kernkraftwerk Tschernobyl von den IT-Angriffen mit der Schadsoftware NotPetya betroffen. Dort fiel infolge des IT-Angriffs die Strahlungsüberwachung aus und musste in der Folge manuell durchgeführt werden musste.

Beim Thema Kollateralschäden ist es häufig schwierig, zwischen tatsächlichen, von den Angreifern unbeabsichtigten Kollateralschäden und wissentlich beabsichtigten Folgeschäden des eigentlichen Angriffs zu unterscheiden, da die Angreifermotivation häufig nicht vollständig klar oder nur indirekt ersichtlich ist. Während bei den oben beschriebenen Beispielen recht wahrscheinlich ist, dass die hier angesprochenen Auswirkungen von den Angreifern so nicht beabsichtigt waren, sondern höchstens in Kauf genommen wurden, gibt es auch Fälle, in denen die resultierenden Auswirkungen den Angreifern entweder direkt in die Hände spielten, oder tatsächlich mit beabsichtigt waren. Hierbei handelt es sich dann zwar möglicherweise um Kollateralschäden, möglicherweise aber auch um beabsichtigte Auswirkungen, die den Angreifern beispielsweise weitere Druckmittel liefern:

- Ein Beispiel hierfür ist der Ransomware-Angriff auf den Betreiber der Colonial Pipeline (siehe Kapitel B.13.5 im Anhang), bei dem es zu einer Außerbetriebnahme der gesamten Pipeline, auch Tage über die Zahlung des Lösegeldes hinaus, kam. In der Folge kam es zu Lieferengpässen, sodass aufgrund der Treibstoffknappheit der Flugverkehr an manchen Flughäfen beeinträchtigt wurde. Zudem war in einzelnen Gebieten an bis zu 80 % der Tankstellen kein Benzin mehr erhältlich. In den stark betroffenen Gebieten wurde der Notstand ausgerufen.

Die wenigsten der erfolgreichen IT-Angriffe haben ausschließlich von den Angreifern erwünschte oder beabsichtigte Auswirkungen. Bei Schadsoftwarekomponenten mit der

Fähigkeit, sich selbst zu kopieren, übersteigt die Zahl der infizierten Rechner häufig bei weitem die Zahl der eigentlich anvisierten Rechner. Gleiches gilt auch für IT-Angriffe über die Lieferkette. Diese Auswirkungen sind insbesondere dann von den Angreifern nicht erwünscht, wenn eigentlich ein Angriff im Verborgenen anvisiert war, weil so die Entdeckungsmöglichkeiten deutlich ansteigen. Bei manchen Angreifern kommt es sogar zu erheblichen, von den Angreifern eigentlich nicht beabsichtigten Auswirkungen. Solche Kollateralschäden können in Einzelfällen die tatsächlich gewünschten Auswirkungen deutlich übersteigen. Generell stehen aus Opfersicht die Auswirkungen eines IT-Angriffs im Vordergrund. Ob es sich dabei um beabsichtigte Auswirkungen oder Kollateralschäden handelt, spielt zunächst nur eine untergeordnete Rolle. Der Schaden des eigentlich anvisierten Angriffsopfers und der entstandene (Kollateral-)Schaden kann gleichermaßen erheblich oder u. U. sogar immenser sein.

3.11 APT for hire

Als Advanced Persistent Threat (APT) bezeichnet man typischerweise gut ausgebildete, oftmals staatlich gesteuerte Angreifer, die zum Zweck der Spionage oder Sabotage über einen längeren Zeitraum hinweg sehr gezielt ein System oder Netzwerk angreifen, um Informationen zu sammeln oder Manipulationen vorzunehmen. Von APTs durchgeführte Angriffe sind in der Regel von langer Hand geplant, sehr komplex und erfolgen typischerweise in mehreren Stufen (z. B. Auskundschaftung, Infiltration, Ausbreitung/Rechteeskalation und Exfiltration). Eine APT-Gruppierung kann dabei oftmals auf große zeitliche, personelle und finanzielle Ressourcen und ausgeprägte technische Fähigkeiten zurückgreifen. Häufige Ziele von staatlich geförderten APTs waren bisher kritische Infrastrukturen und generell das Erlangen von vertraulichen Informationen von Unternehmen, Organisationen oder Behörden. In den letzten Jahren wurden zunehmend Entwicklungen beobachtet, die darauf hindeuten, dass APT-Gruppierungen ihre Dienste darüber hinaus aus finanziellem Interesse gegen Bezahlung anbieten (APT for hire). Dabei können Angreifer mit weitaus weniger umfangreichen Ressourcen und technischem Verständnis auf die Fähigkeiten einer solchen Gruppierung zugreifen und diese für vorgesehene IT-Angriffe nutzen. Der Austausch zwischen den Auftraggebern und der APT-Gruppierung kann dabei je nach genauer Konstellation und Bedarf unterschiedlich stark ausgeprägt sein. Beispielsweise können einfache, unspezifische oder aber auf definierte Gegebenheiten angepasste Angriffswerkzeuge ausgetauscht werden. Dies stellt insofern eine ernstzunehmende Bedrohung dar, dass dadurch beispielsweise hochentwickelte Angriffswerkzeuge, die nur durch einen kleinen, technisch hochausgebildeten

Personenkreis entwickelt werden konnten, potenziell einer Vielzahl von Angreifern zur Verfügung stehen, die keine tiefergehenden technischen Fähigkeiten haben müssen, sondern entsprechend darauf zurückgreifen können. Andere Beispiele sind die Nutzung von Angreiferinfrastruktur und die Bereitstellung von spezifischen Informationen.

Zusätzlich zu APT-for-hire-Angeboten kommt es auch immer häufiger dazu, dass APT-Gruppierungen die bei Ransomware-Angriffen (siehe Abschnitt 3.1) eingesetzte Schadsoftware als Ransomware-as-a-Service gegen Bezahlung im Darknet anbieten. Diese Ransomware kann entsprechend unspezifisch sein oder bei Bedarf auf spezifische Gegebenheiten angepasst werden. Beispiele für APT-Gruppierungen, die mutmaßlich Ransomware-as-a-Service anbieten bzw. bereits angeboten haben, sind die mit den IT-Sicherheitsvorfällen des IT-Angriffs auf die Colonial Pipeline und kritische Infrastrukturen im Zusammenhang stehenden Gruppierungen DarkSide (siehe Kapitel B.13.2 bzw. B.13.5) und Black Matter (siehe Kapitel B.13.7). Auch die vor allem für ihre Ransomware-Angriffe auf den Fleischkonzern JBS (siehe Kapitel B.13.10) und den IT-Dienstleister Kaseya (siehe Kapitel B.13.4) bekannte APT-Gruppierung REvil (siehe Abschnitt 3.12.10) bietet Ransomware-as-a-Service-Dienste an.

3.12 APT-Gruppierungen

Hier werden vornehmlich APT-Gruppierungen dargestellt, die in Zusammenhang mit den in Kapitel B des Anhangs beschriebenen IT-Angriffen stehen. Diese Liste ist keineswegs abdeckend.

3.12.1 APT28/Fancy Bear

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

Die APT-Gruppierung APT28 ist spätestens seit 2004 aktiv /BSI21i08/. Sie ist an Verteidigungs- und geopolitischen Informationen interessiert und betreibt Spionage gegen politische und militärische Ziele sowie Regierungen in Georgien und Osteuropa. Nach dem Krieg in Georgien 2008 und aufgrund der Beziehungen des Landes zu westlichen Staaten, führte APT28 Angriffe gegen das georgische Ministerium für innere Angelegenheiten und das Verteidigungsministerium durch. Darüber hinaus zählen zu den Angriffszielen Sicherheitsorganisationen, die in Europa tätig sind, wie zum Beispiel die NATO oder die Organization for Security and Cooperation in Europe (OSCE). Bei einem IT-Angriff auf den deutschen Bundestag im Jahr 2015 wurden von APT28 16 Gigabyte an Daten gestohlen. Zwischen Dezember 2018 und Mai 2020 griff APT28 Netzwerke US-amerikanischer Regierungsbehörden, Bildungseinrichtungen und Unternehmen im Energiesektor an. Nach Angaben des Bundesamtes für Verfassungsschutz (BfV) von 2016, gibt es Hinweise auf Vorbereitungen von Angriffen auf deutsche Energiekonzerne. /FIR14r01, ITE20w01, TAG16w01/

Seit 2019 führt APT28 eine Brute-Force-Kampagne gegen US-amerikanische und europäische Organisationen aus den Bereichen Regierung und Parteien, Militär und Verteidigungsunternehmen, Energie- und Logistikzentren, Universitäten und Medien sowie Anwaltskanzleien durch /BSI21i08/. Ein jüngerer IT-Angriff von APT28 erfolgte im Jahr 2021. Ende September 2021 führte APT28 einen Spear-Phishing-Angriff auf die E-Mail-Postfächer von 1.400 Gmail-Nutzern von Google durch. Ziel des Angriffs war der Diebstahl von Passwörtern, um Zugriff auf die Postfächer zu erhalten und die darin enthaltenen Informationen abzuschöpfen. Diese Informationen sollten dann genutzt werden, um auf die Postfächer weiterer Personen und die darin enthaltenen Informationen zuzugreifen. Der Angriff war zwar global, richtete sich aber gegen einen ausgewählten Personenkreis von Aktivisten, Journalisten, Regierungsmitarbeitern, Menschenrechtlern, Rechtsanwälten und Angestellten im Bereich der Nationalen Sicherheit. Alle schadhaften E-Mails wurden jedoch von Gmail automatisch als Spam-Nachrichten klassifiziert und blockiert. /BSI21i06, MALw03, MOT21w01/

In Verbindung mit dem Ukrainekrieg führt APT28 seit Juni 2022 eine Kampagne durch, die auf Benutzer in der Ukraine abzielt. APT 28 verbreitet ein bösartiges Dokument mit Dateinamen „Nuclear Terrorism A Very Real Threat.rtf“, in dem sich ein Artikel des Atlantic Council vom 10. Mai 2022 mit der Schlagzeile „Wird Putin in der Ukraine Atomwaffen einsetzen? Unsere Experten beantworten drei brennende Fragen“ beinhaltet.

Dabei zielt APT28 auf die Furcht der ukrainischen Bürger vor einem nuklearen Angriff durch Russland ab. Das Dokument beinhaltet das Exploit Follina (CVE-2022-30190), um einen .Net-Stealer herunterzuladen. Der Stealer wird dann eingesetzt, um die Daten der Benutzer aus mehreren gängigen Browsern zu stehlen. /ITD22w01/

APT28 nutzt Spear-Phishing-E-Mails, um Zugriff auf Accounts und Netzwerke zu erhalten. Eine weitere Taktik ist das Vortäuschen von legitimen Nachrichten-, Politik- und anderen Webseiten. Seit 2007 hat die APT-Gruppierung ihre Schadsoftware regelmäßig aktualisiert. Sie besteht aus drei wesentlichen Komponenten, dem Downloader SOURFACE, der Backdoor EVILTOSS und dem modular aufgebauten Schadsoftware-Werkzeug CHOPSTICK. Der SOURFACE-Downloader lädt die Backdoor EVILTOSS, um eine persistente Verbindung zum infizierten Netzwerk herzustellen. Darüber hinaus ermöglicht die Backdoor die Netzwerküberwachung, den Diebstahl von Berechtigungen und die Ausführung von Shellcode. Das modular aufgebaute Schadsoftware-Werkzeug CHOPSTICK bietet zusätzliche, für den Angriff zugeschnittene Funktionalitäten und wirkt als eine weitere Backdoor. Die Anwendung von Reverse-Engineering-Techniken auf die Schadsoftware wird durch diverse Gegenmaßnahmen erschwert. Dazu zählen Laufzeitüberprüfungen zur Identifizierung von Analyseumgebungen, das Entpacken bedeutungsloser Strings während der Laufzeit zur Verschleierung der Funktionalität der Schadsoftware und die Einbindung ungenutzter Maschinenbefehle zur Verlangsamung von Softwareanalysefunktionen. /FIR14r01/

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

3.12.2 APT29/Cozy Bear/Nobelium

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

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

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

3.12.3 APT 38/ Lazarus Group

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

Die erstmaligen Operationen der Lazarus Gruppe waren direkt in den Koreakonflikt eingebettet, mit initialen Angriffen auf südkoreanische Regierungsstellen, Finanzinstitutionen, Medienkonzerne, und weiteren kritischen Infrastrukturunternehmen. Zu diesen Angriffen gehören insbesondere die DDoS-Angriffe im Juli 2009 gegen US-amerikanische und südkoreanische Webseiten unter dem Titel Operation Troy und die im Jahr 2013 durchgeführten IT-Angriffe gegen den südkoreanischen Staat und seine Institutionen. Hierbei wurden bekannte Typen von Schadsoftware wie der Computerwurm Mydoom verwendet, wodurch ein von den Angreifern nutzbares Computernetzwerk aus fernsteuerbaren Bots entstand. Mit diesem Netzwerk wurden massenhaft Anfragen an Webseiten gesendet, wodurch diese temporär nicht verfügbar waren. 2013 wurde mit dem DarkSeoul Wiper eine eigene Schadsoftware der Gruppe gegen südkoreanische

Fernsehsender, Internetanbieter und Banken angewendet. Hierbei wurde nach bisherigen Informationen über ein Update die Schadsoftware an die IT-Systeme verteilt, die Schadsoftware führte dann zu einer vollständigen Löschung aller auf dem IT-System gespeicherten Daten. Durch die Betroffenheit eines Internetanbieters waren Teile Südkoreas mehrere Stunden vom Internet getrennt. /CPO21w01/

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

In den Jahren nach dem IT-Angriff auf Sony-Pictures begann die Gruppe Lazarus nach bisherigen Erkenntnissen mit deutlich verstärkten IT-Angriffen auf Finanzdienstleister, Finanzunternehmen, Besitzer und Handelsbörsen von digitalen Währungen sowie auf Rüstungsunternehmen und genereller Informationsbeschaffung. So führte die Gruppe einen IT-Angriff auf die Zentralbank von Bangladesch aus, bei welchem die Gruppe insgesamt 81 Millionen Dollar erbeutete. Im Jahr 2018 konnte die Gruppe mehr als 530 Millionen Dollar durch einen Angriff auf die japanische Börse Coincheck für digitale Währungen erbeuten. WannaCry, ein sich 2017 schnell verbreitender wurmartiger Erpressertrojaner, wird ebenfalls der Gruppe Lazarus zugeordnet. Dabei wird WannaCry als Fehlschlag angesehen, da die initiale Version aufgrund eines Programmierfehlers keine individuellen Adressen zur Bezahlung des geforderten Lösegelds zur Entschlüsselung erzeugte, sondern drei festgeschriebene und die Erpresser somit keine

individuellen Codeschlüssel automatisch nach Bezahlung verteilen konnten. WannaCry legte hunderttausende IT-Systeme weltweit innerhalb kürzester Zeit lahm und verursachte hohe wirtschaftliche Schäden. Auch die Schadsoftware DTrack, mit welcher insbesondere indische Geldautomaten und damit Bankkunden angegriffen wurden und über 3 Millionen Kreditkartendaten abgegriffen wurden, wird der Gruppe Lazarus zugeordnet. /INT19r01, AVI20r01/

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

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

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

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

Kerntechnischer Bezug

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

3.12.4 Chernovite

Übersicht

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

auszugehen, dass die dahinterstehende Gruppierung Chernovite mindestens seit 2021 aktiv ist. /CIS22r01, DRA22w01, MAN22w01/

Weitere Bezeichnungen

Bislang sind keine weiteren Bezeichnungen der Gruppierung bekannt.

Aktivitäten

Nach Angaben von Dragos wurde Incontroller/Pipedream mit hoher Wahrscheinlichkeit bisher noch nicht für einen IT-Angriff eingesetzt. Die bisherigen Aktivitäten von Chernovite beschränken sich somit nach bisherigen Informationen auf die Entwicklung der IT-Angriffswerkzeuge. Mit diesen hat Chernovite ein leistungsfähiges, offensives ICS-Malware-Framework entwickelt, mit dem die Gruppierung in der Lage ist, industrielle Umgebungen und physische Prozesse in industriellen Umgebungen zu stören, zu beeinträchtigen und potenziell zu zerstören. Incontroller/Pipedream bietet Angreifern konkret beispielsweise Möglichkeiten, Geräte im Netzwerk zu suchen, Passwörter mit Brute-Force-Angriffen zu knacken, Verbindungen zu trennen und Zielgeräte zum Absturz zu bringen, beispielsweise über Denial-of-Service-Angriffe. Auf höchster Ebene bieten die SPS-bezogenen Komponenten von Incontroller/Pipedream Angreifern eine Schnittstelle zur Manipulation entsprechender Zielgeräte. Zu diesem Zweck verwendet Incontroller/Pipedream mehrere verschiedene Protokolle, darunter das von Omron-SPS verwendete FINS, Modbus, OPC-UA[3] und die CoDeSys-Implementierung von Schneider Electric.

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

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

3.12.5 Dragonfly/Energetic Bear

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

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

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

3.12.6 Electrum

Übersicht

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

Weitere Bezeichnungen

Bislang sind keine weiteren Bezeichnungen bekannt.

Aktivitäten

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

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

3.12.7 Erythrite/SolarMarker

Übersicht

Die APT-Gruppierung Erythrite ist seit mindestens Mai 2020 bekannt. Die Aktivitäten von Erythrite zielen vor allem auf die Vergiftung von Suchmaschinen[4] (Suchmaschinen-Poisoning) und den Einsatz von Malware zum Diebstahl von Zugangsdaten und sensiblen Informationen ab. Ein weiteres Ziel ist der Fernzugriff auf OT-Umgebungen. Die IT-Angriffe von Erythrite richten sich vor allem gegen Unternehmen in den USA und Kanada, wobei Angriffe auf die OT-Umgebung eines Fortune-500-Unternehmens sowie auf IT-Netzwerke von Stromversorgungsunternehmen, Lebensmittel- und Getränkeherstellern, Automobilherstellern, IT-Dienstleistern, Öl- und Erdgasunternehmen sowie einem Unternehmen zur Verwaltung elektronischer Verträge und Dokumente (mehrere Millionen Nutzer weltweit) bekannt sind. Schätzungen zufolge waren im Jahr 2021 etwa 20 % der Fortune-500-Unternehmen durch die Angriffe von Erythrite gefährdet. Die Aktivitäten von Erythrite deuten auf einen Sitz der Organisation in Russland hin, wobei Reverse Proxys in Nordamerika und Europa genutzt werden. /DRA22w02, ASI22w01, IND22w01/

Weitere Bezeichnungen

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

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

Aktivitäten

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

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

Bei seinen IT-Angriffen nutzt Erythrite legitime Webseiten, die zur Verbreitung von Malware kompromittiert werden. Dabei werden speziell gestaltete pdf-Dokumente auf ansonsten legitime Webseiten hochgeladen. Diese pdf-Dokumente sind mit Webseiten zur Verbreitung von Malware verlinkt. Zum Hochladen der pdf-Dokumente wird das WordPress-Plugin „Formidable Forms“ verwendet, wobei eine große Menge maliziöser pdf-Dateien hochgeladen werden, die mit tausenden von Schlüsselworten versehen sind. Diese Schlüsselworte wurden für das Crawling durch Suchmaschinen mittels Methoden wie Cloaking[5] oder Link Farming[6] optimiert, um den Seitenrang der manipulierten Webseiten bei einer Suche zu erhöhen. Außerdem wurde eine große Menge weiterer Webseiten kompromittiert oder neu erstellt und mit Links versehen, die auf die maliziösen pdf-Dokumente verweisen. /DRA22w02, ASI22w01/

3.12.8 Kimsuky (teilweise beinhaltet in Hidden Cobra)

Übersicht

Im Oktober 2020 wurde von der Cybersecurity and Infrastructure Security Agency (CISA), dem Federal Bureau of Investigation (FBI) und der U.S. Cyber Command Cyber National Mission Force (CNMF) der USA ein Warnhinweis in Bezug auf die

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

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

nordkoreanische APT-Gruppe Kimsuky veröffentlicht /CIS20i02/. Diese Gruppierung operiert weltweit, mutmaßlich bereits seit 2012, im Auftrag der nordkoreanischen Regierung. Hauptsächlich standen dabei Organisationen und Individuen in Südkorea, Japan und den USA im Fokus der Gruppe, die sich auf die Beschaffung spezifischer und vertraulicher Informationen spezialisiert hat. Kimsuky konzentriert die Aktivitäten nach Angaben der CISA-Meldung neben Think Tanks und der Kryptowährungsindustrie auf südkoreanische Regierungs- und Militäreinrichtungen, außenpolitische und nationale Sicherheitsfragen im Zusammenhang mit der koreanischen Halbinsel, sowie auf die Nuklearindustrie.

Weitere Bezeichnungen

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

Aktivitäten

Die Gruppierung nutzt zur Erlangung des initialen Zugriffs auf das Netzwerk des Opfers neben Phishing-E-Mails mit Login-Sicherheitswarnungen und Watering-Hole-Angriffen überwiegend Spear-Phishing-Techniken, bei denen E-Mails mit schadsoftwarebehaftetem Anhang gezielt an Personen oder Organisationen versendet werden. Dazu werden teilweise auch Ziele außerhalb der eigentlichen Zielgruppe angegriffen, um Schadsoftware auf Subdomains zu platzieren, die legitime Website und Dienste wie beispielsweise Google oder Yahoo-Mail imitieren, um an Zugangsdaten zu gelangen. Außerdem agierte die Gruppierung, um das Vertrauen Ihrer Zielpersonen zu erlangen, in einigen Fällen zunächst über die Kontaktaufnahme via E-Mail ohne Schadsoftwareanhang, wobei eine falsche Identität vorgegeben wurde, bevor weitere E-Mails mit schadsoftwarebehaftetem Anhang oder entsprechende Links gesendet wurden /CIS20i02/. Dabei sind die Spear-Phishing-Angriffe jeweils auf für die Zielperson relevante Themengebiete, wie das nordkoreanische Atomprogramm, Medienanfragen oder aktuell auch die COVID-19-Pandemie /MAL20w01/ ausgerichtet.

Nach der Erlangung des initialen Zugriffs setzt Kimsuky die erstmals im November 2018 beobachtete, auf Microsoft Visual Basic skriptbasierte Malware Babyshark ein. Durch diese wird u. a. zusätzlicher Schadsoftwarecode heruntergeladen und es werden Informationen über das System gesammelt.

Unter Ausnutzung verschiedener Exploits erfolgen zudem die Rechteausweitung und Aktionen zur Umgehung von Schutzmaßnahmen des Systems /TAR13w01/, unter anderem mit Hilfe des open-source Metasploit-Framework /GIT21f01/, einem Werkzeug zur Entwicklung und Ausführung von Exploits.

Im Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines IT-Angriffs wurde, bei dem Informationen in Form von Mitarbeiterdaten und Bauplänen von Kernkraftwerken gestohlen wurden /TRE14w01/. Die Angreifer verwendeten dabei Techniken, die mit dem Angriffsmuster von Kimsuky übereinstimmen. So wurden etwa 6000 E-Mails mit schadsoftwarebehaftetem Anhang an über 3500 Mitarbeiter der Korea Hydro & Nuclear Power Co. gesendet, wobei acht Computer mit Malware infiziert wurden /KIM19r01/. Die Staatsanwaltschaft in Seoul vermutet, dass die Gruppierung Kimsuky für den Angriff verantwortlich ist /PAR15w01/. Nach Informationen des auf Cybersecurity spezialisierten Unternehmens Cyberreason, welches u. a. nordkoreanische Akteure im Bereich IT-Sicherheit beobachtet, hat die Gruppierung ihr Zielgebiet in den vergangenen Jahren zudem neben den USA und dem asiatischen Raum nach Russland und Europa ausgeweitet, wobei insbesondere staatliche Organisationen, nicht-staatliche Forschungsorganisationen, der Sicherheitsrat der Vereinten Nationen und neuerdings auch Organisationen aus dem pharmazeutischen Bereich, die an Impfstoffen und Medikamenten im Zusammenhang der COVID-19-Pandemie arbeiten, im Fokus stehen /CYB20w01/.

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

Im Juni 2021 wurde bekannt, dass es einen Monat zuvor einen Cyberangriff aus Nordkorea auf eine südkoreanische Forschungsorganisation für Nuklearenergie gab.

Dabei wurden nach Angaben eines Abgeordneten aus Südkorea möglicherweise Technologieinformationen gestohlen. Ziel des Angriffs war demnach das Korea Atomic Energy Research Institute, welches sich mit Forschungen und Fragestellungen zur Kernenergie beschäftigt. Die im Zusammenhang dieses Angriffs beobachteten IP-Adressen werden mit der Gruppierung Kimsuky in Verbindung gebracht. /NIK21w01/

3.12.9 Kostovite

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

Die Kostovite genannte Gruppierung wurde erstmalig im Jahr 2021 beschrieben und zeichnete sich durch tiefgreifenden Zugriff auf die Netzwerke von industriellen Steuerungssystemen eines Wartungs- und Betreiberunternehmens im Bereich der erneuerbaren Energien aus. Hierbei nutzte Kostovite eine bis dahin unbekannte Schwachstelle der Pulse Connect Secure (siehe Kapitel B.14.12) um erstmaligen Netzwerkzugriff auf die IT-Netze des betroffenen Unternehmens zu erhalten. Von hier aus eignete sich Kostovite legitime Accountdetails an, um schrittweise im Netzwerk tiefergehende Zugriffe zu erhalten. Schließlich erlangte Kostovite Zugriff auf mehrere leittechnische Systeme und Netzwerke der Kunden des betroffenen Unternehmens. Es wurde bis zur Entdeckung der Zugriffe kein direkter Schaden durch Kostovite verursacht, obwohl der Netzwerkzugriff zur Abschaltung von Anlagen hätte genutzt werden können. Die Datenlage deutet darauf hin, dass Kostovite ein Interesse am langfristigen Netzwerkzugang und dem Erlangen

von Daten und Informationen hatte. Kostovite hatte mindestens einen Monat lang unerkannten Zugriff auf das leittechnische Netzwerk des betroffenen Unternehmens. /DRA21r01/

3.12.10 REvil

Übersicht

Bei der APT-Gruppierung REvil handelt es sich um eine der finanziell profitabelsten Ransomware- und Ransomware-as-a-Service Gruppierungen weltweilt mit jährlichen Umsätzen im Bereich von 100 Millionen US-Dollar, die seit 2019 agiert. Mutmaßlich handelt es sich um eine aus Russland heraus agierende Gruppierung, die sich nach dem Ende der Aktivitäten der APT-Gruppierung GandCrab und möglicherweise aus Mitgliedern dieser Gruppierung gebildet hat. Die eingesetzte Schadsoftware fragt unter anderem die Spracheinstellungen des infizierten Systems ab und wird bei Benutzern mit russischer Spracheinstellung nicht aktiv. Nach der Verschlüsselung der Daten im Falle eines erfolgreichen Angriffs stellt die Gruppierung bzw. der Auftraggeber eine Lösegeldforderung und droht mit der Veröffentlichung von Informationen im Falle der Verweigerung einer Zahlung der Opfer. Wenn die Betroffenen daraufhin weiterhin nicht der Lösegeldforderung nachkommen, startet die Gruppierung typischerweise im dritten Schritt Distributed-Denial-of-Service-Angriffe auf deren Kunden und Geschäftspartner. Im November 2021 gelang es dem US-Justizministerium, mehrere Partner des REvil-Netzes zu verhaften und rund sechs Millionen Dollar an erbeuteten Lösegeldern zu beschlagnahmen. Im Januar 2022 nahmen der russische Inlandsgeheimdienst FSB und die russische Polizei nach eigenen Angaben auf Ersuchen von Behörden der Vereinigten Staaten 14 mutmaßliche REvil-Mitglieder fest und zerschlugen das Netzwerk. Im April 2022 veröffentlichte die Gruppierung auf ihrem Blog jedoch Informationen über zwei neue Opfer und seitdem wurden weitere Angriffe bekannt, sodass davon auszugehen ist, dass die Gruppierung zumindest teilweise weiterhin aktiv ist. /MAL22w03, SEC22w11/

Weitere Bezeichnungen

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

Aktivitäten

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

Zu den von REvil angegriffen Unternehmen zählt mutmaßlich der taiwanische Computerhersteller Acer, der am 14. März 2021 Opfer eines entsprechenden Ransomware-Angriffs wurde. Dabei wurde nicht nur das Verwaltungsnetz von Acer verschlüsselt, sondern auch vorher Daten gestohlen. Die Erpresser forderten 50 Millionen Dollar Lösegeld in Form der Kryptowährung Monero und drohten damit, ggf. die erbeuteten Daten zu veröffentlichen, sollte die Zahlung durch Acer nicht erfolgen. Möglicherweise nutzte REvil bei dem Angriff auf Acer die Schwachstelle ProxyLogon aus, die Teil der 2021 in Microsoft Exchange (siehe Kapitel A.5.1 im Anhang) bekannt gewordenen Schwachstellen ist. Acer äußerte sich nicht zu dem Vorfall. /SPI21w01, HEI21w11/

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

Im Juli 2021 kam es zu einem IT-Sicherheitsvorfall, der weltweit erhebliche Auswirkungen hatte und durch einen Angriff von REvil auf den amerikanischen IT-Dienstleister Kaseya ausgelöst wurde (siehe Kapitel B.13.4 im Anhang). Im Rahmen dieses Ransomware-Angriffs wurde durch die Gruppierung ein schadsoftwarebehaftetes Softwareupdate der Remote-Monitoring und -Management-Tool-Software VSA erstellt und auf die Systeme der Kunden von Kaseya aufgespielt. So waren weltweit tausende Systeme von dem Angriff betroffen und wurden durch die Ransomware verschlüsselt.

Die Lösegeldforderungen für die Entschlüsselung aller Daten beliefen sich auf etwa 70 Millionen Dollar. Nach Informationen des Bundesamts für Sicherheit in der Informationstechnik (BSI) waren auch Unternehmen in Deutschland betroffen. Die Auswirkungen beschränkten sich nicht nur auf direkte Kunden von Kaseya, sondern auch auf Institutionen und Organisationen, deren IT-Dienstleister Kaseya-Produkte einsetzten. Dazu zählte beispielsweise die schwedische Supermarktkette Coop, die in der Folge am 3. Juli 2021 alle 800 Filialen schließen musste, da die Kassensysteme blockiert waren. /VAR21w01/

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

3.12.11 Sandworm

Übersicht

Bei der APT-Gruppierung Sandworm handelt es sich um eine Gruppierung des russischen, militärischen Geheimdienstes GRU /BID20w01, FDD20w01, WIR19w01/, die ihre Aktivitäten bereits 2009 aufnahm /INT20r01/. Sie ist an kritischen Infrastrukturen in Europa und den USA interessiert, wobei sie klassische, strategische Cyber-Spionage betreibt. Darüber hinaus ist die Gruppe auf IT-Angriffe auf industrielle Steuerungssysteme spezialisiert. Aktionen von Sandworm wurden zum ersten Mal 2014 aufgedeckt, als die Schadsoftware Black Energy 2 gegen Telekommunikationsinfrastrukturen der EU und der NATO eingesetzt wurde /SOC20w01, UAG15r01/.

Dabei fanden sich in der Schadsoftware BlackEnergy 2 codierte Referenzen zur Sciencefiction Serie Dune, weshalb der Gruppe der Name Sandworm gegeben wurde /ZDN14w01/. Nach der Entdeckung ihrer Tätigkeiten 2014 trat die Gruppe einige Monate lang nicht in Erscheinung bevor sie am 23.12.2015 /EWB20w01/ wieder einen viel beachteten IT-Angriff durchführte und mit der Schadsoftware Black Energy 3 (siehe Kapitel B.7.1) einen Blackout im ukrainischen Stromnetz verursachte. /FIR16w01/

Weitere Bezeichnungen

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

Aktivitäten

Sandworm war in den letzten Jahren sehr aktiv. Im Juni 2017 wurden immense Schäden mit der Schadsoftware NotPetya (siehe Kapitel B.9.6) in Europa und den USA angerichtet, die ebenfalls dieser APT-Gruppierung zugerechnet wird. Zu den Opfern zählen zum Beispiel die Firmen Maersk und Merck. Am stärksten war jedoch die Ukraine mit 300 Firmen, 22 Banken, vier Krankenhäusern, mehreren Flughäfen und nahezu allen Regierungsbehörden betroffen. Ebenfalls im Jahr 2017 gelang es Sandworm, die Präsidentschaftswahlen in Frankreich zu beeinflussen. Über Phishing-Mails erhielt die Gruppe Zugriff auf neun Gigabyte der E-Mails der Präsidentschaftskampagne von Emmanuel Macron. Im Oktober 2017 erfolgte eine globale IT-Angriffswelle gegen Behörden und Unternehmen. Nach der Behörde für nationale Cybersecurity des Vereinigten Königreichs, dem National Cyber Security Center (NCSC), ist für die Angriffe vermutlich Sandworm verantwortlich. Die Angriffe richteten sich vor allem gegen Organisationen in der Ukraine und Russland. Betroffen waren die russische Nachrichtenagentur, die U-Bahn in Kiew und der Flughafen in Odessa. Weitere Angriffsziele befanden sich in europäischen Staaten (darunter Deutschland), den USA und Japan. Ziel der Angriffe war die Datenverschlüsselung mit anschließender Lösegeldforderung. Im Herbst und Winter 2017 zielte Sandworm auf Südkorea und einige Unternehmen ab, die an den Olympischen Winterspielen in Pyeongchang 2018 beteiligt waren. Dabei infizierten sie einige in Südkorea beliebte Apps für Android-Mobiltelefone wie Transitplan-Apps, darunter auch eine App für Busfahrpläne, koreanische Sprach-Apps sowie Medien- und Finanzsoftware.

Zwei Monate zuvor war dies auch mit einer Version der ukrainischen Mail-App Ukr.net geschehen. Die eingesetzte Schadsoftware konnte sich dann über Android-Telefone verbreiten. /AIR17w01, NCS18i02, TRE17w02, WIR19w01, CSO19w01/

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

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

Im Zuge der russischen Invasion der Ukraine wurde im April 2022 von Sandworm mit der Schadsoftware Industroyer2 ein IT-Angriff gegen das ukrainische Stromnetz durchgeführt. Der Angriff wurde jedoch nach ukrainischen Angaben rechtzeitig entdeckt und Schäden konnten verhindert werden. Die Schadsoftwarekomponente Industroyer2 basiert auf der Schadsoftware Industroyer/Crashoverride, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert. /BSI22i03, BSI22i04, ESE22w01, MAN22w02/

Nach Informationen der NSA /NSA20i01/ nutzt die Gruppe mindestens seit August 2019 eine Schwachstelle im Exim Mail Transfer Agent (MTA) aus. Exim wird häufig in Unix-Systemen verwendet und ist in manchen Linux-Systemen vorinstalliert. Mit Hilfe der Schwachstelle kann ein nicht authentifizierter Angreifer eine spezielle E-Mail senden,

über die er verschiedene Aktionen wie die Installation von Programmen, die Modifikation von Daten und die Erstellung neuer Accounts durchführen kann. So können die Angreifer ihre eigenen privilegierten Nutzer zum E-Mail-Server hinzufügen, Sicherheitseinstellungen des Netzwerks deaktivieren, ihren Nutzern mehr Rechte für den Fernzugriff einräumen und ein Skript ausführen, welches weitere Schritte zur Ausspionierung des Netzwerks ermöglicht. Die infizierten Server dienen als Ausgangspunkt für das weitere Vordringen in andere Netzwerkbereiche. Die Zielobjekte der Angreifer wurden von der NSA allerdings nicht bekannt gegeben. /NSA20i01, WIR20w01/

3.12.12 Tonto Team

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

Dem BSI ist ein Vorfall bekannt, bei dem ein nicht näher genanntes Unternehmen angegriffen wurde, das Software für das Handeln und Verwalten von Wertpapieren entwickelt und für solche Systeme Unterstützungsdienstleistungen anbietet. Dabei soll der Remote Access Trojaner (RAT) Bisonal verwendet worden sein.

Diese Schadsoftware ist bereits seit über zehn Jahren bekannt und wurde im Laufe der Zeit angepasst, um eine Erkennung zu vermeiden /MER20w01/. Neben eigener Schadsoftware verwendet die Gruppierung auch diverse Schadprogramme, die von mehreren weiteren APT-Gruppen gemeinsam genutzt werden. Neben dem Ausspähen von Informationen gehören auch der Up- und Download von Dateien, sowie das Ausführen von Kommandozeilen-Befehlen zu den Funktionalitäten der verwendeten Schadsoftware. Ein Beispiel ist die Nutzung der Schadsoftware ShadowPad, die u. a. bei einem Supply-Chain-Angriff auf das südkoreanische Server-Management Unternehmen NetSarang im Jahr 2017 verwendet wurde.

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

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

Im Juli 2022 wurden Informationen zu einer mutmaßlich von einer chinesischen Gruppierung initiierten Kampagne gegen russische Organisationen zur Informationsbeschaffung über Aktivitäten der russischen Regierung veröffentlicht. Hinter diesen Angriffen steht mutmaßlich die Gruppierung Tonto Team. Die Angreifer nutzen dabei vermeintliche behördliche Empfehlungen in Form von Rich Text Files (RTFs) aus, wobei diese mit Schadsoftware präpariert sind und die Opfer dazu bewegt werden sollen, die Dokumente

zu öffnen und das Ausnutzen von Remote-Code-Execution-Sicherheitslücken in Microsoft Office zu ermöglichen. Die präparierten, in russischer Sprache formulierten Dokumente erwecken den Anschein, dass es sich um Sicherheitswarnungen handelt. Sie geben vor, Behörden und Infrastrukturanbieter vor potenziellen Angriffen zu warnen und auf die Einhaltung der russischen Gesetze hinzuweisen. Obwohl es in der Vergangenheit bereits Angriffe von chinesischen Gruppierungen auf russische Organisationen und Behörden gab, hat die Intensität seit Beginn der russischen Invasion der Ukraine stark zugenommen. /DAR22w01, SEN22w01/

3.12.13 Turla

Übersicht

Die APT-Gruppierung Turla ist für IT-Angriffe zur Cyber-Spionage bekannt. Ziel von Turla ist es dabei, möglichst lange unentdeckt zu bleiben und Informationen zu sammeln. Hierbei setzt sie häufig Spear-Phising-Angriffe, Watering-Hole-Attacken und Living-off-the-Land-Techniken ein. Die IT-Angriffe von Turla richten sich oftmals gegen diplomatische Ziele, wie beispielsweise die Botschaften von Belgien, der Ukraine, China, Jordanien, Griechenland, Kasachstan, Armenien, Polen und Deutschland. /MAL21w04/ Es wurden aber auch eine Reihe anderer Branchen wie Militär, Bildung, Forschung sowie Medizin angegriffen. /MIT21w03/ Die Aktivitäten von Turla deuten auf einen militärischen Geheimdienst hin, der vermutlich in Russland agiert. /HEI20w02/

Weitere Bezeichnungen

Turla ist ebenso unter den Namen Group 88, Belugasturgeon, Waterbug, Venomous Bear, Snake, Krypton, Wraith, Pfinet, TAG_0530, CTG-8875, ATK 13, ITG12, Hippo Team, Pacifier APT, Popeye, SIG2, SIG15, SIG23, Iron Hunter, Makersmark und Uroburos bekannt. Im Zusammenhang mit Turla fällt auch immer wieder der Name WhiteBear, wobei noch nicht klar ist, ob es sich bei WhiteBear und Turla um ein und dieselbe Gruppierung handelt. /CER21w01, MIT21w03, MAL21w04/

Aktivitäten

Turla ist seit mindestens 2004 aktiv. Weltweite Aufmerksamkeit erlangte die APT-Gruppierung spätestens 2014 durch die unter dem Namen Epic Turla bekannt gewordenen IT-Angriffe (siehe B.6.4). Turla ist auch dafür bekannt, immer wieder die

Schadsoftwarekomponenten und IT-Angriffswerkzeuge sowie die Command-and-Control Infrastruktur anderer Angreifergruppierungen zu kapern und bei ihren eigenen Angriffen einzusetzen, wie beispielsweise 2019, als Turla IT-Angriffe auf britische Angriffsziele mit und über IT-Angriffswerkzeuge und Infrastruktur der iranischen APT-Gruppierung APT34 (in diesem Bericht aufgrund der bisherigen Ausrichtung der Gruppierung nicht näher beschrieben) durchführte. Auch wurden 2019 weitere IT-Angriffswerkzeuge von Turla bekannt. /SYM19w01/

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

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

Laut Kaspersky nutzt Turla Tools, die darauf abzielen, das Erkennungsrisiko ihrer Malware zu minimieren. Beispielhaft genannt werden die JavaScript-Malware „KopiLuwak“

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

3.12.14 Xenotime

Übersicht

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

Weitere Bezeichnungen

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

Aktivitäten

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

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

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

4 Zusammenfassung und Fazit

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

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

(Zero-Day-Exploits). Hinzu kommt, dass Schwachstellen in vielen Fällen sehr spät oder gar nicht gepatcht werden, sodass sie auch noch Jahre nach ihrem Bekanntwerden für Angreifer interessant sind und entsprechend ausgenutzt werden. Beispielsweise war die 2010 als Zero-Day-Schwachstelle im Rahmen des IT-Angriffs mit der Schadsoftware Stuxnet bekannt gewordene LNK-Schwachstelle noch Jahre nach Veröffentlichung eines geeigneten Patches die von IT-Angreifern am häufigsten ausgenutzte Einzel-Schwachstelle. Prinzipiell gibt es zwei unterschiedliche Ursachen dafür, dass bereits bekannte Schwachstellen nicht gepatcht werden: Entweder stehen herstellerseitig keine oder noch keine Patches zur Verfügung oder zur Verfügung stehende Patches werden anwenderseitig nicht eingespielt. Für beides gibt es eine Vielzahl von Gründen, die beispielsweise von fehlender Schachstellenbehebung in Alt-Systemen über langwierige Entwicklungszyklen und Genehmigungsverfahren über Nachlässigkeit und Unwissen auf Anwenderseite bis hin zur Einhaltung von Testzeiträumen und Nichtumsetzung aufgrund erfolgter Risiko-Nutzen-Abwägungen reichen. Allein aus dieser beispielhaften Aufzählung wird ersichtlich, dass es trotz der Problematik ungepatchter Schwachstellen eine generelle Kritik am Nicht-Patchen nicht möglich ist, da teilweise dieses Vorgehen auf sorgfältigen, nachvollziehbaren Überlegungen basiert. Grundsätzlich stellt eine ungepatchte Schwachstelle aus IT-Sicherheitssicht aber immer ein Problem dar, das einer Lösung bedarf, gegebenenfalls in Form alternativer Sicherungsmaßnahmen. Ein weiterer, herausfordernder Aspekt im Zusammenhang mit dem Patchen von Schwachstellen besteht darin, dass nicht jeder Patch das zugrunde liegende Problem löst, sondern in manchen Fällen die Problematik nur verschiebt und gleichzeitig mit dem Schließen einer Schwachstelle eine weitere Schwachstelle offenlegt. Dies trifft insbesondere auf in Eile entwickelte Patches zu. Darüber hinaus gibt es immer wieder Schwachstellen, mit deren Ausnutzung weitere, eigentlich bereits gepatchte Schwachstellen wieder zutage treten können, beispielsweise durch das Downgraden von Firm- und Softwareversionen.

In den vergangenen Monaten wurde eine Vielzahl von Schwachstellen in und IT-Angriffen auf Kommunikationseinrichtungen bekannt. Dies betrifft in großer Zahl TCP/IP-Stacks, aber auch Kommunikationsprotokolle, VPN-Verbindungen, Firewalls und Router. Kommunikationskomponenten bieten insgesamt eine große Angriffsoberfläche, gleichzeitig sind kontinuierlich oder temporär bestehende Datenverbindungen weiterhin der Hauptverbreitungsweg für Schadsoftwarekomponenten und maßgeblich für unautorisierte Zugriffe und den Aufbau von Command-and-control-Strukturen. Einzelne Kommunikationskomponenten sind typischerweise stark verbreitet. Schwachstellen und die daraus entstehenden potenziellen Angriffsmöglichkeiten betreffen daher immer eine

Vielzahl von Unternehmen, Einrichtungen und IT-Systemen. Gerade in Bezug auf VPN-Verbindungen und andere Kommunikationskomponenten, die für Remote-Zugriffe eine große Rolle spielen, hat sich die Situation vor dem Hintergrund der Pandemie noch verschärft. Im Zuge der Infektionsschutzmaßnahmen wurde verstärkt auf Arbeit aus dem Homeoffice gesetzt, was häufig zur hastigen Etablierung von Remote-Zugriffsmöglichkeiten geführt hat. Auch bei industriellen Steuerungssystemen wurde in diesem Zusammenhang ein Anstieg bei der Etablierung von Remote-Zugriffsmöglichkeiten festgestellt. Dies wurde und wird von IT-Angreifern ausgenutzt, daher ist die parallele Etablierung geeigneter Sicherungsmaßnahmen unverzichtbar.

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

Neben gezielten Supply-Chain-Angriffen auf ausgewählte Kunden werden häufig auch Supply-Chain-Angriffe beobachtet, die aufgrund des Kundenkreises der betroffenen Hersteller bzw. Zulieferer oder Beratungs-, Wartungs- oder sonstige im Unterauftrag eingesetzte Unternehmen einen sehr hohen Verbreitungsgrad aufweisen. Besonders kritisch sind IT-Angriffe über die Lieferkette dann, wenn davon weit verbreitete Software betroffen ist, die auf IT-Systemen, auf denen sie installiert ist, mit weitreichenden Rechten ausgestattet ist, wie beispielsweise Überwachungs-, Management- oder Antiviren-Software. Dies hat sich in den letzten Monaten besonders deutlich bei den IT-Angriffen über schadsoftwarebehaftete SolarWinds Produkte gezeigt. 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 Footprint beim eigentlichen Angriffsziel kleiner bleibt. Daher sind die Erfolgsaussichten bei Supply-Chain-Angriffen auf gut geschützte Ziele meist deutlich höher als bei direkten IT-Angriffen von außen. Daher muss gerade bei Anlagen und Einrichtungen, die ein hohes Sicherungsniveau in Bezug auf die IT-Sicherheit umgesetzt haben, potenziellen Supply-Chain-Angriffen besondere Aufmerksamkeit gewidmet werden.

Bei Supply-Chain-Angriffen steht das Einbringen von kompromittierter Soft- oder Hardware im Vordergrund. Neben diesem klar ersichtlichen Weg gibt es aber noch einen diffuseren Weg einer Angreifbarkeit oder Kompromittierung über die Lieferkette: den Weg über Abhängigkeiten der eingesetzten, lokal installierten Softwarekomponenten von weiteren, in diese eingebundenen, zentralen Softwarekomponenten wie Bibliotheken. Hier besteht die Problematik häufig darin, dass dem Endanwender im Detail gar nicht bekannt ist, welche der eingesetzten IT-Systeme letztlich welche Abhängigkeiten besitzen. Dies hat sich deutlich bei den Schwachstellen in der Java-Bibliothek Log4j gezeigt, die eine weit verbreitete, häufig eingebundene Funktionalität bereitstellt. Daher war die Angreifbarkeit über die entsprechende Schwachstelle für eine sehr große Anzahl von IT-Systemen prinzipiell gegeben. Es ist bereits jetzt absehbar, dass die Nutzung von externen Softwarekomponenten wie Bibliotheken sich in Zukunft noch verstärken wird. Daher sollte dieser Aspekt der IT-Angriffe über die Lieferkette zukünftig stärker berücksichtigt werden.

Ein weiterer, zunehmend an Bedeutung gewinnender Angriffstyp, ist der Ransomware-Angriff. Gründe hierfür sind sowohl die starke finanzielle Motivation durch die zu erzielenden hohen Lösegeldbeträge als auch die gleichzeitig immer einfachere Möglichkeit, dies durch in Inanspruchnahme von RaaS-Lösungen auch ohne eigene Fachkenntnisse zu erreichen. Trotz der häufig finanziell motivierten Ransomware-Angriffe ist es wichtig zu beachten, dass nicht alle Ransomware-Angriffe darauf abzielen, Geld zu erpressen und danach auch die verschlüsselten Daten wieder zu entschlüsseln. Immer häufiger ist zu beobachten, dass Ransomware ähnlich wie Wiper-Schadsoftware rein destruktiv eingesetzt wird, mit dem Ziel die infizierten Systeme unbrauchbar zu machen. Ein weiterer, immer stärker zutage tretender Aspekt von Ransomwareangriffen ist, dass sich die Erpressung meist nicht auf die Wiedererlangung der verschlüsselten Daten beschränkt, sondern sich zumeist auch auf eine angedrohte Veröffentlichung von im Zuge des Angriffs gestohlenen, sensiblen Daten beziehen. Darüber hinaus erstrecken sich die Drohungen der Angreifer häufig auch mögliche Angriffe auf den Kundenstamm eines Unternehmens. Ein in den letzten Monaten verstärkt beobachteter Trend zeigt zudem, dass besonders erfolgreiche Angreifergruppierungen mehr und mehr auch durch die Hervorrufung von Ausfällen bei verfahrenstechnischen Prozessen den Druck auf die betroffenen Unternehmen noch deutlich erhöhen. Dieser Aspekt wiegt bei Ransomware-Angriffen auf Organisationen im Bereich der kritischen Infrastrukturen besonders schwer.

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

der äußeren Maßnahmen und Barrieren durch einen Angriff über die Lieferkette der industriellen Steuerungssysteme.

Darüber hinaus ist auch ein IT-Angriff mit Hilfe eines – wissentlich oder unwissentlich agierenden – Innentäters denkbar, wobei die ersten beiden Möglichkeiten deutlich häufiger beobachtet werden als letztere. Daher muss neben der Lieferkettenproblematik auch möglichen Einfallstoren, die IT-Angreifern von außen einen Erstzugriff auf die IT-Infrastruktur ermöglichen könnten, besondere Aufmerksamkeit gewidmet werden. Hierbei spielen insbesondere Spear-Phishing-Angriffe, Watering-Hole-Angriffe, Social-Engineering und andere Formen von Credential Harvesting eine große Rolle. Dies ist insbesondere als kritisch anzusehen, da hier auf Mitarbeiter abgezielt wird, die aufgrund von Unachtsamkeit oder durch mangelnde Vorsicht die Aushebelung oder Umgehung von Sicherheitsmaßnahmen ermöglichen können, sodass diese einem potenziellen Angriff nicht mehr oder nur noch unvollständig entgegenstehen. Grundsätzlich zielen viele Angriffstechniken, insbesondere bei den ersten Angriffsschritten auf die Arglosigkeit der Nutzer und den Mangel an IT-Sicherheitsbewusstsein sowie das unzureichende Verständnis für die Vielzahl der Gefahren. Dies unterstreicht, wie essentiell eine Einbeziehung der Mitarbeiter in Sicherungsmaßnahmen und gezieltes Training im Hinblick auf potenzielle Angriffsversuche sind.

Kritische Infrastrukturen sind inzwischen häufig von IT-Angriffen betroffen. Auch rückt die Ausspähung, Manipulation oder Sabotage von industriellen Steuerungssystemen immer stärker in den Fokus von IT-Angreifern. Gerade für und insbesondere in weiterführenden Angriffsschritten ist gezielte Spionage in Bezug auf industrielle Steuerungssysteme keine Seltenheit. Insgesamt sind industrielle Steuerungssysteme zunehmend von IT-Angriffen betroffen. Die beobachteten IT-Sicherheitsvorfälle und IT-Angriffe der vergangenen Jahre zeigen sehr deutlich, dass es eine ganze Reihe von Angreifer-Gruppierungen gibt, die durchaus in der Lage sind, komplexe und über lange Zeiträume unentdeckte IT-Angriffe auszuführen, die – sofern dies zum Ziel der Angreifer zählt – sich auch auf industrielle Steuerungssysteme erstrecken. Hierzu zählen ausdrücklich nicht nur die hier vorgestellten APT-Gruppierungen, sondern neben weiteren APT-Gruppierungen auch andere Typen von Angreifern. In den letzten Monaten hat insbesondere das Bekanntwerden von Incontroller/Pipedream, einem umfangreichen und mächtigen Werkzeugkasten für IT-Angriffe auf industrielle Steuerungssysteme, hier noch einen weiteren Aspekt offengelegt. Incontroller/Pipedream ist nicht nur modular aufgebaut und daher für eine individuelle Anpassung auf einzelne Angriffsziele geeignet, sondern wurde offenbar

gezielt so entwickelt, dass die enthaltenen Werkzeuge auch von Angreifern mit weniger detaillierten Fähigkeiten einsetzbar sind. Damit 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.

In den vergangenen Jahren ist das Feld an Advanced Persistent Threats stetig gewachsen. Zu beobachten sind hierbei teils seit vielen Jahren aktive Gruppierungen, die immer komplexere IT-Angriffe durchführen, aber auch eine hohe Zahl an neueren APT-Gruppierungen. Viele dieser Gruppierungen verbreitern ihren Fokus nach und nach, beispielsweise von einem kritischen Infrastruktursektor auf weitere Sektoren. Wie breit der Fokus der Angreifer ist, hat jedoch nicht zwangsläufig etwas mit den eingesetzten Angriffstechniken und der Zahl der Angriffsziele zu tun. So gibt es Angreifer, die bei einem breiten Spektrum von Angriffszielen äußerst zielgenau arbeiten, während es auch stark fokussierte Angreifer gibt, die nicht vor ersten Angriffsschritten nach dem „Gießkannenprinzip“ zurückschrecken. Insgesamt ist zu beobachten, dass von vielen Angreifern Kollateralschäden durchaus in Kauf genommen werden. Bei manchen IT-Angriffen kommt es sogar zu erheblichen, von den Angreifern vermutlich nicht beabsichtigten Auswirkungen. Dies hat sich in den vergangenen Monaten beispielsweise bei den IT-Angriffen auf die Kommunikation über KA-Sat gezeigt, bei dem die Remote-Zugriffsmöglichkeiten auf tausende Windkraftanlagen in Deutschland nicht mehr verfügbar und auch nicht ohne Weiteres wiederherstellbar waren, obwohl diese Anlagen nach derzeitigen Informationen keineswegs das eigentliche Angriffsziel waren, sondern lediglich ein Kollateralschaden.

Der genannte Angriff auf KA-Sat ist nur ein Beispiel für die große Zahl an IT-Angriffen im Zusammenhang mit dem Krieg in der Ukraine. Bereits vor Beginn der Kampfhandlungen war eine deutliche Zunahme an IT-Angriffen zu verzeichnen. Seit Beginn der Kampfhandlungen wurde darüber hinaus ein deutlicher Anstieg bei den bekannt gewordenen IT-Angriffen festgestellt. Hierzu zählen IT-Angriffe auf kritische Infrastrukturen und Kommunikationskanäle, aber insbesondere auch strategisch und politisch motivierte IT-Angriffe, die nicht nur die Ukraine sondern auch Russland und alle NATO-Partner betreffen.

Grundsätzlich ist davon auszugehen, dass nur ein kleiner Teil der tatsächlich stattfindenden IT-Angriffe publik gemacht wird.

Dies gilt noch verstärkt im Umfeld der kriegerischen Auseinandersetzungen in der Ukraine, da hier die Bekanntmachung erfolgreicher wie auch vereitelter IT-Angriffe, insbesondere auf kritische Infrastrukturen, eine starke politische Dimension hat. Daher ist vor dem Hintergrund des laufenden Angriffskrieges von einer stark verschärften IT-Bedrohungslage und einer Zunahme an IT-Angriffen bei gleichzeitig dünner werdender Informationslage auszugehen. Ähnliches trifft auch auf IT-Angriffe zu, die vor dem Hintergrund anderer schwelender Konflikte und politischer Spannungen stattfinden. Ein Beispiel hierfür ist der IT-Angriff auf drei iranische Stahlkonzerne, bei dem es derzeitigen Informationen zufolge zum Ausbruch eines Feuers und vermutlich erheblichen physischen Schäden gekommen ist.

Prinzipiell zählen auch alle deutschen kerntechnischen Anlagen zu der Art Angriffsziel, auf die sich die Gruppierung der Angreifer mit ihren bisherigen IT-Angriffen und weiteren Aktivitäten konzentrieren könnte. Zudem sind auch in deutschen kerntechnischen Anlagen programmierbare und rechnerbasierte industrielle Steuerungssysteme und -komponenten vorhanden, so dass grundsätzlich hochentwickelte IT-Angriffe auf diese unterstellt werden können. Grundsätzlich bietet die korrekte und vollständige Umsetzung der SEWD-Richtlinie IT aus Sicht der GRS weitreichenden Schutz vor den Gefahren solcher hochentwickelter IT-Angriffe. In deutschen Kernkraftwerken fordert die SEWD-Richtlinie IT eine Trennung zwischen den betrieblichen und sicherheitstechnisch wichtigen Leittechniksystemen durch physische, technische und administrative Maßnahmen. Aus Sicht der GRS ist zunächst davon auszugehen, dass in Anlagen, die ihre IT-Systeme konsequent gemäß SEWD-Richtlinie IT schützen, die Hürden für die Kompromittierung eines sicherheitstechnisch relevanten Systems deutlich höher sind als in vielen anderen kritischen Infrastrukturen, da die IT-Systeme verschiedener IT-Schutzbedarfsklassen konsequenter voneinander getrennt sind. Insgesamt ist allerdings zu beachten, dass auch die korrekte und vollständige Umsetzung der SEWD-Richtlinie IT – oder eines beliebigen anderen Regelwerks zur IT-Sicherheit – zwar einen weitreichenden, aber keinen vollumfänglichen Schutz vor den Gefahren eines langfristig angelegten IT-Angriffs durch eine Angreifer-Gruppierung mit den entsprechenden zeitlichen, finanziellen und personellen Ressourcen bieten kann. Die hier beschriebenen IT-Sicherheitsvorfälle und weiteren Aktivitäten der Angreifer verdeutlichen, dass Strategien zur frühzeitigen Detektion solcher IT-Angriffe und angemessene Maßnahmen zur Reaktion auf entsprechende IT-Sicherheitsvorfälle in diesem Zusammenhang von zentraler Bedeutung für die Sicherheit und Sicherung deutscher kerntechnischer Anlagen sind. Dies wird noch unterstrichen durch eine signifikante Entwicklung der

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

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

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

Quellen

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/BSI21i11/ BSI, Tageslagebericht vom 29.07.2021

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

/BSI22i06/ BSI, Tageslagebericht vom 29.04.2022

/BSI22i07/ BSI, Tageslagebericht vom 14.04.2022

/BSI22r17/ BSI, Tageslagebericht vom 19.05.2022

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/HEI22w15/ Heise Online, Schadcode-Attacken auf Videoueberwachungssystem und NAS von Qnap moeglich, Wichtige Sicherheitsupdates schliessen mehreren Luecken in Netzwerkprodukten von Qnap, 06.05.2022, https://www.heise.de/news, [abgerufen am 08.08.2022]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/NVD18w01/ National Vulnerability Database NVD, CVE 2017-0144 Details, 20 June 2018, nist.gov [abgerufen am 25.01.2021]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/WIR18r01/ Wored, Lily Hay Newman, Inside the Unnerving Supply Chain Attack That Corrupted CCleaner, 208

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

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

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

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

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

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

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

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

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

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

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

Relevante Fachbegriffe

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

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

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

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

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

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

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

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

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

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

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

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

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

Abbildungsverzeichnis

Abkürzungsverzeichnis

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

Anhang

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

A Schwachstellen und IT-Angriffswerkzeuge

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

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

A.1 2017

A.1.1 Brutal Kangaroo – IT-Angriffswerkzeug der CIA

Übersicht

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

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

Beschreibung

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

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

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

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

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

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

Das als Brutal Kangaroo zusammengefasste Set von IT-Angriffswerkzeugen zeigt laut BSI, dass die Realisierung eines Air-Gaps zur physikalischen Trennung schützenswerter Systeme von Netzwerken als alleinige Schutzmaßnahme „unzureichend“ ist. Des Weiteren geht das BSI davon aus „dass weltweit zahlreiche weitere Nachrichtendienste oder kriminelle Organisationen entsprechende Werkzeuge gegen durch Isolation besonders geschützte Systeme entwickelt haben und für zielgerichtete Angriffe einsetzen“. /BSI17i06/

Kerntechnischer Bezug

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

A.2 2018

A.2.1 Meltdown – Schwachstellen in CPUs

Übersicht

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

Beschreibung

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

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

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

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

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

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

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

Kerntechnischer Bezug

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

A.2.2 Spectre – Schwachstellen in CPUs

Übersicht

Im Januar 2018 veröffentlichten Forscher verschiedener Universitäten in Australien, Österreich und den Vereinigten Staaten von Amerika sowie von Googles Project Zero mit dem Paper „Spectre Attacks: Exploiting Speculative Execution“ /KOC18r01/ Informationen zur Sicherheitslücke Spectre, die eng mit der Schwachstelle Meltdown (siehe Kapitel A.2.1) verknüpft ist und auf den gleichen Prinzipien moderner Prozessoren basiert. Spectre nutzt dabei ebenfalls Out-of-Order-Execution, Speculative Execution und Branch-Prediction aus, um unberechtigt Informationen beispielsweise aus dem Speicher anderer ablaufender Prozesse bzw. Programme auszulesen.

Beschreibung

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

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

Um diese Schwachstelle auszunutzen, werden wie bei Meltdown keine weiteren Hilfsmittel benötigt. Angreifer brauchen lediglich eine Zugriffsmöglichkeit auf das System, die es erlaubt, Code auszuführen. Da es sich um eine Hardware-Schwachstelle handelt, kann eine direkte Ausnutzung nicht durch Antivirus-Software verhindert werden.

Diese schützt ggf. lediglich vor Malware oder Viren, die dazu entwickelt wurden, die Schwachstelle auszunutzen. Auch für Spectre haben Entwickler der drei Betriebssysteme Windows, Linux und macOS Anfang 2018 bereits Patches veröffentlicht, die die Ausnutzung der Schwachstelle verhindern sollten. Die Installation der entsprechenden Patches ist auf den von der Schwachstelle betroffenen Systemen die einzige verfügbare Schutzmaßnahme.

Kerntechnischer Bezug

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

A.3 2019

A.3.1 SPPA-T3000 – Schwachstellen in ICS

Übersicht

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

Beschreibung

Bei dem System des Herstellers Siemens mit der Typenbezeichnung SPPA-T3000 handelt es sich um ein betriebliches Leittechniksystem bzw. Prozessleitsystem (Distributed Control System, DCS), welches häufig zur Turbinensteuerung in Kraftwerken aber auch für verschiedene andere Aufgaben zur Steuerung verfahrenstechnischer Prozesse eingesetzt wird /SIE18w01/. SPPA-T3000 wird in einer Vielzahl von konventionellen Kraftwerken eingesetzt, z. B. im Kraftwerk Eemshaven in den Niederlanden sowie fossilen

Kraftwerken in Deutschland, beispielsweise Westfalen D&E, Neurath F&G, GKM 9, Schwarze Pumpe, Altbach, Heilbronn, Lippendorf, Niederaußem K, RDK 8. /SIE15f01/

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

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

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

Kerntechnischer Bezug

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

A.3.2 S7 und PCS7 – Schwachstellen in ICS

Übersicht

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

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

Beschreibung

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

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

Schadcode unerkannt auf dem System ausgeführt werden, ohne dass dies beim Anzeigen des auf der SPS gespeicherten Codes auffallen würde.

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

Kerntechnischer Bezug

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

A.4 2020

A.4.1 Profinet – Schwachstellen in einem Kommunikationsstandard

Übersicht

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

leittechnische Systeme, welche grundsätzlich auf Ethernet basierende Kommunikation unterstützen. Profinet, ebenfalls wie sein Vorgänger Profibus, unterstützen die Kommunikation von Sicherheitsleittechnik bis zu einem Sicherheitsintegritätslevel SIL 3.

Beschreibung

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

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

Kerntechnischer Bezug

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

A.4.2 ABB 800xA – Schwachstellen in ICS

Übersicht

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

Beschreibung

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

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

Mit später veröffentlichten Sicherheitshinweisen wurden mehrere weitere Schwachstellen bekannt, welche ABB 800xA betreffen.

Unter anderem ist das zentrale Lizenzmanagementsystem der ABB betroffen, welches in den meisten ABB Leittechniklösungen, darunter 800xA, verwendet wird sowie die Intersystemkommunikation von 800xA. /ABB20r08/, /ABB20r09/, /ABB20r10/

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

Kerntechnischer Bezug

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

A.4.3 Zerologon – Schwachstelle im Windows Netlogon Remote Protocol

Übersicht

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

Funktionalitäten zur Ausnutzung der Schwachstelle erweitert. Es ist daher davon auszugehen, dass Angriffe auf ungepatchte Systeme durchgeführt werden.

Beschreibung

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

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

Zur Ausnutzung der Schwachstelle ist eine Verbindung zum Netzwerk erforderlich, die entweder lokal (z. B. über einen Innentäter) oder über das Internet (z. B. durch global agierende Angreifer) erfolgen kann. Das BSI hebt in der Sicherheitswarnung die Kritikalität der Schwachstelle hervor, da es eine große Anzahl über das Internet erreichbarer Domänencontroller gibt, die möglicherweise auch nach Veröffentlichung des Updates nicht aktualisiert wurden und somit ungeschützt sind. Außerdem werden die weitreichenden Auswirkungen im Falle einer Kompromittierung herausgestellt. Dass bereits Code-Beispiele zur Ausnutzung der Schwachstelle veröffentlicht wurden, wodurch die Anwendung auch durch nicht spezialisierte Angreifer ermöglicht wird, dass der Code vergleichsweise einfach anzuwenden ist und dass entsprechende Teile des Codes bereits in einschlägige Werkzeuge im Bereich der Cyber-Kriminalität integriert wurden, unterstreicht die Kritikalität. Microsoft beobachtete in diesem Zusammenhang bereits eine Zunahme an Aktivitäten der u. a. bereits in Deutschland agierenden Gruppierung TA505. Außerdem wurden vom Federal Bureau of Investigation (FBI) und der Cybersecurity and Infrastructure Security Agency (CISA) der Vereinigten Staaten von Amerika mehrere Warnmeldungen in Bezug auf die Schwachstelle veröffentlicht.

Demnach wurden Angriffe von Advanced Persistent Threat (APT)-Gruppierungen unter Ausnutzung von Vulnerability-Chaining-Techniken, bei dem mehrere Schwachstellen im Verlauf eines einzigen Angriffs ausgenutzt werden, um ein Netzwerk oder ein System zu kompromittieren, beobachtet, wobei auch die hier genannte Schwachstelle Zerologon verwendet wurde. /CIS20r02/ Laut einer weiteren CISA-Warnmeldung wird die Schwachstelle auch von der APT-Gruppierung Dragonfly/Energetic Bear benutzt, die in der Vergangenheit u. a. bereits Organisationen, Firmen und Anlagen im Energiesektor angegriffen hat. /CIS20r01/ Windows Server werden branchenübergreifend in einer Vielzahl von Firmen, Organisationen und Institutionen eingesetzt. Dem BSI liegen Informationen über die Betroffenheit von sich im Einsatz befindlichen, nicht gepatchten Altsystemen bei Betreibern kritischer Infrastrukturen vor.

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

Kerntechnischer Bezug

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

A.4.4 Amnesia:33 – Schwachstellen in Netzwerkstacks

Übersicht

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

Beschreibung

Im Rahmen der Untersuchungen fand Forescout in vier von sieben untersuchten Stacks Schwachstellen, von denen die Forscher einige als kritisch einstuften.

Die betroffenen Netzwerkstacks werden in einer Vielzahl von IT-, IoT- und OT-Umgebungen eingesetzt und betreffen daher eine ganze Reihe Hersteller, darunter auch den Leittechnikhersteller Siemens. Die Schwachstellen sind unabhängig von der herstellerspezifischen Anwendungssoftware ausnutzbar. Heise /HEI20w01/ nennt unter Berufung auf Forescout folgende Beispiele für potenziell betroffene Gerätetypen:

- IoT (Internet of Things): Kameras, Umgebungssensoren (z. B. Temperatur, Luftfeuchtigkeit), intelligente Beleuchtung, intelligente Stecker, Strichcodelesegeräte, Spezialdrucker, Audiosysteme für den Einzelhandel, Geräte in Krankenhäusern, Sensoren
- OT (Operational Technology): Gebäudeautomationssysteme (GA) wie physische Zugangskontrolle, Feuer- und Rauchmelder, Stromzähler, HVAC (Heating, Ventilation and Air Conditioning (dt. Heizung, Lüftung, Klimatechnik)) und industrielle Steuerungssysteme (ICS) einschließlich beispielsweise PLCs, RTUs, Protokoll-Gateways und Seriell-Ethernet-Gateways, IP Kameras
- IT: Drucker, Switches und WLAN-Access-Points, Server

Forescout veröffentlichte am 7.12.2020 einen detaillierten Forschungsbericht zu Amnesia:33 /FOR20r01/ und gab am 9.12.2020 weitere Details auf der IT-Sicherheitskonferenz Blackhack Europe 2020 bekannt /FOR20f01/. Forescout schätzt die Zahl der von Amnesia:33 betroffenen Hersteller auf über 150 und die Zahl der letztlich betroffenen Geräte auf mehrere Millionen. Bei geeigneter Ausnutzung der bekannt gewordenen Schwachstellen können potenzielle Angreifer beispielsweise Denial-of-Service-Angriffe durchführen oder sensible Informationen auslesen, bei den kritischen Schwachstellen sogar per Fernzugriff und ohne Authentifizierung beliebigen Schadcode auf betroffenen Geräten ausführen /BSI20r03/. Die CISA nennt als konkrete Handlungsmöglichkeiten die Korrumpierung von Speicher, das Auslösen von Endlosschleifen, unautorisierten Zugriff auf Daten und Durchführung von DNS-Cache-Vergiftungsangriffen[7] /CIS20r03/.

Das BSI berichtet, die Ausnutzung der Schwachstellen basiere in allen Fällen auf manipulierten Netzwerkpaketen, die zwischen betroffenem Gerät und IT-Angreifer

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

ausgetauscht werden /BSI20r03/. Die CISA veröffentlichte bereits kurz zuvor ein speziell auf Siemens-Produkte ausgerichtetes ICS Advisory /CIS20r04/ zu den entdeckten Amnesia:33 Schwachstellen. Auch Siemens selbst veröffentlichte ein entsprechendes Security Advisory /SIE20r13/. Eine der 33 bekannt gewordenen Schwachstellen (CVE-2020-13988) betrifft die folgenden Siemens Produkte:

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

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

Kerntechnischer Bezug

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

A.4.5 Ramsay – IT-Angriffswerkzeug für Cyberspionage

Übersicht

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

Kerntechnischer Bezug

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

A.4.6 Schwachstelle in Hirschmann Switchen

Übersicht

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

Beschreibung

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

Die Schwachstelle wurde am 14.02.2020 für Hirschmann Switche bekannt, am 26.02.2020 veröffentlichte Belden mit der HiOS Version 07.0.03 sowie der HiSecOS Version 03.3.00 Updates für alle betroffenen unterstützten Produkte, welche die Schwachstelle behebt. /BEL20r01/, /BSI22r13/

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

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

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

Kerntechnischer Bezug

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

A.5 2021

A.5.1 Microsoft Exchange – Schwachstelle des Microsoft Exchange Servers

Übersicht

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

Beschreibung

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

Vier Schwachstellen sind seit dem 02.03.2021 unter dem Namen ProxyLogon bekannt. Sie ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware. Davon ausgenommen ist Exchange-Online. Für die Durchführung von Angriffen über diese Schwachstellen muss die Möglichkeit bestehen eine nichtvertrauenswürdige Verbindung zu Port 443 des Exchange-Servers aufzubauen. Server ohne nichtvertrauenswürdige Verbindungen oder mit VPN-Verbindung sind zwar gegen einen initialen Angriff

geschützt, haben die Angreifer aber bereits Zugriff auf den Server oder führt ein Administrator eine schadhafte Datei aus, so bieten auch diese Maßnahmen keinen Schutz mehr. Angriffe, bei denen die vier Schwachstellen ausgenutzt wurden, wurden vermutlich von der APT-Gruppierung HAFNIUM durchgeführt, welche im Auftrag der chinesischen Regierung arbeitet. Nachstehend werden die Schwachstellen aufgelistet und ihre Auswirkungen beschrieben /BSI21i03/:

- **CVE-2021-26855**: Diese Schwachstelle ermöglicht einem Angreifer das Senden einer HTTP-Anfrage sowie die Authentifizierung am Exchange-Server. Am 11. März 2021 berichtete Bleeping Computer über eine Ausbreitung der Ransomware DearCry unter Ausnutzung dieser Schwachstelle /BSI21i04/. CVSS-Score: CVSS:3.0 9.1 / 8.4 /MIC21w09/.
- **CVE-2021-26857**: Ermöglicht die Ausführung beliebigen Programmcodes als SYSTEM auf dem Exchange-Server. Dafür werden vom Angreifer Administratorrechte benötigt oder er muss eine weitere, geeignete Schwachstelle ausnutzen. CVSS-Score: CVSS:3.0 7.8 / 7.2 /MIC21w10/.
- **CVE-2021-26858 und CVE-2021-27065**: Über diese Schwachstellen können nach erfolgreicher Authentifizierung Dateien auf den Exchange-Server geschrieben werden. Die Authentifizierung kann über die oben beschriebene Schwachstelle CVE-2021-26855 oder gestohlene Administratorrechte erfolgen. Beide Schwachstellen besitzen den CVSS-Score CVSS:3.0 7.8 / 7.2 /MIC21w11, MIC21w12/.

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

- **CVE-2021-31207**: Diese Schwachstelle ermöglicht es einem Angreifer per Fernzugriff den Authentifizierungsprozess zu umgehen. CVSS-Score: CVSS:3.0 6.6 / 5.8 /MIC21w13/.
- **CVE-2021-34523**: Ermöglicht einem Angreifer die Erhöhung von Zugriffsrechten. CVSS-Score: CVSS:3.0 9.0 / 7.8 /MIC21w14/.

- **CVE-2021-34473**: Die Schwachstelle erlaubt einem Angreifer die Ausführung beliebigen Programmcodes im SYSTEM-Kontext. Der Angreifer benötigt dazu eine Authentifizierung. CVSS-Score: CVSS:3.0 9.1 / 7.9 /MIC21w15/.

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

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

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

Kerntechnischer Bezug

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

A.5.2 NAME:WRECK – Schwachstellen in Netzwerkstacks

Übersicht

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

Beschreibung

Forescout geht von insgesamt mehr als 100 Millionen betroffenen Systemen aus, wobei eine große Anzahl betroffener Siemensprodukte in der Leittechnik der kritischen

Infrastruktur anzunehmen ist. Die Schwachstellen selbst betreffen insbesondere das Domain Name System (DNS) der TCP/IP Kommunikation, welches als Adresssystem beschrieben werden kann. Die Schwachstellen ermöglichen Angreifern die Auslösung von DoS-Bedingungen und auch die Ausführung beliebigen Codes und werden damit als schwerwiegend eingeschätzt. /FOR21r01/

Forescout veröffentlichte ein quelloffenes Script, mit welchem jeder Anwender innerhalb seines Netzwerks herausfinden kann, ob Systeme mit betroffenen TCP/IP Stacks genutzt werden.

Die Anbieter der TCP/IP Stacks, insbesondere Siemens, haben im Vorfeld der Veröffentlichung mit Forescout zusammengearbeitet, sodass für alle Nucleus NET Versionen Sicherheitsupdates bereitstehen. Ob und welche Siemensprodukte betroffen sind und bereits produktspezifische Sicherheitsupdates verfügbar sind, ist zum Zeitpunkt der Berichtserstellung noch nicht bekannt.

Kerntechnischer Bezug

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

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

A.5.3 Schwachstellen in Bachmann Controllern

Übersicht

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

Beschreibung

Die gefundenen Schwachstellen betreffen die M1-Hardware-Controller von Bachmann, die bezüglich des Betriebssystems und der Middleware alle M-Base-Versionen seit

MSYS V1.06.14 verwenden. Das M1-Automatisierungssystem ist das Herzstück aller Systemlösungen von Bachmann, die in den Bereichen erneuerbare Energien wie z. B. Windkraft, Energieverteilung sowie zur Automatisierung im Maschinenbau und Anlagenbau eingesetzt werden. Nachfolgend werden die gefundenen Schwachstellen angegeben und beschrieben: /BSI21i09, BAC22w01/

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

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

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

Kerntechnischer Bezug

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

A.5.4 INFRA:HALT – Schwachstellen in Netzwerkstacks

Übersicht

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

Beschreibung

Seit mehreren Jahren analysiert Forescout verschiedene TCP/IP Stacks auf Schwachstellen und stellt die Veröffentlichungen in umfassenden Berichten der Öffentlichkeit vor.

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

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

Kerntechnischer Bezug

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

A.5.5 Nucleus:13 – Schwachstellen in Netzwerkstacks

Übersicht

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

Beschreibung

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

Siemens veröffentlichte zum selben Zeitpunkt wie Forescout ein Security Advisory, welches die Schwachstellen darstellt. Für alle betroffenen Nucleus Versionen sowie das Nucleus RTOS hat Siemens Updates veröffentlicht, welche die Schwachstellen beseitigen. Die Hersteller von Systemen, welche Nucleus Produkte nutzen (gemäß Siemens mehr als 3 Milliarden IT-Systeme), müssen nun die Updates des Nucleus TCP/IP Stack

oder des Nucleus RTOS mittels eigenen Updates an die Kunden ausliefern. Analog zu den NAME:WRECK Schwachstellen sind weder die genauen betroffenen IT-Systeme noch der aktuelle Stand der individuellen Systemupdates. /FOR21r04/, /SIE21r03/

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen.

Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet. /GRS21r08/

A.5.6 Schwachstellen im DDS Protocol

Übersicht

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

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

Beschreibung

Data Distribution Service (DDS) ist eine sogenannte Middleware, im Schichtsystem der Kommunikation (ISO-OSI Modell) übernimmt Middleware die Aufgabe einer Verteilungsplattform oder eines Protokolls und verteilt bereitgestellte Daten zwischen unterschiedlichen Anwendungen. Industrielle Steuerungssysteme benötigen in den meisten Fällen eine Form von Echtzeitkommunikation, welche sich von der normalen TCP/IP Kommunikation abweichend durch höhere Reaktionsgeschwindigkeiten und Zeitgenauigkeiten

auszeichnet. Mehr als 10 verschiedene Anbieter führen DDS Lösungen zur Implementierung im Echtzeitkommunikationsumfeld an. Es ist daher anzunehmen, dass DDS Lösungen in mehreren Milliarden echtzeitfähigen Geräten in industriellen Steuerungssystemen zur Anwendung kommen. Die 13 Schwachstellen teilen sich auf die DDS Lösungen Fast-DDS, OpenDDS, Connext DDS, CoreDX DDS, Gurum DDS und CycloneDDS und wurden mit einem CVSS Base Score von 6,6 bis 8,7 bewertet. Die Schwachstellen ermöglichen Angreifern unterschiedliche Einwirkungsmöglichkeiten wie das Schreiben von beliebigen Werten in spezifische XML-Dokumente, die Auslösung von Denial-of-Service Bedingungen und die Ausführung beliebigen Codes. Die Anbieter der DDS Lösungen veröffentlichten in Folge des Bekanntwerdens der Schwachstellen Updates, als Supply-Chain Softwareelemente müssen diese Updates jedoch von Anbietern der tatsächlich betroffenen IT-Systeme verarbeitet und schließlich mit eigenen Updates verbreitet werden. Die CISA hat daher eine Reihe von Mitigationsmaßnahmen veröffentlicht, wie der minimalen Zugriffsmöglichkeit im Anlagennetzwerk, der Isolation des leittechnischen Echtzeitnetzes von anderen Netzwerken und Schutzmaßnahmen für Remotezugriffe wie VPNs. /CIS22r02/

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

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

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

Übersicht

Unter dem Namen BadAlloc werden eine Serie von mehr als 25 Schwachstellen in insbesondere bei Echtzeitbetriebssystemen für OT-, IoT- und IIoT-Systeme zusammengefasst. Der Name leitet sich daraus ab, dass die Schwachstellen verschiedene Speicherfunktionen ausnutzen, welche als „Bad Allocation of Memory“ (kurz BadAlloc) bezeichnet

werden. Werden die Schwachstellen ausgenutzt, können Angreifer zum einen Denial-of-Service-Zustände bei betroffenen Geräten auslösen, zum anderen ermöglichen ein Teil der BadAlloc Schwachstellen das Ausführen beliebigen Codes durch Angreifer. /CIS21i01/

Beschreibung

Fehlerhaftes Speichermanagement und damit einhergehende Schwachstellen waren bereits vor den Veröffentlichungen zu BadAlloc ein bekanntes Problem.

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

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

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

Unsichere Allokationen von Speichern sind weit verbreitete Schwachstellen, welche seit Jahrzehnten zu den Hauptgründen für gefundene Softwareschwachstellen zählen. Neuartig an BadAlloc war die von Microsoft gesammelte Untersuchung von verschiedenen

Echtzeitbetriebssystemen und SDKs, welche insbesondere bei IoT-, aber auch bei OT- und IIoT-Systemen Anwendung finden. Zu den betroffenen Echtzeitbetriebssystemen und SDKs gehören sowohl freie als auch kommerzielle Versionen namhafter Anbieter wie Amazon, ARM, BlackBerry, Samsung, Tencent, Texas Instruments, Windriver und viele weitere. Für die meisten betroffenen Betriebssysteme und SDKs stehen Updates bereit, welche die Schwachstellen beheben. Einige betroffene Systeme wie das ARM mbedualloc oder das Texas Instruments SimpleLink MSP432E4 erhalten als veraltete Systeme keine weiteren Updates. /CIS21i01/

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

Kerntechnischer Bezug

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

A.5.8 Siemens SIPROTEC 4

Übersicht

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

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

Beschreibung

Siemens berichtete erstmals am 08.03.2018 in seinem Sicherheits-Advisory SSA-203306: Password Vulnerabilities in SIPROTEC 4 and SIPROTEC Compact Relay Families // von zwei Schwachstellen, die SIPROTEC 4-Schutzrelais betreffen.

Das Advisory wurde am 13.07.2021 zuletzt aktualisiert. Darin wird beschrieben, dass Angreifer über die beiden nachfolgend erläuterten Schwachstellen und über die DIGSI4- und EN100-Ethernet-Kommunikationsmodule der Geräte Autorisierungspasswörter rekonstruieren oder überschreiben können: /SIE18i03/

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

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

Die Cybersecurity & Infrastracture Security Agency (CISA) der USA berichtete in ihrem ICS Advisory (ICSA-18-067-01) /CIS21i02/ ebenfalls über die Schwachstellen. Sie empfiehlt zusätzlich sicherzustellen, dass über das Internet nicht auf die Geräte zugegriffen werden kann, indem das ICS, in dem sich die Geräte befinden, vom Firmennetzwerk getrennt ist.

Es müsse beachtet werden, dass auch VPN-Verbindungen Schwachstellen aufweisen können und nur so sicher wie die miteinander verbundenen Geräte sind. VPN-Server sind regelmäßigen Updates zu unterziehen. /CIS21i02/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

A.5.9 Kameras Geutebrück

Übersicht

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

Beschreibung

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

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

- **CVE-2021-33543**: Fehlende Authentifizierung: Die Schwachstelle erlaubt nicht authentifizierten Remote-Zugriff auf sensible Dateien durch Voreinstellungen bei der Benutzerauthentifizierung. CVSS v3 Base Score: 9.8.
- Bei den sieben Schwachstellen CVE-2021-33544, CVE-2021-33548 und CVE-2021-33550 bis CVE-2021-33554 handelt es sich um Remote Code Execution (RCE) Schwachstellen. Sie ermöglichen einem Angreifer per Remote-Zugriff die Ausführung von beliebigem Programmcode und besitzen jeweils den CVSS v3 Base Score 7.2.

- Die verbleibenden vier Schwachstellen sind ebenfalls RCE-Schwachstellen. Sie ermöglichen einen speicherbezogenen Pufferüberlauf in einem von der jeweiligen Schwachstelle abhängigen Parameter: CVE-2021-33545 (Zähler-Parameter), CVE-2021-33546 (Namens-Parameter), CVE-2021-33547 (Profil-Parameter) und CVE-2021-33549 (Aktions-Parameter). Dadurch ist ein Angreifer in der Lage beliebigen Programmcode per Remote-Zugriff auszuführen. Alle vier Schwachstellen besitzen den CVSS v3 Base Score 7.2.

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

Kerntechnischer Bezug

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

A.5.10 DIAEnergie

Übersicht

Im Jahr 2021 wurde bekannt, dass das industrielle Energiemanagementsystem (EMS) DIAEnergie des Herstellers Delta Electronics mehrere kritische Sicherheitslücken aufweist. DIAEnergie ermöglicht Unternehmen unter anderem die Visualisierung von elektrischen und energetischen Systemen sowie die Überwachung und Steuerung durch manuelle und automatisierte Systeme.

Im letzten Jahr wurde von insgesamt acht Sicherheitslücken berichtet, wobei sechs der acht Sicherheitslücken mit einem CVSS-Score von 9,8 bewertet wurden. Die sich aus den Sicherheitslücken ergebenden Angriffsmöglichkeiten umfassen das Abfangen von Passwörtern im Klartext, das Hinzufügen neuer Benutzer mit Admin-Rechten und das

Ausführen beliebigen Codes auf Basis von SQL-Injections bzw. Dateiupload-Möglichkeiten. /HEI21w12/ Im März 2022 veröffentlichte die CISA einen aktualisierten Sicherheitshinweis DIAEnergie betreffend mit einer Übersicht über diverse Schwachstellen. /CIS22i04/

Beschreibung

Das industrielle Energiemanagementsystem DIAEnergie dient Unternehmen in vielfältigen Bereichen der Überwachung und Steuerung von Anlagen, beispielsweise zur Echtzeitüberwachung und Analyse des Energieverbrauchs, der Optimierung der Anlagenleistung und zur Maximierung der Energieeffizienz. Dazu erstreckt sich das System über weite Anlagenteile und kann über industrielle Netzwerk bis hin zur Feldebene mit einzelnen Komponenten kommunizieren. DIAEnergie kann unter anderem auch für die Fernwartung verwendet werden und lässt sich in verschiedene industrielle Steuerungssysteme (ICS) integrieren. Die Kommunikation findet dabei generell über Modbus bzw. OPC statt. Eine Vielzahl der öffentlich gewordenen Schwachstellen basiert auf sogenannten SQL-Injections, bei denen Sicherheitslücken im Zusammenhang mit SQL-Datenbanken ausgenutzt werden. Eine Sicherheitslücke entsteht dabei durch einen Programmierfehler in einem Programm, das auf die Datenbank zugreift. Dadurch können potenzielle Angreifer zum Beispiel Befehle einschleusen, Daten aus der Datenbank auslesen, Daten unberechtigt ändern oder löschen und ggf. die Kontrolle über den kompletten Datenbankserver übernehmen. /SEC21w16/

Ursprünglich wurde im August 2021 von insgesamt 8 Sicherheitslücken berichtet, woraufhin die CISA eine entsprechende Meldung veröffentlichte. /CIS22i04/ Diese wurde mittlerweile mehrfach aktualisiert und es wurde eine weitere Warnmeldung durch die CISA veröffentlicht, die ebenfalls mehrfach aktualisiert wurde /CIS22r02/. Darin wird berichtet, dass etwa 30 Sicherheitslücken DIAEnergie betreffend gefunden wurden, wobei mittlerweile mit Hilfe von Softwareupdates einige Sicherheitslücken behoben werden konnten. Eine Ausnutzung der Schwachstellen erfordert keine Authentifizierung und ermöglicht es einem Angreifer unter Umständen die vollständige Kontrolle über DIAEnergie und die Systeme zu übernehmen, auf denen es eingesetzt wird. Betroffen sind dabei verschiedene Versionen von DIAEnergie. /SEC21w16/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

A.5.11 Schwachstelle in Johnson Controls Videoüberwachungs- und Zugangskontrollsystem

Übersicht

Am 26.08.2021 veröffentlichte die Cybersecurity & Infrastructue Security Agency (CISA) der USA Informationen zu einer Schwachstelle im Zugangskontroll- und Sicherungssystem CEM Systems AC2000 von Johnson Controls. Zwei weitere Schwachstellen, die das Videoüberwachungssystem ExacqVision von Johnson Controls betreffen, wurden am 07.10.2021 bekannt. Auch über diese Schwachstellen wurde vom CISA berichtet. /BSI21i07/, /CIS21i03/, /CIS21i04/, /CIS21i05/

Beschreibung

CEM-Systems ist ein Anbieter von Zugangskontrollsystemen und vollständig integrierten Sicherheitsmanagementsystemen. Die folgende Schwachstelle hat Auswirkungen auf das Unternehmens-Zugriffskontroll- und integriertes Sicherheitsmanagementsystem AC2000 von CEM Systems, welches von Johnson Controls vertrieben wird. AC200 wird in den USA in den Bereichen kommerzielle Einrichtungen, Petrochemie, Flugzeugverkehr, Bildungswesen und Kritische Fertigung eingesetzt. /BSI21i07/, /JCC20t01/, /JCI21i01/

- **CVE-2021-27663:**

Unter bestimmten Bedingungen wird für Funktionen, die eine prüfbare Nutzeridentifizierung benötigen, keine angemessene Autorisierungsprüfung durchgeführt.

Diese Schwachstelle betrifft nur Nutzer, die die Single Sign On (SSO)-Funktion implementiert und das Application Programming Interface (API) des AC2000 installiert haben und die Programmversionen 10.1 bis 10.5 verwenden. Betroffene sollten sich an den technischen Support des CEM wenden, um das erforderliche Patch zu erhalten. CVSS Base Score: CVSS v3 8.2. /JCI21i01/, /CIS21i03/

ExacqVision ist eine Videoüberwachungslösung von Exacq Technologies, ein Unternehmen, das zu Johnson Controls gehört. Das Produkt umfasst Videomanagementsoftware (VMS), Netzwerk-Videorekorder (NVR) und Speicher-Server. Die beiden folgenden Schwachstellen haben Auswirkungen auf den exacqVision-Internetdienst und den

exacqVision-Server. Der Internetdienst erlaubt Nutzern Videodateien und andere Daten über einen Browser oder über das Mobiltelefon vom exacqVision-Server abzurufen. Durch die Ausnutzung der Schwachstellen können Zugangsdaten gestohlen und das Videoüberwachungssystem außer Funktion gesetzt werden. ExacqVision wird im Bildungs- und Gesundheitswesen, in Unternehmen und im Einzelhandel eingesetzt. /HEI21w05, JCI21i02, JCI21i03/

- **CVE-2021-27664**:

Wenn die Passthrough-Funktion bzw. der nicht authentifizierte Zugriff aktiviert sind, können über den Internetdienst Anmeldeinformationen für andere mit exacqVision verbundene Systeme offengelegt werden. Einem nicht authentifizierten, per Fernzugriff agierenden Nutzer kann auf diese Weise Zugang zu Berechtigungen gewährt werden, welche auf dem exacqVision-Server gespeichert sind. Betroffen sind die Version 21.06.11.0 des exacqVision-Servers und ältere Versionen. Johnson Controls empfiehlt den exacqVision-Server auf Version 21.09. upzugraden. CVSS Base Score: CVSS v3 9.8. /JCI21i02, CIS21i04/

- **CVE-2021-27665**:

Unter bestimmten Einstellungen kann ein nicht authentifizierter, per Fernzugriff agierender Nutzer eine potenzielle Integer-Overflow-Bedingung des exacqVision-Servers in Verbindung mit einem speziell angefertigten Skript ausnutzen, um einen DoS-Angriff durchzuführen. Betroffen sind die 32-Bit-Version 21.06.11.0 des exacqVision-Servers und ältere Versionen. Johnson Controls empfiehlt die 32-Bit-Version des exacqVision-Servers auf Version 21.09. oder auf 64-Bit-Versionen upzugraden. CVSS Base Score: CVSS v3 7.5. /JCI21i03/, /CIS21i05/

Das CISA berichtet in seinen ICS Advisories ICSA-21-238-01, ICSA-21-280-01 und ICSA-21-280-03 über die Schwachstellen und empfiehlt vorbeugende Maßnahmen. Steuerungssysteme, Systeme und Geräte sollten vom Internet getrennt sein, durch Firewalls abgesichert und vom Firmennetzwerk getrennt werden. Bei Fernzugriff auf Systeme sollten Virtuelle Private Netzwerke (VPNs) eingesetzt werden.

Dabei ist zu beachten, dass auch VPN-Verbindungen Schwachstellen aufweisen können und daher immer auf die neueste Version aktualisiert werden müssen. Darüber hinaus sind VPN-Verbindungen nur so sicher wie die über sie verbundenen Geräte. /CIS21i03, CIS21i04, CIS21i05/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

A.5.12 Log4Shell: Kritische Zero-Day Schwachstelle in der Java Bibliothek log4j

Übersicht

Am 09. Dezember 2021 wurden auf der Code-Sharing Plattform GitHub Informationen zur Schwachstelle Log4Shell für die Java Logging-Bibliothek Log4j veröffentlicht. Da die Programmiersprache Java keine eigenen Logging-Funktionen besitzt und Log4j sich in der Vergangenheit als die zentrale Logging-Bibliothek für Java etablierte, besitzt Log4j eine sehr hohe Verbreitung bei Java-basierten Softwaren sowie Systemen. Java selbst ist auf Milliarden von IT-Systemen installiert, neben Bürosystemen auch insbesondere auf Linux-basierten Industriellen PCs (IPCs), (industrial) Internet of Things (IoT/IIoT) Anwendungen und leittechnischen Systeme. /CIS21w03, /APA21w01/

Beschreibung

Log4j wurde im Januar 2001 erstmal vom Entwickler Ceki Gülcü veröffentlicht und seitdem als Open-Source Software von der Apache Software Fondation weiterentwickelt. Da die Programmiersprache Java bzw. das Java Development Kit für Entwickler keine eigenen Logging-Funktionen besitzt, haben sich im Laufe der Zeit eine Reihe von speziellen Frameworks[8] etabliert, mit welchen Logging-Funktionen in auf Java basierender Software und Betriebssystemen integriert werden können.

Log4j ist das weiteste verbreitete Logging-Framework für Java und wird von einer sehr hohen Anzahl an auf Java basierenden Software-Pakete, Firmeware und Betriebssystemen verwendet. Java selbst ist eine von Oracle entwickelt und vertriebene objektorientierte Programmiersprache, welche zu den drei meistverbreiteten Programmiersprachen der Welt gehört. Logger wie Log4j übernehmen bei Implementierung in auf Java

[8] Frameworks, wörtlich übersetzt Rahmenstruktur, beschreiben in der Softwareentwicklung sogenannte Programmiergerüste. Frameworks sind keine allein lauffähigen Softwareprogramme, sondern ermöglichen Programmierern mit Hilfe des Frameworks Anwendungen zu schaffen oder in bestehenden An-wendungen Funktionen zu integrieren.

basierender Software die Aufgabe der Sammlung und Verarbeitung von auflaufenden Meldungen der Software. /CIS21w03, /APA21w01, NVD21w01/

Auf Java basierende Programme senden Nachrichten verschiedener Level an den Logger. Der Logger greift auf sogenannte Levelklassen zurück, mit welchen die aufgelaufenen Meldungen bewertet werden. Eingesetzte Filter ermöglicht eine weitergehende Kontrolle über den Umgang mit Meldungen, mit einem ResourceBundle können optional Meldetexte und andere Informationen mit den Meldungen verknüpft werden. Niederstufig definierte Meldungen und solche Meldungen, die über den Filter definiert werden, werden vom Logger verworfen, alle anderen Meldungen werden an den LogRecorder weitergeleitet, welcher die Meldungen in ein Objekt bindet und an den Handler weiterleitet. Der Handler kann weitere Logik abhängig von den Loglevelns und anderen angewendeten Filtern verwenden. Der Handler wird anhand dieser Logik weitere Nachrichten verwerfen und die übrigen entsprechend den Vorgaben des Formatters in ein bestimmtes Format überführen und über eine Console, einen Bildschirm, eine Datei oder eine andere Ausgabemöglichkeit ausgeben. Die so herausgegebenen Logging-Nachrichten können dann von Nutzern oder Administratoren gelesen werden. /CIS21w03, APA21w01/

Die Log4j Ausgabe ermöglicht die Einbeziehung von Java-Variablen. Die Schwachstelle Log4Shell ermöglicht, dass diese Einbeziehung praktisch unbegrenzt und ohne Rechteabfrage genutzt werden kann, sodass auch externe Java-Bibliotheken über Log4j aufgerufen werden können. In diesen Bibliotheken kann sogenannter Shell-Code[9] integriert werden, welcher dann zur Ausführung beliebigen Codes auf dem betroffenen System führen kann, woher der Name der Schwachstelle Log4Shell stammt. Betroffen sind die Log4j Versionen 2.0 bis 2.14 mit Ausnahme der Version 2.12.2.

Mit dem Update auf Log4j 2.15 wurde am 06. Dezember 2021 die Möglichkeit zur Deaktivierung der der Schwachstelle Log4Shell zugrunde liegenden Befehlsreihen etabliert. Mit dem Update Log4j 2.16 wurden die zugrunde liegenden Befehlsreihen aus dem Code von Log4j vollständig entfernt. In Log4j 2.16 wurden weitere Fehler entdeckt, die mit der Version Log4j 2.17 und anschließend 2.17.1 vollständig behoben wurden.

[9] Shell-Code beschreibt in der Programmierung eine bestimmte Sorte getarnten Codes. Dieser Code wird erst geschrieben, kompiliert, zurückübersetzt und anschließend nachprogrammiert. Man erhält hier-durch einen getarnten Code, welcher in andere Programme integriert werden kann. Ziel ist es mittels dieses Codes ein Kommandozeilensystem wie die Windows-Konsole oder Linux Bash zu starten und schadhaften Code hiermit auszuführen.

Die Version Log4j 2.17.1, veröffentlicht am 28. Dezember 2021, ist nach bisherigen Erkenntnissen frei von allen bekannten Log4j Schwachstellen. /HIS21r01, CIS21w03, /CIS21w04/

Java ist neben dem Consumerbereich auch umfassend in Servern und im leittechnischen Bereich verbreitet, die Verbreitung von Log4j ist durch die umfassende Nutzung von Log4j in Java analog anzusehen. Zu den betroffenen Systemen gehören darüber hinaus Java nutzende Systeme mit eingeschränkter Programmierfähigkeit wie industrielle Steuerungen, SCADA oder DCS Systeme, Systeme im Internet of Things (IoT und II-oT), Netzwerksysteme wie Router und weitere Systeme wie Kameras, Scanner, RFID-gesteuerte Systeme usw.. In einer aktuelle Übersichtsliste werden mehr als 2800 betroffene IT-Systeme von mehr als 100 betroffenen Herstellern von der amerikanischen CISA aufgeführt. Zu den betroffenen Herstellern gehören große und weit verbreitete Hersteller wie ABB /ABB21r01/ Cisco /CIS21w01/ Citrix /CIT21w01/ Emerson /EME21r01/ Phoenix Contact /PHO21r02/ Rockwell Automation /GIT21w02/ Schneider Electric /GIT21w02/ Siemens /SIE21r04/ oder VMware /VMW21r01/.

Die ersten Angriffe über die Schwachstelle fingen spätestens mit dem 01. Dezember 2021 an, die Anzahl der Angriffe hat sich mit der Veröffentlichung am 09. Dezember 2021 drastisch zugenommen. Da die Schwachstelle vollautomatisiert direkt über das Internet angegriffen werden kann, ist ein großer Teil der Angriffslast auf automatisierte Angriffe zurückzuführen. Innerhalb von Netzwerken kann die Schwachstelle zur lateralen Bewegung ausgenutzt werden. Log4Shell ermöglicht damit mit einfachsten IT-Angriffen die vollständige IT-Systemübernahme und wird daher mit einem CVSS Base Score von 10 von 10 Punkten als hoch kritisch bewertet. /AQU21w01/

Zur Mitigation besteht mittlerweile das schwachstellenfreie Update Log4j 2.17.1 bereit. Anbieter müssen für ihre Produkte eigene Patches entwickeln und bereitstellen. Alternativ kann Log4j deaktiviert werden, was zu Funktionseinschränkungen führt. Das ältere Log4j 1 ist nicht von Log4Shell betroffen, jedoch von anderen schwerwiegenden Schwachstellen, für welche keine Updates mehr erscheinen. /HIS21r01, CIS21w03/

Kerntechnischer Bezug

Die GRS ist bekannt, dass Log4J aufgrund seiner enormen Verbreitung u. a. auch in Servern und im leittechnischen Bereich in IT-Systemen kerntechnischer Anlagen eingesetzt wird. Der kerntechnische Bezug der gefundenen Schwachstellen ist dennoch zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Aus Sicht der GRS besteht eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wird der Sachverhalt von der GRS aktuell detailliert ausgewertet. /GRS22r01/

A.6 2022

A.6.1 Incontroller/Pipedream – Set aus ICS-spezifischen IT-Angriffswerkzeugen

Übersicht

Am 13.04.2022 veröffentlichte die US-amerikanische CISA in Zusammenarbeit mit dem FBI, der NSA und dem DoE eine Warnmeldung zu einem ICS-spezifischen Set aus IT-Angriffswerkzeugen „APT Cyber Tools Targeting ICS/SCADA Devices“. /CIS22r01/ Zudem gibt es entsprechende Berichte und Analysen dieses Sets von den IT-Analysten der Firmen Dragos („Pipedream“) /DRA22w01/ und Mandiant („Incontroller“) /MAN22w01/. Es folgten kurze Zeit später Warnmeldungen des BSI /BSI22i02/ sowie weiterer ausländischer CERT-Behörden zu diesem Thema. Dieses Set aus Angriffswerkzeugen ist inzwischen unter den Namen Incontroller und Pipedream bekannt. Es handelt sich um ein hochkomplexes, maßgeschneidertes und sehr breit aufgestelltes Set aus IT-Angriffswerkzeugen, die zum Einsatz gegen industrielle Steuerungssysteme entwickelt wurden. Dragos und Mandiant geben an, ein Sample von Incontroller/Pipedream bereits seit Anfang 2022 untersucht zu haben. Es gibt bisher keine Informationen zu einem aktiven Einsatz von Incontroller/Pipedream. Aus Sicht des BSI erhöht unabhängig vom bisherigen Einsatz die bloße „Existenz von Incontroller/Pipedream das Bedrohungsszenario für ICS-Systeme“. /BSI22i02/ Nach Einschätzung von Dragos wurde Incontroller/Pipedream von staatlich geförderten Angreifern entwickelt. Die verantwortliche Angreifergruppierung, die Dragos unter dem Namen „Chernovite“ (siehe Kapitel3.12.4) führt, zielt vor allem auf die Manipulation von industriellen Steuerungssystemen.

Beschreibung

Bei Incontroller/Pipedream handelt es sich um ein Set aus maßgeschneiderten IT-Angriffswerkzeugen, die auf industrielle Steuerungssysteme zugeschnitten sind. Incontroller/Pipedream ist in der Lage, ein breites Spektrum von PLCs und im industriellen Umfeld gebräuchlicher Software zu beeinflussen. Hierzu zählen insbesondere ausgewählte Controller von Schneider Electric und Omron. Der modulare Aufbau von Incontroller/Pipedream erlaubt es Angreifern, weitere Komponenten zu entwickeln, um das Set für andere leittechnische Komponenten einsetzbar zu machen und PLCs diverser anderer Hersteller anzugreifen. Incontroller/Pipedream nutzt häufige Industrieprotokolle, sodass auch eine potenzielle Interaktion mit anderen leittechnischen Komponenten, die diese Protokolle nutzen, denkbar ist. Zudem erlaubt es Incontroller/Pipedream Angreifern, IT-Angriffe mit hohem Automatisierungsgrad auf die anvisierten Controller durchzuführen, sodass auch weniger spezialisierte bzw. weniger befähigte Angreifer prinzipiell die Kenntnisse und Fähigkeiten hochqualifizierter Angreifer nachahmen können.

Mit Incontroller/Pipedream demonstrieren die dafür verantwortlichen IT-Angreifer signifikante Kenntnisse und Fähigkeiten zur Unterbrechung, Schwächung und potenziell auch Zerstörung von Industrieanlagen und verfahrenstechnischen Prozessen. Die Möglichkeiten, die Incontroller/Pipedream potenziellen IT-Angreifern bietet, stellen eine Bedrohung für die Verfügbarkeit, die Funktion und die Sicherheit von industriellen Steuerungssystemen und verfahrenstechnischen Prozessen dar. Denkbare Szenarien bei einem Einsatz von Incontroller/Pipedream beinhalten beispielsweise:

- Störungen von Controllern in der betrieblichen Leittechnik zur Unterbrechung verfahrenstechnischer Prozesse,
- die Umprogrammierung von Controllern in der betrieblichen Leittechnik zur Sabotage verfahrenstechnischer Prozesse und
- die Deaktivierung von Controllern in der Sicherheitsleittechnik zur Hervorrufung physischer Schäden.

Konkret ist beispielsweise die Manipulation von Drehgeschwindigkeit und Drehmoment von Omron Motoren möglich. Incontroller/Pipedream erlaubt zudem die schnelle Auskundschaftung von industriellen Netzwerken über eine Vielzahl von Mechanismen, die beispielsweise auf MAC-Adressen, Ports, Modbus oder proprietäre Protokolle von Omron bzw. Schneider Elektrik abzielen.

Insgesamt kann Incontroller/Pipedream auch zu IT-Angriffen auf Codesys (Integrierte Entwicklungsumgebung für Speicherprogrammierbare Steuerungen), Modbus (eines der am häufigsten genutzten Industrieprotokolle, De-facto-Standard bei der Kommunikation mit PLCs), Windows-basierte Engineering Work Stations (über eine bekannte Schwachstelle CVS2020-15368 in der weit verbreiteten ASRock Motherboard Utility für BIOS- und System-Updates) sowie Open Platform Communications Unified Architecture (OPC-UA, Standard für Datenaustausch) Server eingesetzt werden. Mit Hilfe von Incontroller/Pipedream sind Angreifer unter anderem in der Lage, ein Anlagennetzwerk auszuspähen, Exchange Web Services (EWS) zu infiltrieren, Controller zu deaktivieren und ihre Programmierung zu manipulieren. Die IT-Angriffswerkzeuge sind zudem deutlich auf das Maskieren als „Trusted Processes“ ausgerichtet und nutzen bei den ICS-spezifischen Modulen keine spezifischen Schwachstellen aus, sondern verwenden legitime Funktionen wie eine legitime Programmierstation. Vor dem Einsatz von Incontroller/Pipedream ist eine Modifikation oder individuelle Anpassung an die anvisierte Umgebung sehr wahrscheinlich, sodass eine spezifische Detektion schwierig ist. Der von Incontroller/Pipedream auf den PLCs platzierte maliziöse Schadcode ist nach Einschätzung von Dragos für normales Monitoring nicht detektierbar. Dragos geht davon aus, dass solcher Schadcode nur durch eine forensische Analyse der Firmware der Controller detektierbar wäre, und sich daher jahrelang unentdeckt auf PLCs befinden kann.

In der untersuchten Version enthält Incontroller/Pipedream die folgenden Komponenten (die meisten IT-Angriffswerkzeuge enthalten wie auch das gesamte Set zwei Namen, wobei einer von Mandiant und der andere von Dragos stammt):

- Codecall/Evilscholar: IT-Angriffswerkzeug für Erkennung von, Zugriff auf, Manipulation von und Abschaltung von Schneider Electric PLCs. Das Modul enthält Modbus und CODESYS Funktionalitäten.
- Omshell/Badomen: IT-Angriffswerkzeug zur Auffindung von, Identifikation von und Interaktion mit OMRON PLCs.
- Tagrun/Mousehole: IT-Angriffswerkzeug zur Interaktion mit OPC-UA Servern.
- Icecore/Dusttunnel: IT-Angriffswerkzeug für Aufklärung und Command-and-Control.
- Lazycargo: IT-Angriffswerkzeug zur Ausnutzung der CVS2020-15368 Schwachstelle in einem Treiber für ASRock Motherboards.

Das Ausmaß der Fähigkeiten von Incontroller/Pipedream deckt eine große Mehrheit der aufgeführten Angriffstaktiken der MITRE ATT&CK ICS Matrix ab, wobei lediglich zur Erlangung des Erstzugriffs andere bzw. weitere IT-Angriffswerkzeuge benötigt werden. Derzeit ist nicht bekannt, welche IT-Angriffswerkzeuge die IT-Angreifer für die initiale Infektion vorgesehen haben. Anhand der Controller-spezifischen Module von Incontroller/Pipedream lässt sich momentan auf eine Ausrichtung auf Anlagen zur Energieversorgung sowie LNG-Anlagen (Liquified Natural Gas) schließen.

Kerntechnischer Bezug

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

A.6.2 ICEFALL

Übersicht

Im Juni 2022 veröffentlichten Forscher des Unternehmens ForeScout unter dem Namen OT:ICEFALL einen Bericht über insgesamt 56 Schwachstellen, die Geräte von zehn Anbietern von OT betreffen. Die Schwachstellen werden in dem Bericht in vier Katego-rien eingeteilt: unsichere technische Protokolle, schwache Verschlüsselung oder fehlerhafte Authentifizierungsverfahren, Fehler in Firmware-Updates und Remote-Code-Ausführung über native Funktionen. Angreifern mit Netzwerkzugriff zu einem betroffenem Gerät ermöglichen diese Schwachstellen unter anderem die Remote-Ausführung von Code, Veränderungen an der Logik, an Daten oder der Firmware von OT-Geräten und Denial-of-Service-Angriffe. Die betroffenen Geräte sind für ihren Einsatz in kritischen Infrastrukturen wie beispielsweise der Öl-, Gas, Chemie- und Nuklearindustrie sowie Stromerzeugung bekannt und werden als „Secure by Design“ bzw. zertifiziert mit entsprechenden OT-Sicherheitsstandards angesehen. Das BSI wurde vor der Veröffentlichung des Berichts über die Schwachstellen informiert und veröffentlichte diesbezüglich Informationen am 23.06.2022. Die CISA veröffentlichte einen entsprechenden Sicherheitshinweis am 22.06.2022. /BSI22r13/, /CIS22r03/, /FOR22r01/

Beschreibung

Ein wesentlicher Aspekt, der im OT:ICEFALL-Bericht aufgegriffen wird, ist die Tatsache, dass für Operational Technology in der Vergangenheit oftmals wesentliche Grundzüge der Praxis „Security by Design“ nicht angewendet bzw. vernachlässigt wurden, was dazu geführt hat, dass es diverse Schwachstellen in OT-Geräten gibt, die beispielsweise mit sehr alten Protokollen kommunizieren, keine Schutzmechanismen besitzen und generell eine schlechte allgemeine Sicherheit aufweisen. Demnach gab es bisher t in der Regel für OT-Schwachstellen keine Common Vulnerabilities and Exposures (CVE) Meldungen, da allgemein bekannt war, dass OT-Protokolle und Kommunikation entsprechend unsicher sind. Aufgrund dieses Sachverhalts ist nach Einschätzung des BSI die Gefahr groß, dass ein Angreifer, der Zugriff auf ein Prozesssteuerungsnetz (SCADA-Netz) hat, beliebige Befehle ausführen kann, wodurch es beispielsweise zu einem temporären Ausfall kritischer Dienstleistungen kommen kann. Das BSI geht davon aus, dass eine dauerhafte, physische Schädigung schwieriger zu realisieren ist, da diese genaue Kenntnisse des Prozesses voraussetzt und oft zusätzlich analoge Schutzmaßnahmen etabliert sind. Nach Angaben des BSI haben bereits einige der betroffenen Hersteller auf den Bericht reagiert und Patches bereitgestellt. Die im Bericht genannten Geräte stammen von den Herstellern Bently Nevada, Emerson, Honeywell, JTEKT, Motorola, Omron, Phoenix Contact, Siemens und Yokogawa und entsprechend verwundbare Geräte wurden in Deutschland mit Hilfe der Suchmaschine Shodan gefunden worden (Honeywell Saia Burgess, Phoenix Contact DDI und ProConOS SOCOMM). Neben der Veröffentlichung der entsprechenden CVEs wurden von der CISA außerdem diverse Industrial Control Systems Advisories (ICSAs, Sicherheitshinweise zu industriellen Steuerungssystemen) bezüglich der Schwachstellen veröffentlicht. Die genauen Auswirkungen der einzelnen Schwachstellen hängen maßgeblich von den jeweiligen Funktionalitäten und genauen Einsatzbedingungen ab. Im Bericht sind fünf allgemeine Angriffsmöglichkeiten durch Ausnutzung der Schwachstellen angegeben:

- Remote Code Execution, bei der Angreifer beliebigen Code auf das betroffene Gerät aufspielen und ausführen können (für die Erlangung der vollständigen Kontrolle über das Gerät ist darüber hinaus ein Überschreiben der Firmware erforderlich),
- Denial-of-Service, wobei ein Angreifer den Zugriff auf die Funktion eines Geräts blockiert bzw. dessen Verfügbarkeit einschränkt,
- Datei-/Firmware-/Konfigurationsmanipulation, bei der ein Angreifer wichtige Komponenten bzw. gespeicherte Daten oder die Firmware manipuliert,

- Kompromittierung von Anmeldeinformationen, wobei Angreifer Anmeldeinformationen erlangen, da diese ungesichert gespeichert sind oder übertragen werden und
- Umgehung der Authentifizierung, bei der Angreifer in der Lage sind, bestehende Authentifizierungsmaßnahmen zu umgehen.

Als Mitigationsmaßnahmen werden Im Bericht unter anderem Updates der betroffenen Geräte mit entsprechenden Patches und die Einhaltung gängiger, elementarer Sicherungsmaßnahmen im Bereich Cybersicherheit empfohlen.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

A.6.3 Retbleed – Schwachstellen in CPUs

Übersicht

Forscher der Eidgenössischen Technischen Hochschule Zürich haben Informationen zu einer Schwachstelle in Intel- und AMD-Prozessoren veröffentlicht, die ähnlich wie die Spectre-Schwachstellen (siehe Abschnitt A.2.2) auf spekulativer Codeausführung (siehe Abschnitte A.2.1 undA.2.2) beruht. Bei Ausnutzung der „Retbleed“ genannten Schwachstellen können Daten bzw. Datenfragmente von Angreifern unberechtigt aus dem Speicher ausgelesen werden. Den Retbleed-Schwachstellen wurden die CVE-Einträge CVE-2022-29900 bzw. CVE-2022-29901 (für AMD- und Intel- Prozessoren) zugeteilt. Google entwickelte 2019 die Kompiliertechnik „Retpoline“ zum Schutz vor Spectre-artigen Angriffen, was unter anderem Teil der Windows 10 Sicherheitsupdates im Mai 2019 war. Mit Retbleed ist es möglich, die Sicherheitsmaßnahmen der zum Schutz vor Spectre entwickelten Sicherheitsupdates zu umgehen. Das BSI sieht in Retbleed ein Gefährdungspotenzial vergleichbar mit den Spectre-Schwachstellen. /HEI22w13/, /BSI22r14/

Beschreibung

Retbleed umgeht die Sicherheitsmaßnahmen, die im Zusammenhang mit Spectre-artigen Angriffen entwickelt wurden, durch die geschickte Gestaltung von Return-Kommandos. Dadurch können Datenfragmente aus vermeintlich geschützten RAM-Speicherbereichen ausgelesen werden. Dies ist bei Retbleed mit sehr geringen

Geschwindigkeiten von 219 Bytes pro Sekunde für Intel-Prozessoren und 3,9 KByte pro Sekunde für AMD-Prozessoren möglich. Die Forscher haben die Funktionalität für die AMD-Prozessoren AMD Zen1, Zen1+ und Zen 2 und für die Intel-Prozessoren der Generation 6, 7 und 8 erfolgreich getestet. Dabei griffen die Forscher auf Linux-Systeme zurück, wobei angemerkt wurde, dass das grundlegende Problem auf der Hardware-Ebene der betroffenen Prozessoren liegt und auch Microsoft Windows und Apple bzw. MacOS Systeme betroffen sind. Nach Ansicht der Forscher ist Retbleed insbesondere für virtuelle Maschinen mit geteilter Hardware, zum Beispiel bei Cloud-Systemen, relevant. Es wurden bereits mitigative Maßnahmen entwickelt, die jedoch zu Performance-Einbußen im Bereich von 14 % bis 39 % führen. /COM22w02/, /WAT22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.4 SpringShell – Schwachstelle in der Java Bibliothek Spring

Übersicht

Am 31. März 2022 wurde durch VMware die kritische Schwachstelle SpringShell (häufig Spring4Shell) in der Java Bibliothek Spring MVC und Spring WebFlux öffentlich gemacht. Die als CVE-2022-22965 bekannt gewordene Schwachstelle betrifft analog zu Log4Shell eine weit verbreitete Bibliothek der Programmiersprache Java. Das Spring Framework ist eine umfassende unterstützende Bibliothek, um grundlegende programmiertechnische Infrastruktur in Java-Applikationen zu integrieren, wodurch Java-Programmierer Zeit und Aufwand im Rahmen der Programmierung sparen können. Java selbst ist auf Milliarden von IT-Systemen installiert, neben Bürosystemen auch insbesondere auf Linux-basierten Industriellen PCs (IPCs), auf Systemen im (industrial) Internet of Things (IoT/IIoT) und leittechnischen Systemen. /VMW22w01/, /SPR22W01/

Beschreibung

Das Framework Spring wurde erstmalig im Oktober 2002 in seiner ursprünglichen Version von Rod Johnson entwickelt und wird mittlerweile als Open-Source Software von VMware verwaltet. Als Framework zur Unterstützung der Programmierung in Java bietet Spring eine Vielzahl von Funktionalitäten an und ist gemäß VMware Millionenfach in

Endnutzergeräten verbreitet. Im März 2022 kamen Gerüchte zu einer kritischen Schwachstelle in einer Java Bibliothek auf. Tatsächlich analysierten Sicherheitsforscher bereits länger eine kritische Schwachstelle in der Bibliothek Spring für Java, welche dann kurzzeitig über einen Proof of Concept Bekanntheit gewann und dann am 31. März 2022 offiziell als CVE-2022-22965 vom Hersteller veröffentlicht wurde. SpringShell wird aufgrund der Analogien zu Log4Shell auch Spring4Shell genannt und betrifft die Spring Versionen 5.3.0 bis 5.3.17, 5.2.0 bis 5.2.19 sowie ältere Versionen. Unter bestimmten Umständen kann SpringShell auf betroffenen Systemen insoweit ausgenutzt werden, dass beliebiger Code in Form von Shellcode ausgeführt werden kann und damit Vertraulichkeit, Verfügbarkeit und Integrität der Systeme beeinflusst werden kann. Zur Nutzung der Schwachstelle muss das betroffene Java Programm auf dem System im Java Development Kit 9 oder höher entwickelt worden sein, es muss eine bestimmte seltenere Form von Java Container für das Programm angewendet werden und es müssen die Abhängigkeiten spring-webmvc oder spring-webflux angewendet werden. Mit den Spring Versionen 5.3.18 sowie 5.2.20 stehen seit dem 31.März 2022 aktualisierte Versionen von Spring zur Verfügung. /VMW22w01/, /SPR22W01/

Hauptbetroffene Software ist Apache Tomcat, ein Open-Source Webserver mit hoher Verbreitung. Apache Tomcat wird vielfältig in IT- und auch OT Umgebungen eingesetzt, mit der Version 10.0.20 steht eine Version ohne SpringShell Schwachstelle bereit. /SPR22w01/

Besondere Aufmerksamkeit erfuhr SpringShell durch die Ähnlichkeit zur wenige Monate früher bekannt gewordenen Log4Shell Schwachstelle. Beide Schwachstellen betreffen populäre Java Bibliotheken, beide Schwachstellen werden als kritisch angesehen (Log4Shell mit einem CVSS Score von 10 von 10 Punkten, SpringShell mit einem CVSS Score von 9,8 von 10 Punkten) und beide Schwachstellen ermögliche die Ausführung beliebigen Codes bei geringem Aufwand durch die Angreifer. Analog zu Log4Shell wurde auch SpringShell als Schwachstelle noch vor der offiziellen Warnung des Herstellers bekannt, jedoch nicht in der Intensität wie die von Log4Shell.

Der große Unterschied zwischen beiden Schwachstellen ist, dass die SpringShell Schwachstelle nur beim Zusammenkommen von mehreren Bedingungen ausgenutzt werden kann und nicht wie Log4Shell grundsätzlich bei jedem betroffenen System. Bisher sind keine umfassenden Angriffsserien auf Java Systeme mit Spring Bibliothek bekannt geworden. /VIA22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.5 Schwachstelle in Schneider Electric Easergy P3 und P5

Übersicht

Vier Schwachstellen betreffen die Mittelspannungsschutzrelais Easergy P3 und P5 von Schneider Electric. Sie ermöglichen Angreifern den Datenverkehr in ICS-Netzwerken zu beobachten und Schadsoftware in die Netzwerke einzuschleusen.

Beschreibung

Im Januar 2022 informierte Schneider Electric seine Kunden über Schwachstellen in Mittelspannungsschutzrelais. Bezüglich der Schwachstellen erfolgte im März 2022 eine Warnmeldung der Cybersecurity & Infrastructure Security Agency (CISA) der USA. Sie betreffen die Schutzrelais Easergy P3 und P5 und werden mit dem Bedrohungsgrad „hoch“ eingestuft. Erhalten IT-Angreifer Zugriff auf den fest codierten SSH-Schlüssel des Geräts, können sie auf das mit dem Gerät verbundene ICS-Netzwerk zugreifen und dessen Datenverkehr beobachten sowie Schadsoftware in das Netzwerk laden. Die Schwachstellen werden nachstehend angegeben. /HEI22w11, SEC22w10/

Die folgenden drei Schwachstellen betreffen die Schutzrelais Easergy P5 /SCH22i01, CIS22i03/:

- **CVE-2022-22722**: Hart codierte Anmeldeinformationen können zur Offenlegung von Informationen führen. Ein Angreifer, der den kryptografischen SSH-Schlüssel für das Gerät und die Kontrolle über das lokale Betriebsnetzwerk erhält, kann den mit der Produktkonfiguration verbundenen Datenverkehr beobachten und manipulieren. CVSS v3.1 Base Score: 7.5
- **CVE-2022-22723**: Kopien des Speicherpuffers ohne Überprüfung der Speichergröße können zu einem Überlauf des Puffers führen, der Programmabstürze und die Ausführung beliebigen Codes verursacht, falls speziell gestaltete Datenpakete an das

Gerät gesendet werden. Schutz- und Auslösefunktionen über GOOSE[10] können beeinträchtigt werden. CVSS v3.1 Base Score: 8.8

- **CVE-2022-34758**: Eine fehlerhafte Eingabevalidierung kann dazu führen, dass die Watchdog-Funktion des Gerätes deaktiviert wird, falls ein Angreifer Zugriff auf privilegierte Benutzeranmeldeinformationen hatte. CVSS v3 Base Score: 5.1

Die drei Schwachstellen können durch Updates der Firmware auf die Versionen 01.401.101 und 01.303.202 geschlossen werden. Auf welche der beiden Versionen die Firmware zu aktualisieren ist, hängt von der auf dem Gerät installierten Firmware ab. Um das geeignete Firmwareupdate zu erhalten, ist eine Anfrage bei Schneider Electric erforderlich. Falls Kunden nicht das Firmwareupdate für die Schwachstelle CVE-2022-22723 nutzen möchten, können sie die GOOSE-Anwendung des Gerätes deaktivieren, um das Risiko zu minimieren. Ist dies nicht möglich, sollte das Gerät nur in einem sicheren lokalen Netzwerk eingesetzt werden. /SCH22i01/

Die folgende Schwachstelle betrifft Easergy P3 Schutzrelais /SCH22i02/:

- **CVE-2022-22725**: Kopien des Speicherpuffers ohne Überprüfung der Speichergröße können zu einem Überlauf des Puffers führen, der Programmabstürze und die Ausführung beliebigen Codes verursacht, falls speziell gestaltete Datenpakete an das Gerät gesendet werden. Schutz- und Auslösefunktionen über GOOSE können beeinträchtigt werden. CVSS v3.1 Base Score: 8.8

Die Schwachstelle wird durch ein Update der Firmware auf Version 30.205 geschlossen. Um das Update zu erhalten, ist eine entsprechende Anfrage an Schneider Electric zu stellen. Für die GOOSE-Anwendung gelten die gleichen Empfehlungen wie für die Schwachstelle CVE-2022-22723. /SCH22i02/

Die betroffenen Schutzrelais werden in Kraftwerken und im elektrischen Stromnetz eingesetzt.

Angreifer können Schutzrelais käuflich erwerben und auf die Schwachstellen untersuchen. Über Spear-Phishing-E-Mails können sie Zugriff auf das Büronetzwerk eines

[10] GOOSE steht für Generic Object Oriented System-Wide Events. Ziel von GOOSE ist es, die herkömmliche festverdrahtete Logik, die für die Koordination innerhalb der Relais erforderlich ist, durch die Kommunikation zwischen Station und Bus zu ersetzen. /SCH11w01/

Unternehmens erhalten, das die Relais in seinen ICS-Netzwerken einsetzt. Bei ungünstiger Netzwerkarchitektur können die Angreifer den Zugriff vom Büronetzwerk auf das ICS-Netzwerk ausweiten. Sie haben dann die Möglichkeit Spannungsversorgungen von Geräten und Schutzeinrichtungen abzuschalten, so dass auch physische Schäden an anderen Geräten entstehen können. /SEC22w010/

Kerntechnischer Bezug

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

A.6.6 TL Storm 2.0, Schwachstelle in Aruba und Avaya Switches

Übersicht

Aruba und Avaya sind Anbieter von Netzwerktechnologien für Unternehmen und bieten insbesondere Switches und andere Komponenten zum Aufbau von LAN, Wide Area LANs und VLANs an. Am 03.05.2022 wurden von Sicherheitsforschern des Unternehmens ARMIS mit einem unter TLStorm 2.0 genannten Whitepaper insgesamt fünf Schwachstellen in verschiedenen Netzwerktechnologien der Unternehmen Aruba und Avaya der Öffentlichkeit bekannt gemacht. Die auf der Supply-Chain basierenden Schwachstellen werden durch die Nutzung von spezifischen externen Bibliotheken ermöglicht und wurde von ARMIS als schwerwiegend bis kritisch eingestuft. /ARM22r01/

Beschreibung

Im März 2022 veröffentlichte ARMIS einen Bericht zu kritischen Schwachstellen in SMART-UPS™ unterbrechungsfreien Stromversorgungen (USV) des Unternehmens APC (Tochter von Schneider Electric). Die TLStorm genannten Schwachstellen betrafen mit Cloud-Funktionen ausgestattete USV und ermöglichten die Ausführung beliebigen Codes durch IT-Angreifer. Die Schwachstellen basierten auf einer fehlerhaften Implementierung der TLS[11] Bibliothek Mocana nanoSSL, welche zur Sicherung der Anbindung

[11] TLS steht für Transport Layer Security und ist der Nachfolger von SSL, dem Secure Sockets Layer. TLS ist ein Verschlüsselungsprotokoll für Datenübertragungen und dient der sicheren Kommunikation in Netzwerken wie auch dem Internet.

der USVs an die APC Cloud dient. Mittels der Schwachstellen ist es den Angreifern möglich, die USVs bis zur physischen Zerstörung zu manipulieren. Am 03. Mai 2022 veröffentlichte ARMIS mit TLStorm 2.0 einen Bericht zu Netzwerksystemen, welche ebenfalls die Bibliothek Mocana nanoSSL für TSL Verschlüsselungen nutzen. Zur Implementierung der Mocana nanoSSL Bibliothek müssen die Anwender einer genauen Dokumentation folgen. Ein Beispiel für die Folgen solcher Fehlimplementierungen ist ein schwerer Fehler, der zur Ausführung beliebigen Codes durch Angreifer führen kann, wenn Anwender bei der Implementierung von nanoSSL einen Codezeilenkommando missachten. In den Netzwerkswitchen von Aruba wurden die Schwachstellen CVE-2022-23677 und CVE-2022-23676 entdeckt, welche mit einer CVSS Base Score von 9,0 und 9,1 als schwerwiegend bewertet wurden. Die Schwachstellen betreffen mehrere Interfaces der Aruba-Geräte und ermöglichen Angreifern die Ausführung beliebigen Codes. In Netzwerkswitchen von Avaya wurden die kritischen Schwachstellen CVE-2022-29860 und CVE-2022-29861 mit je einem CVSS Base Score von 9,8 und eine kritische, nicht nummerierte Schwachstelle von nicht mehr unterstützten Baugruppen (legacy Systemen) entdeckt. Mithilfe der bekannt gewordenen Schwachstellen können die genannten Netzwerkkomponenten vollständig übernommen werden und es kann Einfluss auf den Netzwerkverkehr genommen werden wie auch die Ausbreitung in Netzwerken ermöglicht werden. Für alle betroffenen, noch von den Herstellern unterstützten IT-Systeme wurde von Aruba und Avaya Updates bereitgestellt. Die Geräte sind weltweit in Unternehmen und Behörden im Einsatz, eine Ausnutzung der Schwachstellen ist jedoch nicht bekannt geworden. /ARM22r01, ARM22r02/

Schwachstellen in Softwarebibliotheken sind in den letzten Jahren vermehrt festgestellt worden, wobei die TLStorm Schwachstellen der nanoSSL Bibliothek insbesondere wegen der hohen Verbreitung von nanoSSL auf Interesse stießen. TLStorm basiert jedoch nicht auf direkten Schwachstellen der Softwarebibliothek, sondern ausschließlich auf einer nicht vollständig korrekten Implementierung, wodurch Schwachstellen entstehen. Im Gegensatz zu Log4Shell sind daher nur eine geringe Anzahl von Herstellern betroffen. /ARM22r01/, /ARM22r02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

A.6.7 SATAn

Übersicht

Im Juli 2022 veröffentlichten Forscher der Ben-Gurion-Universität in Israel ein Konzeptpapier, in dem eine Methode vorgestellt wird, mit der es möglich ist, Informationen aus einem mit Hilfe eines AirGaps gesicherten IT-Systems durch die Verwendung von Radiosignalen über SATA-Kabel zu extrahieren. Bei Serial ATA (SATA) handelt es sich um eine Schnittstelle für den Datenaustausch mit Festplatten und anderen Speichergeräten, die weit verbreitet ist. Die Forschergruppe hat neben der in dem Konzeptpapier vorgestellten Methode in der Vergangenheit weitere Veröffentlichungen publiziert, die sich mit der Überwindung von AirGaps durch verschiedene Methoden (USB-Kabel, Monitor-Kabel oder Ethernet-Kabel als Antennen, Geräusche von Festplatten, Temperaturschwankungen eines PC-Systems usw.) befassen. Der Schwerpunkt der Forschungsarbeiten liegt dabei nicht auf der Überwindung von AirGaps zur Erlangung des Zugriffs oder Platzierung von Schadsoftware, sondern auf der Extraktion von Daten über AirGaps. /HEI22w14/, /HEI21w13/

Beschreibung

Die Forscher zeigen in dem veröffentlichten Konzeptpapier, wie ein SATA-Kabel als Funkantenne missbraucht werden kann, um Informationen zu übertragen. Dazu wurde auf einem präpariertem System eine entsprechende Schadsoftware installiert, sodass das SATA-Kabel während Lese- und Schreiboperationen Daten im Bereich von 5.9995 und 5.996 GHz übertragen hat und somit als Antenne zweckentfremdet wurde. Es wurde eine Datenübertragungsrate von 1 Bit/s erreicht, wobei die erzielte Sendeleistung so gering war, dass sich der Empfänger in einem Abstand von maximal 1,2 m befinden musste. Auch wenn sich die Reichweite eines derartigen Angriffs vermutlich durch Verbesserungen der Empfangstechnik erhöhen lässt, schätzt das BSI die praktische Anwendbarkeit des Angriffs als gering ein, da dazu zunächst eine entsprechende Software auf das über ein AirGap abgeschottete System platziert werden muss.

Zudem werden in Anbetracht der Tatsache, dass kompromittierende Abstrahlungen von Computersystemen seit längerem bekannt sind, durch das BSI entsprechende Vorgaben für d kritische Computersystemen erstellt.

Dennoch zeigt unter anderem diese Veröffentlichung, dass es Möglichkeiten zur Überwindung von AirGaps gibt und dass es Forschungsarbeiten und auch erste erfolgreiche praktische Demonstrationen diesbezüglich gibt. /BSI22r15/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Weitere Bearbeitung

Aus Sicht der GRS besteht derzeit keine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen, diese kann zukünftig jedoch nicht ausgeschlossen werden.

A.6.8 Schwachstellen in GPS-Trackern

Übersicht

Im Juli 2022 veröffentlichte das BSI einen Tageslagebericht mit Informationen zu sechs teilweise kritischen Schwachstellen in GPS-Trackern der Firma MiCODUS /BSI22r12/. Zuvor wurde bereits ein ICS-Advisory zu dieser Thematik veröffentlicht /CIS22i01/, welches sich auf einen Untersuchungsbericht der IT-Sicherheitsfirma BitSight /BIT22r01/ bezieht, von welcher die Schwachstellen entdeckt worden sind.

Beschreibung

Im Rahmen der Untersuchungen fand BitSight sechs teilweise kritische Schwachstellen im GPS-Tracker mit der Typenbezeichnung MV720 des chinesischen Herstellers MiCODUS. Dieser GPS-Tracker wird festverdrahtet in Fahrzeugen eingebaut und hat neben einer Ortungsfunktion die Fähigkeit zur Fernsteuerung, zum Geofencing oder zum Aktivieren einer Kraftstoffsperre. Hauptsächlich wird der GPS-Tracker als Fahrzeugortungsgerät für Flottenmanagement und Diebstahlschutz eingesetzt. Der GPS-Tracker kann über ein Webinterface oder eine Handy-App gesteuert werden. Die Kommunikation mit dem GPS-Tracker erfolgt über einen dedizierten TCP-Port (7700) oder via SMS.

Die verfügbaren Dienste für den GPS-Tracker werden von einem einzigen Webserver gehostet, wobei die Kommunikation zwischen dem Browser und diesem Webserver verschlüsselt erfolgt, alle anderen Verbindungen wie z. B. für die Handy-App aber im Klartext erfolgen. /BSI22r12/, /BIT22r01/

In dem von BitSight veröffentlichten Forschungsbericht /BIT22r01/ werden folgende Schwachstellen genannt:

- Verwendung eines hartkodierten Masterpasswortes (kritische Schwachstelle): Es wird ein hartkodiertes Masterpasswort für die Kommunikation zwischen der Handy-App und dem Webserver verwendet, welches es einem Angreifer ermöglicht, sich auf dem Webserver anzumelden und sich als Benutzer auszugeben. Somit könnte ein Angreifer direkte SMS-Befehle an den GPS-Tracker senden, die so aussehen, als kämen sie von der Handynummer des legitimen Besitzers. Unter Ausnutzung dieser Schwachstelle hätte ein Angreifer die Möglichkeit, vollständige Kontrolle über den GPS-Tracker zu erlangen, inklusive Zugriff auf Standortinformationen, Routen, Tracking-Standorte sowie z. B. die Möglichkeit des Aktivierens der Kraftstoffsperre.

- Möglichkeit, SMS-basierte Befehle ohne Authentifizierung zu senden (kritische Schwachstelle): Es besteht die Möglichkeit des Servers, SMS-Befehle direkt an den GPS-Tracker zu senden. Damit sieht es so aus, als ob diese Nachricht direkt vom mobilen Gerät des Administrators kommt. Befehle können dabei zum Teil ohne Eingabe eines Passwortes gesendet werden, wodurch beispielsweise die IP-Adresse des Administrator-Webservers geändert werden kann. Unter Ausnutzung dieser Schwachstelle könnten Angreifer beispielsweise die volle Kontrolle über den Datenverkehr erlangen.

- Alle Geräte sind mit einem Standardpasswort „123456“ vorkonfiguriert (hoch eingestufte Schwachstelle). Während der Installation erfolgt keine verbindliche Forderung, dass dieses Passwort geändert werden muss. Bei den Untersuchungen hat BitSight festgestellt, dass viele Nutzer ihr Passwort nicht geändert haben, da Sie im Installationsprozess nicht dazu gezwungen werden. Unter Ausnutzung dieser Schwachstelle könnten Angreifer einfach auf GPS-Tracker zugreifen.

- Cross-Site-Scripting-(XSS)-Schwachstelle des Webservers (hoch eingestufte Schwachstelle): Aufgrund dieser XSS-Schwachstelle werden Daten in unsicherer Weise in die Antwort auf eine Anfrage eingefügt. Bei einer Kontrolle des Skriptes

durch einen Angreifer kann dies dazu führen, dass der GPS-Tracker kompromittiert werden kann. Unter Ausnutzung dieser Schwachstelle könnten Angreifer die vollständige Kontrolle über den GPS-Tracker und die verschickten Informationen erlangen.

- Insecure Direct Object Reference (IDOR) Schwachstelle des Webservers (hoch eingestufte Schwachstelle): Der Webserver hat eine authentifizierte IDOR-Schwachstelle im Parameter „Device ID“. Es handelt sich um eine Schwachstelle in der Zugriffskontrolle, die auftritt, wenn eine Anwendung vom Benutzer bereitgestellte Eingaben verwendet, um direkt auf Objekte zuzugreifen. Aufgrund dieser Schwachstelle werden beliebige Geräte-IDs ohne weitere Überprüfung akzeptiert. Unter Ausnutzung dieser Schwachstelle könnten Angreifer auf Daten von jeder Geräte-ID in der Server-Datenbank zugreifen, unabhängig vom angemeldeten Nutzer.
- IDOR-Schwachstelle für POST-Parameter (mittel eingestufte Schwachstelle): Für den Parameter „Device ID“ ist es möglich, dass nicht authentifizierte Nutzer Excel-Berichte über die Geräteaktivität erstellen. Aus diesen geht beispielsweise hervor, wo und wie lange ein Fahrzeug angehalten hat.

Laut /BSI22r12, BIT22r01, CIS22i01/ könnten Angreifer durch ein erfolgreiches Ausnutzen dieser Schwachstellen die Kontrolle über jeden MV720 GPS-Tracker erlangen und damit beispielsweise Zugriff auf Standorte und Routen sowie die Möglichkeit zum Absperren des Kraftstoffs und dem Entschärfen von Alarmen erhalten. Potenziell kann ein Ausnutzen dieser Schwachstellen katastrophale, mitunter lebensbedrohliche Folgen haben. Beispielsweise könnte einer kompletten Flotte der Kraftstoff entzogen oder die Fahrzeuge überwacht und abrupt gestoppt werden. Außerdem besteht die Möglichkeit einer Forderung nach Lösegeld für die Wiederherstellung der Betriebsbereitschaft.

Laut /BIT22r01/ werden die betroffenen GPS-Tracker in 169 Ländern neben Privatpersonen auch von diversen Organisationen genutzt. Insgesamt sind ca. 1,5 Millionen Geräte bei ca. 420.000 Kunden installiert, u. a. in Fortune-50-Energieunternehmen, beim nationalen Militär in Südamerika, nationalen Regierungen und Strafverfolgungsbehörden in Westeuropa sowie einem ausländischen Kernkraftwerksbetreiber. Die Auswertung der ca. 2 Millionen hergestellten Verbindungen zwischen dem Webserver und den GPS-Trackern für den Zeitraum Mai 2021 bis Februar 2022 hat ergeben, dass die meisten Verbindungen in den GUS-Staaten hergestellt wurden. In Deutschland wurden weniger als 5.000 dieser Verbindungen hergestellt.

Deshalb kommt /BSI22r12/ zu dem Schluss, dass die Schwachstellen zwar grundsätzlich als kritisch einzuordnen sind, dass sie aber keine besondere Relevanz in Deutschland haben.

Es ist allerdings aus den Unterlagen nicht zu entnehmen, welche Organisationen konkret betroffen sind. Laut /CIS22i01/ wird empfohlen, die Verwendung der betroffenen GPS-Tracker zu deaktivieren, bis eine Behebung der Schwachstellen erfolgt ist. Ob und wann diese erfolgt, ist momentan nicht absehbar, da der Hersteller trotz mehrfacher Kontaktversuche nicht in ausreichendem Maße reagiert hat. Laut /BIT22r01/ ist es zudem wahrscheinlich, dass auch andere GPS-Tracker des Herstellers MiCODUS von den Schwachstellen betroffen sind.

Kerntechnischer Bezug

Der kerntechnische Bezug der gefundenen Schwachstellen ist zum jetzigen Zeitpunkt nicht vollständig abzuschätzen. Es besteht die Möglichkeit, dass GPS-Tracker beispielsweise in Fahrzeugen zum Transport von kerntechnischem Material eingesetzt werden können und diese damit gezielt angegriffen werden können.

A.6.9 Schwachstellen in Videoüberwachungssystemen und Network Attached Storage von QNAP

Übersicht

Im Jahr 2022 wurden vier Schwachstellen bekannt, die die Videoüberwachungssysteme und NAS (Network Attached Storage[12]) der Firma QNAP betreffen und von QNAP als kritisch eingestuft wurden. Sie ermöglichen einem Angreifer die Ausführung von beliebigem Programmcode sowie die Durchführung von DoD-Angriffen und können zu Vertraulichkeits- und Integritätsverlust führen.

[12] NAS (Network-Attached Storage) Systeme sind IT-Systeme, welche eine hohe Festplattenkapazität an ein Netzwerk anschließen, um so einen von verschiedenen IT-Systemen zugreifbaren Speicherort zu bieten. NAS-Systeme können rein in lokalen Netzwerken betrieben werden, aber je nach Einsatzgebiet auch über das Internet angesteuert werden. Zugriffe auf NAS-Systeme erfolgen entweder über direkten Netzwerkzugriff auf die Speicher der Systeme oder aber über HTML-Anwendungen.

Beschreibung

QNAP (Quality Network Appliance Provider) ist ein Unternehmen mit Hauptsitz in Taipeh, welches Hardware- und Softwarelösungen im Bereich Speicher, Netzwerke und Smart Videoüberwachung anbietet.

Zudem stellt QNAP für seine Nutzer eine Cloud basierte NAS Lösung zur Verfügung. Im Jahr 2022 wurden vier von QNAP als kritisch eingestufte Schwachstellen bekannt, die die Videoüberwachungssysteme und NAS von QNAP betreffen. Sie werden nachfolgend aufgelistet. /QNA22w01, HEI22w15/

Eine kritische Schwachstelle betrifft Netzwerk Videorecorder, die QVR Videoüberwachungssysteme verwenden /QNA22w01, QNA22i01, NIS22i01/:

- **CVE-2022-27588**: Die Schwachstelle ermöglicht einem Angreifer per Fernzugriff beliebige Befehle auszuführen. Sie besitzt einen Base Score CVSS v3.1 von 9.8. Durch ein Update des Systems auf die Firmwareversion QVR 5.1.6 build 20220401 oder höher, wird die Schwachstelle geschlossen.

Drei weitere kritische Schwachstellen betreffen das Netzwerkprotokoll Samba (SMB), das den Zugriff auf Daten über ein Computernetzwerk ermöglicht und Datei- und Druckdienste für Windows-Clients bereitstellt /QNA22w01, QNA22i02, NIS22i02, SUS22i01/:

- **CVE-2021-44141**: Von dieser Schwachstelle sind alle Samba-Versionen vor 4.15.5 betroffen. Ein böswilliger Nutzer kann einen Server-Symlink[13] verwenden, um festzustellen ob eine Datei oder ein Verzeichnis in einem Bereich des Server-Dateisystems vorliegt, der nicht unter der Freigabefunktion exportiert wurde und so ein Informationsleck herbeiführen. Dafür muss SMB1 mit Unix-Erweiterungen aktiviert sein. Base Score CVSS v3.1: 4.3.
- **CVE-2021-44142**: Betroffen sind die Samba-Versionen vor 4.13.17, 4.14.12 und 4.15.5 mit konfiguriertem vfs_fruit. Ein Angreifer mit Schreibzugriff auf erweitere Dateiattribute kann aus der Ferne beliebigen Programmcode ausführen. Base Score CVSS v3.1: 8.8.

[13] Ein Symlink ist ein symbolischer Link. Es handelt sich um eine Verknüpfungsdatei, die sich auf eine physische Datei oder einen physischen Ordner bezieht. /JOE22w01/

- **CVE-2022-0336**: Samba AD DC überprüft beim Hinzufügen von Service Principal Names (SPNs) zu einem Benutzerkonto, dass diese nicht mit den SPNs übereinstimmen, die bereits in der Datenbank existieren. Diese Überprüfung kann umgangen werden, wenn durch eine Kontoänderung ein SPN erneut hinzugefügt wird, der zuvor bereits auf diesem Konto vorhanden war. Ein Angreifer kann dies für einen DoD-Angriff ausnutzen, indem er einen SPN hinzufügt, der einem vorhandenen Dienst entspricht. Darüber hinaus kann ein Angreifer sich als bestehender Dienst ausgeben, was zu einem Vertraulichkeits- und Integritätsverlust führt. Base Score CVSS v3.1: 8.8.

Um NAS bezüglich der drei Schwachstellen abzusichern, empfiehlt QNAP die Deaktivierung von SMB1 und ein Update der Firmware des Systems auf die aktuelle Version /QNA22i02/.

Kerntechnischer Bezug

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

B IT-Sicherheitsvorfälle und IT-Angriffe

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

Wie schon einleitend beschrieben, werden diese Ersteinschätzungen der GRS zu diesen IT-Sicherheitsvorfällen und IT-Angriffen immer wieder an die vorliegenden Informationen angepasst, um weitere Aspekte ergänzt und bei Bedarf vollständig überarbeitet. Sie sind daher Bestandteil eines lebenden Dokuments und nicht als abgeschlossen zu verstehen.

Neben den IT-Sicherheitsvorfällen und IT-Angriffen, für die bereits eine Ersteinschätzung vorgenommen wurde, sind hier auch solche Vorfälle und Angriffe gelistet, deren Auswertung im aktuell laufenden Vorhaben nicht durchgeführt werden konnte, aber im Rahmen des geplanten Anschlussvorhabens erfolgen wird. Dabei handelt es sich sowohl um kürzlich bekannt gewordene IT-Sicherheitsvorfälle und IT-Angriffe, als auch um ältere Vorfälle und Angriffe, die für die IT-Bedrohungslage relevant sind und deren Aufarbeitung nach und nach erfolgt. Der Zeitpunkt, zu dem ein IT-Sicherheitsvorfall oder IT-Angriff bekannt wird, hat keinen Einfluss auf dessen Bedeutung für die IT-Bedrohungslage, daher ist es für ein möglichst vollständiges Verständnis der IT-Bedrohungslage ausschlaggebend, alle bislang bekannt gewordenen, relevanten IT-Sicherheitsvorfälle und IT-Angriffe möglichst umfassend zu berücksichtigen. Daher sind im hier wiedergegebenen lebenden Dokument nicht nur IT-Sicherheitsvorfälle und IT-Angriffe beschrieben, die im Berichtszeitraum bekannt geworden sind, sondern es wurden sukzessive auch herausragende Vorfälle und Angriffe aus früheren Jahren aufgearbeitet, soweit es im Rahmen des Vorhabens möglich war.

Viele IT-Angriffe laufen unbemerkt oder auch ungehindert über mehrere Jahre, daher ist die Zuordnung zu einem einzelnen Jahr oftmals nicht eindeutig. Konkrete IT-Sicherheitsvorfälle werden hier typischerweise dem Jahr zugeordnet, in dem sie bekannt wurden. Länger andauernde IT-Angriffswellen werden dem Jahr zugeordnet, in dem ihr (teilweise auch vorläufiger) Höhepunkt ausgemacht werden kann

B.1 2007

B.1.1 Stuxnet 0.5

Übersicht

Bei Stuxnet 0.5 handelt es sich um die derzeit älteste bekannte Version der Stuxnet-Schadsoftwarefamilie. Sie wurde bereits seit 2005 entwickelt und ab 2007 eingesetzt.

Beschreibung

Mit dem Namen Stuxnet wird nicht nur eine einzige Schadsoftwarekomponente bezeichnet, vielmehr werden unter Stuxnet eine ganze Familie von Schadsoftwarekomponenten zusammengefasst. Als erste entdeckt wurde eine im März 2010 kompilierte Version der Schadsoftware, die heute als Stuxnet Variante B bekannt ist und sich weltweit am meisten verbreitete. Im Zuge der massiven Recherchen und Untersuchungen die nach Bekanntwerden von Variante B angestrengt wurden, entdeckte man auch die nicht ganz so stark verbreitete Variante A aus dem Jahr 2009 und die Variante C aus dem Jahr 2010. Alle drei Varianten haben gemein, dass sie eine Funktionalität zur Manipulation von Motoren besitzen, die speziell im Bereich von Zentrifugen zur Urananreicherung eingesetzt werden.

Eine deutlich früher erstellte Version der Schadsoftware, Stuxnet 0.5, wurde erst 2013 entdeckt. Sie ist im Gegensatz zu den späteren, bereits 2010 entdeckten Varianten auf eine Manipulation von Ventilen zur Regelung des Uranhexafluiddurchflusses im Anreicherungsprozess ausgerichtet und wurde derzeitigen Erkenntnissen zufolge von einem im Geheimdienstauftrag agierenden Innentäter in die Anlage Natanz eingebracht.

Stuxnet 0.5 besitzt deutlich weniger Flexibilität hinsichtlich möglicher Verbreitungswege als spätere Varianten. So verbreitet sich diese Schadsoftware nur über infizierte Step 7 Projekte.

Es ist derzeit nicht bekannt, wie erfolgreich der Angriff mit Stuxnet 0.5 auf die Urananreicherung in Natanz war. Die relativ hohe Austauschrate bei den Zentrifugen im relevanten Zeitraum deutet zumindest auf einen teilweisen Erfolg hin. Auch gibt es Berichte

über den in großer Zahl vorgenommenen Austausch von Technikern. Die Tatsache, dass die späteren Stuxnet-Varianten eine andere Angriffsstrategie verfolgen, deutet allerdings darauf hin, dass man sich von dieser anderen Strategie noch höhere Ausfallraten versprach.

Kerntechnischer Bezug

Die Schadsoftware Stuxnet wurde offensichtlich gezielt entwickelt, um das iranische Atomprogramm zu sabotieren. Tatsächlich kam es zu Beschädigungen an einem erheblichen Teil der in der iranischen Urananreicherungsanlage Natanz eingesetzten Zentrifugen. Zusätzlich zu den physischen Schäden, die durch die von Stuxnet hervorgerufenen Manipulationen langfristig an den Zentrifugen entstanden sind, ist davon auszugehen, dass die Manipulationen auch einen Einfluss auf die Qualität des angereicherten Urans hatten.

B.2 2008

B.2.1 BlackEnergy 1 – IT-Angriffe auf georgische Einrichtungen

Übersicht

Bei BlackEnergy 1 handelt es sich um ein HTTP-basiertes IT-Angriffswerkzeug zur Durchführung von DDoS-Angriffen. BlackEnergy 1 wurde mehrfach weiterentwickelt. In den Jahren 2010 bzw. 2015 wurden die Versionen BlackEnergy 2 bzw. BlackEnergy 3 (siehe Abschnitte 3.2.6.1 bzw. 3.2.8.1) erstmalig bekannt und in den Folgejahren jeweils breit eingesetzt, wobei von jeder Version zahlreiche Varianten in Umlauf sind.

Beschreibung

Die Schadsoftware BlackEnergy 1 besteht aus einem Dropper, einem Treiber bzw. Rootkit und der MainDLL. Diese Komponenten werden im Folgenden erklärt. /ITB16r01/

Der Dropper ist ein Hilfsprogramm. Er lädt den in ihm enthaltenen Rootkit-Treiber und zählt alle auf dem befallenen Gerät bereits installierten Treiber auf. Danach wählt er zufällig einen deaktivierten Treiber aus und ersetzt diesen durch den infizierten Treiber.

Der entsprechende Dateipfad wird so konfiguriert, dass er bei einem Bootvorgang automatisch gestartet wird.

Auf diese Weise erreichen die Angreifer eine persistente Verbindung. Der Rootkit-Treiber bildet somit eine Backdoor. Nur diese Komponente verbleibt dauerhaft auf dem infizierten System. Der Dropper startet das System neu und verweist danach auf sich selbst, wodurch er eine Signatur erzeugt. Er aktiviert unter Windows den Testmodus im Boot-Menü. Somit können Treiber verwendet werden, die nicht von Microsoft digital signiert wurden, was die Anwendung des infizierten Treibers ermöglicht /MIS20w01/. Danach blendet der Dropper die Hinweise aus, dass das System im Testmodus gestartet wurde und umgeht die Benutzerkontensteuerung (User Account Control UAC) von Windows. Der Dropper nutzt die Microsoft-Schwachstelle MS08-025 aus, die es dem Angreifer erlaubt seine Zugriffsrechte auf das System zu erhöhen, auch wenn der Benutzer des infizierten Geräts über keine Rechte verfügt, neue Software zu installieren. Auf diese Weise ist der Dropper in der Lage die Installation des Rootkit-Treibers abzuschließen. /FSE14r01, ITB16r01, SEC10w01/

Der Rootkit-Treiber verwendet API-Hooking[14], um Objekte auf Festplatten, in der Registry und in Speichern zu verbergen. Dadurch wird die Detektion des Treibers erschwert. Schließlich lädt der Treiber die in ihm eingebettete MainDLL der Schadsoftware und führt diese aus. /SEC10w01/

Die MainDLL kann Dateien vom C&C-Server der Angreifer laden und ausführen. Dazu zählen auch Updates der Schadsoftware /SEC10w01/. Ab Version 1.8, welche 2008 entwickelt wurde, verfügt BlackEnergy 1 über drei zusätzliche Plugins zur Durchführung von DDoS-Angriffen. Diese unterscheiden sich in der Art und Weise der Durchführung des Angriffs und werden als *DDoS-Plugin, syn-Plugin und http-Plugin* bezeichnet: /ITB16r01, SEC10w01/

- **DDoS-Plugin**: Dieses Plugin greift das Zielgerät mit zufälligen TCP-, UDP-, ICMP- und HTTP-Nachrichten an. Die Abkürzungen stehen für verschiedene Netzwerkprotokolle. /SEC10w01/

[14] API-Hooking beschreibt Techniken, mit denen das Verhalten und der Fluss von API-Anfragen modifi-ziert und manipuliert werden kann /INF14w01/. APIs (Application Programming Interfaces) wiederum sind Software-to-Software-Schnittstellen /HUB22w01/.

- **syn-Plugin**: Das Plugin lädt einen Kernel-Treiber, der das Zielgerät mit TCP SYN-Paketen bombardiert. SYN steht für Synchronization. Durch Verwendung des Kernels können die SYN-Pakete sehr schnell und ohne Einfluss auf die TCP-Statustabelle des Systems verschickt werden, welche nur eine begrenzte Anzahl an Einträgen aufnehmen kann. /SEC10w01/
- **http-Plugin**: Das Plugin nutzt die OLE-Automatisierung des Internet Explorers, um das Zielgerät mit HTTP-Anfragen zu bombardieren. Obwohl dieser Angriff langsamer als der HTTP-Angriff des DDoS-Plugins abläuft, macht es die Verwendung des Internet Explorers schwieriger zwischen einem Angriff und normalem Browsen zu unterscheiden. /SEC10w01/

Entscheidend ist, dass durch die Möglichkeit des Herunterladens von Plugins ein modularer Aufbau der Schadsoftware realisiert wird, da diese jederzeit durch zusätzliche Plugins erweiterbar ist.

Die Schadsoftware BlackEnergy 1 wurde zum ersten Mal von Arbor Networks in der Mitte des Jahres 2007 entdeckt. Dabei wurden 27 mit BlackEnergy 1 infizierte Botnetze untersucht, von denen jedes aus etwa 100 Bots bestand. Die meisten Botnetze befanden sich in Russland und Malaysia, wobei sich die meisten Ziele für über die Botnetze durchgeführte DDoS-Angriffe in Russland befanden. BlackEnergy 1 wurde im Rahmen zahlreicher IT-Angriffe eingesetzt, unter anderem wohl auch bei mehreren IT-Angriffswellen 2008 auf georgische Einrichtungen im Vorfeld der militärischen Auseinandersetzungen zwischen Russland und Georgien. Betroffen waren unter anderem Webseiten zahlreicher Regierungseinrichtungen, Nachrichtenagenturen und Finanzunternehmen. /THS16r01, FSE14r01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.3 2010

B.3.1 Stuxnet – IT-Angriff auf Natanz

Übersicht

Bei Stuxnet handelt es sich um die erste bekannt gewordene, speziell auf die Manipulation von SPS (Speicherprogrammierbaren Steuerungen) ausgerichtete Schadsoftware. Stuxnet ist eine hochentwickelte, komplexe Schadsoftware, die nach einer erfolgten Erstinfektion in der Lage ist, auch autonom zu agieren und für die Durchführung der gezielten Manipulationen von Steuerungen nicht auf eine Interaktion mit den Angreifern angewiesen ist.

Beschreibung

Bei Stuxnet handelt es sich um eine Schadsoftware, die gezielt mehrere Sicherheitslücken im Microsoft Betriebssystem Windows ausnutzt, um sich zu verbreiten. Eine dieser Schwachstellen nutzt Stuxnet, um sich beispielsweise über Netzwerke oder mobile Datenträger wie USB-Sticks auf ein IT-System einzuschleusen, auch über Air-Gaps hinweg. Hierfür benötigt Stuxnet keine Aktion des Nutzers und keine aktivierte Autostart-Funktion, sondern es reicht aus, ein Verzeichnis zum Betrachten zu öffnen, das eine infizierte LNK-Datei enthält. Der Schadcode wird bereits bei Anzeige des manipulierten Icons im Explorer ausgeführt. Die hierbei ausgenutzte Schwachstelle, die als LNK-Schwachstelle bekannt ist, wurde von Microsoft zeitnah gepatcht, allerdings sind die entsprechenden Patches nach wie vor nicht flächendeckend eingesetzt. Microsoft listete beispielsweise im Security Intelligence Report für 2015 die LNK-Schwachstelle, als die am häufigsten von Angreifern ausgenutzte Einzelschwachstelle des Jahres 2015 /MIC15r01/. Zusätzlich dazu ist trotz Patchen der Schwachstelle eine Infektion mit Stuxnet durch Doppelklick auf eine infizierte Datei möglich. Neben der Verbreitung über Wechselmedien ist Stuxnet aber auch in der Lage, sich über zahlreiche andere Wege wie beispielsweise über das Intranet, gemeinsam genutzte Drucker, die Microsoft SQL Datenbank von WinCC sowie Step-7 Projekte zu verbreiten, teilweise unter Ausnutzung weiterer Schwachstellen im Microsoft Windows Betriebssystem. /GRS12f01/

Bei der Infektion eines Systems mit Stuxnet wird jeweils eine Schadsoftwarekomponente zum Ausspähen von Informationen und ein sogenanntes Rootkit zum Verschleiern der

Infektion installiert. Auf infizierten Systemen sucht Stuxnet gezielt nach Prozesssteuerungssystemen, die SIMATIC WinCC oder SIMATIC PSC7 von Siemens einsetzen. Als erste Schadsoftware ist Stuxnet speziell darauf ausgerichtet, diese Software zu manipulieren und darüber speicherprogrammierbare Steuerungen zu infizieren und zu manipulieren. Die bekannten Versionen von Stuxnet (Variante A und Variante B) zielen auf die Manipulation von Frequenzumrichtern für besonders hohe Frequenzen ab, wie sie beispielsweise für Zentrifugen bei der Urananreicherung eingesetzt werden. /GRS12f01/

Kerntechnischer Bezug

Die Schadsoftware Stuxnet wurde offensichtlich gezielt entwickelt, um das iranische Atomprogramm zu sabotieren. Tatsächlich kam es zu Beschädigungen an einem erheblichen Teil der in der iranischen Urananreicherungsanlage Natanz eingesetzten Zentrifugen. Zusätzlich zu den physischen Schäden, die durch die von Stuxnet hervorgerufenen Manipulationen langfristig an den Zentrifugen entstanden sind, ist davon auszugehen, dass die Manipulationen auch einen Einfluss auf die Qualität des angereicherten Urans hatten.

B.4 2011

B.4.1 Chinese Gas Pipeline Intrusion Campaign

Übersicht

Zwischen den Jahren 2011 und 2013 wurden vom chinesischen Staat unterstützte Spear-Phishing-Angriffe auf US-amerikanische Gaspipeline-Unternehmen durchgeführt. Diese Angriffe hatten das Potential physische Schäden an den Pipelines durchzuführen und ihren Betrieb zu stören.

Beschreibung

Zwischen Dezember 2011 und 2013 wurden im Zuge einer vom chinesischen Staat unterstützten Spear-Phishing-Kampagne US-amerikanische Öl- und Gaspipeline-Unternehmen angegriffen. Von den 23 betroffenen Gaspipeline-Unternehmen wurden 13 kompromittiert, bei acht Unternehmen ist der Grad der Intrusion unbekannt und bei drei

Unternehmen konnte ein Eindringen in das Netzwerk gerade noch verhindert werden. /CIF21i01, EEN21w01/

Die Spear-Phishing-E-Mails waren an die Angestellten der Unternehmen gerichtet und waren mit großem Aufwand so gestaltet, dass sie die Angestellten dazu verleiteten die schadhaften Dateien im E-Mail-Anhang zu öffnen /CSM12w01/. Neben der Spear-Phishing-Kampagne versuchten die Angreifer wohl auch sich durch Social Engineering Zugriff zu den Firmennetzwerken zu verschaffen.

In einem Unternehmen erhielten Angestellte und Manager, die in der Netzwerk-Engineering-Abteilung arbeiteten, dubiose Anrufe, in denen sie über die aktuellen Sicherheitsmaßnahmen zum Schutz des Firmennetzwerks befragt wurden. Dabei gaben sich die Angreifer als Angestellte einer Computersicherheitsfirma aus, die Umfragen durchführen würde. Diese Anrufe erfolgten unmittelbar nachdem die Angriffe erkannt, die Angreifer erfolgreich aus dem Netzwerk ausgesperrt wurden und das System neu gestartet worden war. Während der IT-Angriffe wurden die Dokumente-Repositories von den Angreifern nach SCAD*-Dateien, Personalisten, Benutzernamen und Passwörtern, Dial-up-Zugriffsinformationen sowie Systemhandbüchern durchsucht. Sie kompromittierten eine Vielzahl autorisierter Fernzugriffskanäle. Dazu zählen auch Systeme für den Datentransfer mit und den Zugriff auf ICS-Netzwerke. Darüber hinaus gelang es ihnen auf die SCADA-Netzwerke von Gaspipeline-Unternehmen zuzugreifen. Nach Ansicht des CISA und des FBI könnten die gestohlenen Daten und Informationen für die Vorbereitung eines IT-Angriffs des chinesischen Staates auf die Pipeline-Infrastruktur der USA genutzt werden, mit dem Ziel die Pipelines physisch zu beschädigen oder ihren Betrieb zu stören und so die US-amerikanische Pipeline-Infrastruktur zu gefährden. /CIF21i01, EEN21w01/

Um eine Infizierung von Netzwerken zu vermeiden, empfehlen das CISA und das FBI Zugriffsbeschränkungen und eine Multi-Faktor-Authentifizierung einzurichten. Darüber hinaus sollte der Datenverkehr gefiltert und kontrolliert werden. Eine Segmentierung zwischen IT-Netzen und ICS- bzw. OT-Netzen (OT – Operational Technology) erschwert die Ausbreitung schadhafter Einwirkungen vom Firmennetzwerk auf die Steuerungssysteme. /CIF21i01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.5 2012

B.5.1 Shamoon – IT-Angriff auf Saudi Aramco

Übersicht

Die Schadsoftware Shamoon (auch W32.DistTrack) wurde im Jahr 2012 bei einem IT-Angriff auf Saudi Aramco, das weltweit größte Unternehmen zur Erdölförderung, eingesetzt /BBC12w01/. Shamoon ist in der Lage, die auf den Rechnern enthaltenen Dateien zu überschreiben und die Rechner selbst in einem nicht-bootfähigen Zustand zu hinterlassen. Auf diese Weise kann für ein angegriffenes Unternehmen erheblicher Schaden entstehen.

Beschreibung

Shamoon besteht im Wesentlichen aus drei Schadsoftwarekomponenten /SYM12r01/:

- Einer Dropper-Komponente, die für die Installation der weiteren Komponenten verantwortlich ist,
- einer Wiper-Komponente, welche auf dem infizierten Rechner zuerst Dateien und schließlich auch den Master Boot Record überschreibt, wonach der Rechner nicht mehr gebootet werden kann, sowie
- einer Reporter-Komponente, welche Informationen über die Infektion einschließlich einer Liste der gelöschten Dateien an die Angreifer schickt.

Der beim Angriff auf Saudi Aramco eingesetzte Code von Shamoon enthielt zusätzlich einen Timer, der zu der zeitgleichen Ausführung der Wiper-Komponente auf allen infizierten Rechnern führte.

Der Angriff auf Saudi Aramco begann vermutlich Mitte 2012 mit einer gezielten Spear-Phishing-Attacke, welche zur Infektion eines ersten Rechners führte und den Angreifern Zugriff auf das Anlagennetzwerk verschaffte. Von einem Command-and-Control Server aus nutzten die Angreifer diesen Rechner zur weiteren Verbreitung im Anlagennetz. Dies schließt auch die Infektion von Rechnern mit ein, die selbst nicht mit dem Internet verbunden waren. /SEC12w01/

Am 12. August 2012, zeitgleich um 11:08 Uhr begann Shamoon mit dem Überschreiben von Dateien auf 30 000 Rechnern. Insgesamt waren von dem Angriff etwa drei Viertel der Informationsinfrastruktur von Saudi Aramco betroffen. /BBC12w01, NYT12w01/

Kaspersky und andere IT-Sicherheitsunternehmen haben Shamoon untersucht und auch mögliche Parallelen zu den IT-Angriffen in Zusammenhang mit Flame (siehe Abschnitt B.5.1) untersucht, bezeichnen Shamoon aber letztlich als Copycat und schreiben ihn „begabten Amateuren“ zu. /DAR12w01, SEC12w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.5.2 BlackEnergy 2 – Globaler IT-Angriff

Übersicht

Bei BlackEnergy 2 handelt es sich um eine Weiterentwicklung des als BlackEnergy 1 (siehe Kapitel B.2.1) bekannt gewordenen HTTP-basierten IT-Angriffswerkzeugs zur Durchführung von DDoS-Angriffen. Wie schon von BlackEnergy 1 sind auch von BlackEnergy 2 zahlreiche Varianten in Umlauf. Die IT-Sicherheitsfirma Kaspersky Labs zählte 2010 bereits mehr als 4000 Varianten der beiden Schadsoftware-Versionen /SEC10w02/.

Beschreibung

BlackEnergy 2 wurde 2010 entwickelt und besteht wie BlackEnergy 1 (siehe Kapitel B.2.1) aus dem Dropper, dem Rootkit-Treiber, der MainDLL und wurde zusätzlich um eine Vielzahl herunterladbarer Plugins erweitert, darunter Plugins zur Versendung von Spam-Nachrichten und für Betrügereien beim Online-Banking. Dadurch erhielt die Schadsoftware einen modularen Aufbau. Durch den modularen Aufbau ist die Schadsoftware sehr vielseitig einsetzbar. /ITB16r01/

Der Programmcode wurde dabei von BlackEnergy 1 übernommen. Die Unterschiede zu BlackEnergy 1 bestehen darin, dass BlackEnergy 2 moderne Methoden zum Entpacken des Rootkit-Treibers und der Infiltrierung von Benutzer-Prozessen verwendet. /SEC10w01/

Der Dropper von BlackEnergy 2 lädt zunächst einen Rootkit Decrypter, in dem der eigentliche Rootkit-Treiber enthalten ist. Letzterer wird wiederum vom Rootkit Decrypter entpackt. Abgesehen von dieser zusätzlichen Einbettung, weist BlackEnergy 2 dieselbe verschachtelte Struktur wie BlackEnergy 1 auf. Auch der Entpackungsvorgang der Schadsoftware ist bis auf diesen zusätzlichen Schritt identisch.

Von Antivirenprogrammen wird BlackEnergy 2 häufig als Rustock.E fehlidentifiziert, da der Rootkit-Treiber von BlackEnergy 2 einige ähnliche Techniken verwendet wie das Rootkit der Schadsoftware Rustock.E. Letztere gehört jedoch zu einer anderen Schadsoftware-Familie. Auch die verschachtelte Struktur ist beiden Schadsoftware-Varianten gemein. /SEC10w01/

Nachfolgend werden die zusätzlichen Plugins beschrieben, die BlackEnergy 2 bereitstellt:

- **Spam-Plugin**: Hierbei handelt es sich um eine wieder verwendete Version des Spambots Grum, ein infiziertes Computernetzwerk, das von C&C-Servern dazu gebracht wird Spam-Mails zu verschicken. Dieser Spambot ist mit der Plugin-Architektur von BlackEnergy 2 kompatibel. /SEC10w01, SPI12w01/
- **Ibank-Plugin**: Über dieses Plugin können die Zugangsdaten für das Online-Banking eines Benutzers gestohlen werden. Es besteht aus zwei Komponenten, dem Haupt- und dem in diesem eingebetteten Unter-Modul. Das Haupt-Modul schleust das Unter-Modul in die Internet Explorer-, Firefox-, Flock- Opera- und Java-Browseranwendungen ein. In jeder dieser Anwendungen führt das Unter-Modul eine Programmschleife aus und überprüft die jeweilige Anwendung auf einen auf Java basierenden Dialog. Von diesem speichert es die Tastatureingaben oder Eingaben aus der Zwischenablage durch den Benutzer, um dessen Zugangsdaten für das Online-Banking zu erhalten. Darüber hinaus speichert das Unter-Modul angeforderte Internetadressen zur Identifikation des Geldinstituts. Die gespeicherten Informationen werden schließlich an das Haupt-Modul gesendet. Dieses leitet sie an den C&C-Server der Angreifer weiter. Das Plugin ist auf ein spezielles, auf öffentlicher Verschlüsselung basierendes, Online-Banking-System zugeschnitten, das von vielen russischen und ukrainischen Banken verwendet wird. /SEC10w01/
- **Kill-Plugin**: Dieses Plugin wird in Verbindung mit dem zuvor beschriebenen Ibank-Plugin eingesetzt. Es zerstört das Dateisystem des infizierten Computers, indem es auf jeder unter Windows aufgelisteten Festplatte die ersten 4096 Cluster mit

zufälligen Daten überschreibt und die Bootfähigkeit des Systems zerstört. Danach fährt das Plugin das System herunter. Das Plugin wird vermutlich nach dem Diebstahl der Daten für das Online-Banking eingesetzt. Dadurch wird verhindert, dass der Benutzer sich in sein Portal für das Online-Banking einloggen kann. Auf diese Weise erkennt er nicht, dass von den Angreifern Geld von seinem Konto abgehoben wird, was ihn dazu veranlassen könnte sein Geldinstitut über die illegale Transaktion zu informieren. /SEC10w01/

Die APT-Gruppierung Sandworm übernahm im Jahr 2013 die BlackEnergy 2 Schadsoftware und erweiterte diese um eine Vielzahl eigener, zusätzlicher Plugins. Diese ermöglichen die Erzeugung zusätzlicher Backdoors, die Auskundschaftung des Netzwerkes, das Überschreiben, Löschen, Herunterladen und Ausführen von Dateien, die Aufzeichnung von Tastatureingaben, den Diebstahl von Passwörtern, den Fernzugriff auf den Desktop, die Erstellung von Screenshots, den Diebstahl von Zertifikaten und das Löschen der Festplatte /ITB16r01/, /SEC14w01/

Darüber hinaus hat die ATP-Gruppierung Sandworm Plugins für Linux-Umgebungen geschrieben. Somit wird die Kompatibilität von BlackEnergy 2 von Windows-Betriebssystemen auf Linux-Systeme erweitert. /SEC14w01/

BlackEnergy 2 wurde ab 2010 bei zahlreichen IT-Angriffen eingesetzt, insbesondere Ende 2013 und 2014. Das IT-Sicherheitsunternehmen Kaspersky berichtete für diese Angriffswelle von einer Vielzahl von weltweit verteilten Angriffszielen, unter anderem in Russland, der Ukraine, Polen, Litauen, Weißrussland, Aserbaidschan, Kasachstan, Iran, Israel, der Türkei, Kuwait, Taiwan, Vietnam, Indien, Kroatien, Deutschland, Belgien und Schweden. Als Angriffsziele werden beispielsweise Kraftwerksbetreiber und deren Subunternehmer sowie Hersteller und Zulieferer von Kraftwerkskomponenten und industriellen Steuerungssystemen, aber auch Regierungseinrichtungen, Forschungseinrichtungen, Messstationen, Rettungsdienste und Banken genannt. /SEC14w01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.5.3 Spear-Phishing-Angriff durch ehemaligen U.S. NRC Mitarbeiter

Übersicht

2013 deckte das FBI die Hintergründe eines Spear-Phishing-Angriffs auf Mitarbeiter des U.S. Department of Energy auf. Ein vormaliger Mitarbeiter der U.S. NRC versuchte damit IT-Systeme zu kompromittieren, die sensible Informationen über nukleare Waffen enthalten, um diese Informationen zum Kauf anzubieten. /DOJ16r01/

Beschreibung

Ein ehemaliger Mitarbeiter des Department of Energy (DOE) und der Nuclear Regulatory Commission (NRC) der USA wurde 2010 von der NRC entlassen und griff im Jahr 2015 von den Philippinen aus seine früheren Kollegen beim DOE über eine Spear-Phishing-Kampagne an. Das Ziel des Angriffs war die Infizierung der staatlichen Netzwerke, der Diebstahl von geheimen Daten zu Nuklearwaffen und der Verkauf dieser Daten an ausländische Regierungen. /FED16w01/

Im Jahr 2013 bot er zunächst einer ausländischen Botschaft in Manila 5000 E-Mail-Accounts von DOE-Mitarbeitern, welche nach seinen Aussagen streng geheim waren, zum Verkauf an und verlangte dafür 18800 Dollar. Er sagte den Angestellten der Botschaft, dass falls diese nicht zustimmen würden, er China, dem Iran oder Venezuela das gleiche Angebot machen würde. Man stimmte dem Kauf zu, wobei es sich bei den Angestellten um verdeckt ermittelnde FBI-Agenten handelte. Über eine Zeitspanne von mehr als einem Jahr kauften ihm die Agenten tausende von E-Mail-Accounts ab, welche veröffentlicht werden sollten. Während eines Treffens im Juni 2014 händigte er den Agenten eine Liste von 30000 E-Mails aus und bot ihnen an, einen Spear-Phishing-Angriff gegen die DOE durchzuführen, um noch mehr geheime Informationen zu stehlen. Bei diesem Angriff im Januar 2015 schrieb er eine E-Mail an 80 DOE-Mitarbeiter über eine angeblich bevorstehende Konferenz und bettete darin einen Link ein, den er von einem der FBI-Agenten erhalten hatte und von dem er glaubte, dass er schadhaft sei. Ein Teil der von diesem potenziellen Spear-Phishing-Angriff betroffenen DOE-Angestellten arbeitete in nuklearen Laboren. /FCW16w01, FED16w01/

Als der ehemalige NRC-Mitarbeiter die ihm für den Angriff versprochenen 80000 Dollar abholen wollte, wurde er festgenommen und an die USA ausgeliefert. Er wurde im April 2016 zu einer Haftstrafe von 18 Monaten verurteilt /INF16w01/.

Aufgrund der Arbeit der FBI-Agenten kam es zu keinem realen Schaden und die sensiblen Informationen blieben geheim. /FED16w01/

Kerntechnischer Bezug

Bei diesem Angriff sollten Unbefugten sensible Informationen über nukleare Waffen zugänglich gemacht und diese an ausländische Regierungen verkauft werden. Durch die Arbeit der verdeckt ermittelten FBI-Agenten konnte dies allerdings verhindert werden.

B.6 2014

B.6.1 IT-Angriff auf südkoreanisches Kernkraftwerk

Übersicht

Im Dezember 2014 wurde bekannt, dass der Betreiber südkoreanischer Kernkraftwerke Korea Hydro & Nuclear Power Co. Opfer eines IT-Angriffs in Form eines Informationsdiebstahls wurde. Nach Mutmaßungen der Staatsanwaltschaft in Seoul ist die nordkoreanische Gruppierung Kimsuky für den Angriff verantwortlich, da die eingesetzten Techniken und Angriffsmuster mit denen von Kimsuky übereinstimmen. Weitere Informationen befinden sich in Abschnitt 3.12.8.

Kerntechnischer Bezug

Beim Angriffsziel handelt es sich um einen Kraftwerksbetreiber, der unter anderem auch die südkoreanischen Kernkraftwerke Kori, Shin-Kori, Wolsong, Ulchin und Yeonggwang betreibt.

B.6.2 IT-Angriff auf ein deutsches Stahlwerk

Übersicht

Im Jahr 2014 erfolgte ein IT-Angriff auf ein deutsches Stahlwerk. Dabei kam es zu massiven physischen Schäden an der Anlage. Welche APT-Gruppierung den Angriff durchgeführt hat, ist bislang nicht bekannt. Auch ist derzeit nicht eindeutig bekannt, welche Schadsoftware bei diesem Angriff zum Einsatz kam. /SAN14r01/

Beschreibung

Die Angreifer verschafften sich über eine Spear-Phishing-Kampagne und ausgefeiltes Social Engineering Zugriff auf das Büronetz des Stahlwerks und über dieses wiederum Zugriff auf das OT-Netzwerk des Stahlwerks und die industriellen Steuerungssysteme /BSI14r01/. Die Angreifer verfügten offenbar über fortgeschrittene technische Kenntnisse bezüglich typischer IT-Sicherheitsmaßnahmen und von ICS-Systemen, da es ihnen gelang einen Ausfall mehrerer Systemkomponenten herbeizuführen /BSI14r01/.

Da diese in der Folge nicht mehr gesteuert bzw. geregelt werden konnten, kam es zu massiven physischen Schäden, z. B. am Hochofen, der nicht mehr abgeschaltet werden konnte und sich in einem undefinierten Zustand befand /BSI14r01/. Bei den bekannten betroffenen Systemen handelt es sich um Komponenten der industriellen Steuerungen der Anlage aus den Bereichen Lastkontrolle, Lastverteilung, Massen- und Energieausgleich, kinetische Prozessmodelle und Heißluftsystem sowie um den Hochofen selbst. Als mögliche weitere betroffene Systeme werden zentrale Steuerungen, welche über eine speicherprogrammierbare Steuerung (SPS – programmable logic controller, PLC) angesteuert werden, Alarmsysteme, Komponenten der Sicherheitsleittechnik (SIS) und Mensch-Maschinen-Schnittstellen (Human Machine Interface, HMI). /SAN14r01/

Kerntechnischer Bezug

Da es sich um einen sehr gezielten IT-Angriff handelt und das Angriffsziel ein Stahlwerk war, besteht kein direkter Bezug zu kerntechnischen Anlagen.

B.6.3 Havex und Karagany – Erste IT-Angriffswelle durch APT Dragonfly

Übersicht

Bei den IT-Angriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Kapitel 3.12.5) handelt es sich um hochentwickelte, mehrstufige Angriffe. Die APT-Gruppierung setzt dabei ein breites Spektrum an IT-Angriffswerkzeugen und Schadsoftwarekomponenten ein. Auch verfolgt Dragonfly eine effektive Strategie bei der Kompromittierung von Zielnetzwerken über die Lieferkette.

Beschreibung

Bislang werden Dragonfly zwei Angriffswellen zugeordnet, wobei die erste ihren Höhepunkt 2013 erreichte und nach ihrer Entdeckung 2014 abflaute. Unabhängig von den letztlich eingesetzten IT-Angriffswerkzeugen und Schadsoftwarekomponenten nutzte Dragonfly während der ersten Angriffswelle drei verschiedene Angriffsvektoren /CIS14r01/: Spear Phising über E-Mail mit kompromittierten pdf-Anhängen, Watering-Hole-Angriffe mit verschiedenen Exploit Kits zur Umleitung von Zugriffen auf legitime Webseiten und die Kompromittierung der Update-Seiten von Herstellern industrieller Steuerungssysteme. /SYM14r01/

Als wesentliche IT-Angriffswerkzeuge und Schadsoftwarekomponenten kamen im Rahmen der ersten Angriffswelle vor allem Havex und Karagany zum Einsatz, wobei es sich bei ersterer um eine maßgeschneiderte, bislang nur von Dragonfly eingesetzte Schadsoftwarekomponente handelt /SYM14r01/. Sowohl Havex als auch Karagany dienen dazu, auf infizierten Systemen eine Backdoor für Remote-Zugriffe zu etablieren und einen Kanal für die Einschleusung weiterer Schadsoftware sowie das Extrahieren von gesammelten Informationen bereitzustellen.

Havex enthält neben der Komponente zur Etablierung der Backdoor noch eine persistente Komponente, die mit einem Command-and-Control-Server interagiert, um beliebige weitere Schadsoftwarekomponenten nachzuladen und auszuführen sowie ausgespähte Informationen weiterzugeben. Nach erfolgreicher Infektion sammelt Havex auf den kompromittierten Systemen systematisch Informationen, vornehmlich auch solche Informationen, die mit industriellen Steuerungssystemen in Zusammenhang stehen. Die

Informationen werden anschließend verschlüsselt and den Command-and-Control-Server gesendet. Zu den Schadsoftwarekomponenten, die Havex typischerweise herunterlädt zählen unter anderem auch Komponenten zur Verschleierung des Angriffs. /SYM14r01/

Es ist derzeit nicht genau bekannt, wie viele Unternehmen von der ersten Angriffswelle betroffen waren, Schätzungen zufolge waren es über 2000 /DRA17r02/. Zu den angegriffenen Unternehmen zählten auch Hersteller industrieller Steuerungssysteme, wie beispielsweise die belgische Firma Ewon /SAN16r01/, welche auf Produkte zur Fernwartung spezialisiert ist /EWO20w01/, die schweizerische Firma MESA Imaging /SAN16r01/, welche optische Instrumente einschließlich Überwachungsgeräten herstellt und die deutsche Firma MB Connect Line GmbH, welche ebenfalls Fernwartungslösungen anbietet /MBC20w01/.

Kerntechnischer Bezug

Es ist derzeit nicht bekannt, ob auch kerntechnische Anlagen und Einrichtungen von der ersten Angriffswelle betroffen waren. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r11/.

B.6.4 Epic Turla – Globaler IT-Angriff

Übersicht

Bei Epic Turla handelte es sich um eine IT-Angriffswelle zur Cyber-Spionage, die erstmals im März 2014 publik geworden ist, aber vermutlich bereits seit mindestens 2012 lief. Bei der IT-Angriffswelle wurden mehrere hundert Rechner in über 45 Ländern infiziert. Die Angriffe wurden durch die russische APT-Gruppierung Turla (siehe Kapitel 3.12.13) durchgeführt. Bei den Angriffen handelte es sich um hochentwickelte Angriffe mit dem Ziel der Spionage. Ziele der Angriffe waren Regierungsinstitutionen (Innenministerien, Wirtschaft- und Handelsministerien, Außenministerien, Geheimdienste), Botschaften, militärische Einrichtungen, Bildungseinrichtungen, Forschungsunternehmen und Pharmaunternehmen.

Die Opfer befanden sich meist in Europa und im Nahen und Mittleren Osten, aber vereinzelt auch in anderen Regionen, darunter USA und Russland. /ITS21w01/, /SEC14w03/, /KAS21w03/

Laut /BFV16l01/ wird davon ausgegangen, dass es sich um staatlich gelenkte Angriffe gehandelt hat. Darauf deutet die Verwendung hochwertiger Schadprogramme sowie der lange Zeitraum der Angriffsoperationen und der damit verbundene hohe Aufwand an Ressourcen sowie die IT- und Analysekompetenz der Angreifer.

Beschreibung

Bei Epic Turla wurden verschiedene Angriffsvektoren genutzt: Spear Phishing E-Mails mit Adobe-pdf-Exploits, Social-Engineering-Methoden, um das Opfer dazu zu bringen, Malware mit SCR-Dateierweiterung auszuführen, Watering-Hole-Attacken unter Verwendung von Java-, Flash- oder Internet Explorer-Exploits und auf Social-Engineering fußende Watering-Hole-Attacken, die das Opfer dazu bringen sollten, als Flash Player getarnte Malware auszuführen. Bei den Angriffen wurden mindestens zwei Zero-Day-Exploits ausgenutzt: eine Privilegieneskalations-Sicherheitslücke bei Windows XP und Windows 2003 (CVE-2013-5065) und eine Sicherheitslücke im Adobe Reader, die das Ausführen von beliebigem Code ermöglicht (CVE-2013-3346). /ITS21w01/, /SEC14w03/, /KAS21w03/

Bei der IT-Angriffswelle handelt es sich um eine mehrstufige Infektion. Epic Turla ist dabei die erste Phase der Cyber-Spionage-Kampagne.

In Abhängigkeit von der erkannten IP-Adresse des Opfers stellen die Angreifer Java- oder Browser-Exploits, signierte, aber falsche Adobe Flash Player-Software oder eine gefälschte Version von Microsoft Security Essentials bereits. Außerdem wurden mehr als 100 infizierte Webseiten für Watering-Hole-Attacken entdeckt. Das Öffnen einer mit Malware präparierten Datei (z. B. einer pdf Datei) ruft die Infektion des betreffenden Rechners hervor. Die Schadsoftware ist in der Lage, dem Angreifer die Kontrolle über das System zu verschaffen, Daten zu stehlen und den Netzwerkdatenverkehr mitzuschneiden. Außerdem wird auf den infizierten Systemen eine Backdoor zur Einschleusung weiterer Schadsoftware sowie das Extrahieren von gesammelten Informationen etabliert. Im nächsten Schritt wird dann zielgerichtet Schadsoftware auf den angegriffenen Rechner geladen.

Dazu stellt Epic Turla über eine Backdoor eine Verbindung zum Command-and-Control-Server her, um ein Paket mit Systeminformationen des Opfers an die Angreifer zu senden. Dadurch erhält der Angreifer Informationen zum Opfer, auf deren Basis eine Batch-Datei entwickelt wird, die eine Reihe ausführbarer Befehle enthält. Außerdem werden diverse Tools zur Seitwärtsbewegung des Angreifers hochgeladen. Der Kommunikation zwischen Opfersystem und Command-and-Control-Server sind mindestens zwei Ebenen von Proxy-Servern zwischengeschaltet, um den Angreifern die Wahrung der Anonymität zu ermöglichen. Zur Verschleierung des physikalischen Standorts der Angreifer wird zudem satellitengestützte Kommunikation genutzt, die auf dem Kapern von DVB-S-Verbindungen und dem Fälschen von Datenpaketen basiert und damit hochgradig anonym ist. /ITS21w01/, /SEC14w03/, /KAS21w03/, /BFV16l01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Laut /BFV16l01/ zeigte sich anhand der Zielauswahl ein Interesse der Angreifer an Wirtschaft und Forschung in den Bereichen Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung. Aus diesem Grund ist ein kerntechnischer Bezug nicht auszuschließen.

B.7 2015

B.7.1 BlackEnergy 3 – IT-Angriff auf das ukrainische Stromnetz

Übersicht

Am 23.12.2015 kam es zu einem ungeplanten Ausfall im Stromnetz der Ukraine und zu einem mehrstündigen Stromausfall für ca. 225.000 Kunden. Der Ausfall ereignete sich aufgrund eines IT-Angriffs, bei welchem Systeme von insgesamt drei Energieversorgungsunternehmen erfolgreich angegriffen wurden. Drei weitere Unternehmen wurden ebenfalls angegriffen, ihr Betrieb konnte aber fortwährend weiterlaufen. /CIS16i01/

Beschreibung

Von BlackEnergy sind zurzeit drei Versionen bekannt, BlackEnergy 1, 2 und 3. Erste Versionen von BlackEnergy 1 wurden bereits 2007 aufgefunden. Bei dieser Version der

Schadsoftware handelt es sich um ein HTTP-basiertes Botnet zur Durchführung von DDoS-Angriffen. Diese ursprüngliche Version der Schadsoftware wurde durch eine Vielzahl von herunterladbaren Plugins erweitert, darunter Plugins zur Versendung von Spam-Nachrichten und für Betrügereien beim Online-Banking. Dadurch erhielt die Schadsoftware einen modularen Aufbau. Diese Version wurde 2010 erstmalig aufgefunden und ist unter BlackEnergy 2 bekannt.

In der Schadsoftware-Version BlackEnergy 3, die ab 2014 aufgefunden wurde, ist die Anzahl der Plugins wieder stark reduziert worden, weshalb diese Version der Schadsoftware auch als BlackEnergy Lite bezeichnet wird. Deren Plugins und ihre Funktionen beschränken sich im Wesentlichen auf die Auskundschaftung von Netzwerken. Darüber hinaus verfügt BlackEnergy 3 über die Schadsoftwarekomponente KillDisk.

Eine spätere, abgewandelte Version bietet zusätzlich die Möglichkeit industrielle Steuerungssysteme zu manipulieren. /ICF16w01/, /ITB16r01/, /SEC10w01/, /SEC14w01/ Beim IT-Angriff auf das ukrainische Stromnetz 2015 wird davon ausgegangen, dass die Angreifer vorher IT-Angriffsschritte zur umfassenden Aufklärung durchführten und dann mittels Remote-Zugängen auf Büro-IT und Leittechniksysteme zugriffen. Die Systeme wurden mittels der Schadsoftwarekomponente KillDisk angegriffen und für den Betrieb notwendige Daten wurden gelöscht. Auch wurde die Steuerung der unterbrechungsfreien Stromversorgung für die Server angegriffen.

Die vom IT-Angriff betroffenen Betreiber gaben bekannt, dass die Systeme von der Schadsoftware BlackEnergy 3 betroffen waren, aber in welchem Umfang diese Schadsoftware genutzt wurde, ist bislang nicht klar. Es ist aber sehr wahrscheinlich, dass BlackEnergy 3 bei den Angriffen auf das Stromnetz der Ukraine zumindest eine unter-stützende Rolle spielte, indem die Schadsoftware den Angreifern den Zugriff auf die Computer-Arbeitsplätze und die Netzwerke der Anlagen ermöglichte /CIS16i01/, /ITB16r01/.

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.7.2 GreyEnergy – IT-Angriff auf Stromnetze in Osteuropa

Übersicht

Die Schadsoftware GreyEnergy wurde bei IT-Angriffen gegen kritische Infrastrukturen in Zentral- und Osteuropa eingesetzt, wobei die Angriffsziele hauptsächlich in der Ukraine lagen. Die Schadsoftware weist große Ähnlichkeiten zu BlackEnergy (siehe Kapitel 3.9) auf. Gegen Ende des Jahres 2015 erfolgte ein IT-Angriff mit GreyEnergy auf ein Energieversorgungsunternehmen in Polen. Aber auch danach wurde GreyEnergy bei ähnlichen Angriffen eingesetzt, zuletzt wurden IT-Angriffe mit dieser Schadsoftware Mitte des Jahres 2018 bekannt. /ESE18r01/

Beschreibung

Die APT-Gruppierung, die GreyEnergy entwickelt hat, wird von ESET ebenfalls als GreyEnergy bezeichnet und hat nach Einschätzung dieser IT-Analysten vermutlich mit der APT-Gruppierung TeleBots zusammengearbeitet. Das Interesse der APT-Gruppierung GreyEnergy ist auf Industrienetzwerke und kritische Infrastrukturen gerichtet. /ESE18r01/

Der Angriff über die Schadsoftware GreyEnergy kann auf zwei möglichen Angriffswegen erfolgen. Wenn Unternehmen Webdienste zur Verfügung stellen, die über einen Server mit dem internen Netzwerk des Unternehmens verbunden sind, versuchen die Angreifer sich über diesen Weg Zugang zum Firmennetzwerk zu verschaffen.

Der zweite Angriffsweg verwendet Spear-Phishing-E-Mails mit angehängten Word-Dokumenten, die infizierte Makros enthalten /FSE19r02/. Die Schadsoftware GreyEnergy ist modular aufgebaut. Im Gegensatz zur Schadsoftware Crashoverride (siehe Kapitel B.8.1) besitzt GreyEnergy kein Modul, das ICS-Systeme direkt beeinflussen kann. Die Module dienen hauptsächlich dazu, das Netzwerk auszukundschaften und Zugangsrechte zu erhalten /BLE18w01/. Stattdessen besitzt die Schadsoftware eine Disk-Wiping-Komponente, um Arbeitsprozesse im betroffenen Unternehmen zu unterbrechen und um die Spuren des Angriffs zu verwischen. Angriffsziele sind ICS-Steuerungsrechner mit SCADA-Software und -Servern /ESE18w01/. Die Infiltrierung der Netzwerke dient vermutlich der Spionage und der Erkundung als Vorbereitung für spätere Angriffe /ZDN18w02/. Eine Version von GreyEnergy wurde mit einem gültigen digitalen Zertifikat

gekennzeichnet, das zuvor vermutlich von einer taiwanesischen Firma gestohlen wurde, die ICS-Geräte herstellt. /ESE18r01/

Kerntechnischer Bezug

Derzeit ist kein direkter kerntechnischer Bezug bekannt.

B.8 2016

B.8.1 Crashoverride/Industroyer – IT-Angriff auf die Stromversorgung in Kiew

Übersicht

Bei der Schadsoftware Crashoverride, die auch als Industroyer bezeichnet wird, handelt es sich um die erste Schadsoftware, die gezielt für Angriffe auf elektrische Stromnetze entwickelt wurde. Mit dieser Schadsoftware können die ICS von Umspannwerken und anderen elektrischen Einrichtungen direkt manipuliert werden. Sowohl Dragos als auch ESET gehen davon aus, dass die Schadsoftware beim Angriff auf das ukrainische Stromnetz am 17.12.2016 zum Einsatz kam, bei dem ein Umspannwerk in Kiew von einem massiven IT-Angriff betroffen war. Dieser führte zu einem Stromausfall, der über eine Stunde andauerte. /DRA20r01/, /ESE17r01/

Beschreibung

Die Schadsoftware Crashoverride bietet die Möglichkeit, Schalter und Trennschalter in Umspannwerken direkt zu kontrollieren. Beim Angriff auf das Umspannwerk in Kiew wurden die Handlungsoptionen, die Crashoverride den Angreifern bereitstellt, nicht voll ausgeschöpft. Daher geht Dragos davon aus, dass es sich bei diesem Angriff lediglich um einen Test der Schadsoftware gehandelt hat. /DRA20r01/

Crashoverride ist modular aufgebaut und kann daher durch zusätzliche Module erweitert werden. Somit sind nach Einschätzung der Analysten weitere Angriffsmöglichkeiten denkbar. Die wichtigsten Komponenten der Schadsoftware sind eine Komponente zur Etablierung einer Backdoor, ein Launcher, verschiedene Payloads, ein Werkzeug zur Durchführung von DoS-Angriffen und eine Data-Wiper-Komponente, mit der die Angreifer versuchen, ihre Spuren zu verwischen. /DRA20r01/, /ESE17r01/

Der IT-Angriff auf das Umspannwerk in Kiew wird der APT-Gruppierung ELECTRUM (siehe Kapitel 3.12.6) zugeschrieben, welche nach Einschätzung der Analysten in direkter Verbindung mit der APT-Gruppierung Sandworm (siehe Kapitel 3.12.11) steht. /DRA20r01/

Kerntechnischer Bezug

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

B.8.2 Mirai – IT-Angriff auf IoT-Systeme

Überblick

Bei Mirai handelt es sich um eine auf IoT spezialisierte Schadsoftware, die gezielt nach smarten Geräten wie beispielsweise Routern, Kameras oder Fernsehgeräten, die über das Internet erreichbar sind, sucht und diese infiziert. Infizierte Geräte melden sich bei einem Command-and-Control-Server an und werden so Teil eines Botnetzes. Damit können sie von den Angreifern, die das Botnetz kontrollieren, manipuliert und benutzt werden, beispielsweise zur Durchführung von DDoS-Angriffen.

Beschreibung

Infektionen mit der Schadsoftware Mirai können ohne Nutzerinteraktion auftreten, d. h. ohne, dass der Nutzer die Schadsoftware herunterlädt oder ausführt. Laut BSI sind prinzipiell alle IoT-Geräte gefährdet, „die keinen Passwortschutz haben oder ein schwaches Passwort (z. B. Werks-/Standardpasswörter) verwenden“ /BSI20w04/. Vorrangiges Ziel von Mirai sind dabei Linux-basierte Systeme. Infektionen mit Mirai verlaufen typischerweise unbemerkt. Die Infektion ist nicht persistent, sondern existiert vollständig im flüchtigen Speicher der infizierten Systeme. Daher reicht ein Neustart aus, um die Schadsoftware zu entfernen. Dieses Vorgehen schützt verwundbare Systeme aber nicht vor einer Reinfektion. /BSI20w04/

Von Mirai existieren mehrere Varianten. Neben der Suche nach und Infizierung von Geräten mit Standardkennungen und -passwörtern gibt es weitere Angriffsvektoren. Bei einer dieser Möglichkeiten werden Router über die für das Kommunikationsprotokoll TR-069 reservierten Ports 7547 und 5555 infiziert.

In einer Cyber-Sicherheitswarnung /BSI16i01/ beschreibt das BSI eine Mirai-Version, welche das Kommunikationsprotokoll TR-064 verwendet, das eigentlich für lokale Wartungsarbeiten und die Konfiguration der Router verwendet wird.

Die entsprechende Schnittstelle sollte nicht über das Internet erreichbar und durch eine Authentifizierung gesichert sein. Dies ist aber nicht bei allen Gerätetypen gegeben, was einen Zugriff über den Port 7547 ermöglicht. Daher enthalten neuere Versionen des Mirai-Botnetzes Module, die nach offenen TR-069 Ports suchen. /BSI16i01/

Eine weitere Version nutzt eine Debug-Schnittstelle, die bei manchen Android Geräten fälschlicherweise offen ist. Bei den betroffenen Geräten ist die Schnittstelle über den Port 5555 erreichbar und es können ohne Authentifizierung Befehle auf den Geräten ausgeführt und Programme installiert werden. Eigentlich sollte die Schnittstelle deaktiviert sein (und eine Aktivierung sollte nur über eine USB-Verbindung möglich sein). Allerdings ist dies bei nicht allen Geräten der Fall. Betroffen sind dabei verschiedenste Geräte wie Smartphones, digitale Videorekorder oder Fernseher. Bei diesem Angriff scheint das Ziel nicht eine Etablierung eines Botnetzes, etwa zur Vermietung für weitere Angriffe zu sein, sondern die Geräte zum Generieren von Kryptowährungen zu nutzen. Die Verbindung zu den vorigen Angriffen besteht darin, dass anscheinend eine modifizierte Version des Mirai Codes genutzt wird. /DOU18w01/

Neben den Varianten, die Linux-Systeme als Ziel haben, existiert seit 2017 auch eine Version, die Windows Systeme, insbesondere über ungesicherte SQL-Server, angreift. Ziel dieser Angriffe scheint aber nicht die Infektion der Server, sondern der Zugriff auf die Datenbanken zu sein. Des Weiteren findet auch eine Verbreitung von Mirai durch Windows-Hosts, über bereits bestehende Botnetze, statt. Hierbei werden wie gehabt Linux-Systeme angegriffen, im Unterschied zu früheren Versionen von Mirai kann der Angriff aber auch von einem Windows-Host gestartet werden. /SEC17w01/

Darüber hinaus gibt es noch weitere Varianten, die jeweils verschiedene Angriffspfade benutzen. Gemeinsam ist den Angriffen jeweils das Ausnutzen von Schwachstellen von Geräten, die aus dem Internet öffentlich zugänglich sind.

Durch die Heterogenität der Angriffe und deren Ziele ist es schwer direkte Folgen anzugeben. Die verschiedenen zuvor aufgeführten Angriffe gleichen sich zwar bis zu einem gewissen Grad in der Art des Angriffs und teilen oft auch Teile des Codes (der öffentlich

verfügbar ist), jedoch scheint es, als würden die Angriffe mit unterschiedlichen Zielen und wahrscheinlich auch durch unterschiedliche Akteure durchgeführt.

Im Falle der Etablierung eines Botnetzes dient das Netz als Infrastruktur für weitere Angriffe, insbesondere DDoS-Attacken.

Der tatsächliche entstandene Schaden hängt nicht nur von den direkten Folgen, sondern vornehmlich auch von den folgenden Angriffen durch das Botnetz ab. Angriffe wurden dabei unter anderem auf die Webseiten von GitHub, Twitter, Netflix, Airbnb, aber auch die deutsche Telekom durchgeführt. /REG16w01/

Mit Hilfe des Mirai-Botnetzes wurden mehrere erfolgreiche DDoS-Angriffe durchgeführt, die alle bis dahin verzeichneten DDoS-Angriffe hinsichtlich ihrer Bandbreite übertrafen. Hierzu zählt neben dem viel beachtete DDoS-Angriff auf den Blog des IT-Sicherheitsspezialisten Brian Krebs im September 2016 (620 Gbps) vor allem der DDoS-Angriff auf das US-Unternehmen Dyn, das zum Zeitpunkt des Angriffs weite Teile der Domain Name System (DNS) Infrastruktur kontrollierte. Letzterer Angriff führte im Oktober 2016 zu einem Zusammenbruch des Internets in weiten Teilen Europas und der USA. /SSL20w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9 2017

B.9.1 Ccleaner Hack – IT-Angriff über schadsoftwarebehaftete Ccleaner Version

Übersicht

Der als Ccleaner Hack bekanntgewordene IT-Angriff war ein spezialisierter Supply-Chain-Angriff, welcher am 13. September 2017 der Öffentlichkeit vorgestellt wurde. Ccleaner ist ein kostenlostes Programm zur Optimierung von Betriebssystemen, welches bis zum 18. Juli 2017 vom IT-Unternehmen Piriform entwickelt wurde und nach dem Kauf Piriforms durch das IT-Sicherheitsunternehmen Avast weiter von Avast entwickelt und angeboten wurde. Ccleaner wurde bis zum bekanntgewordenen IT-Angriff über 2 Milliarden Mal von Nutzern heruntergeladen und ist weltweit verbreitet.

Beschreibung

Die forensischen Untersuchungen haben ergeben, dass ab dem 11. März 2017 IT-Angreifer Zugriff auf die IT-Umgebung des Entwicklers hatten. Die hierfür notwendigen Zugriffsdaten sind womöglich bei einem früheren IT-Angriff entwendet worden. Mit der umfassenden Schadsoftware Shadowpad, welche aus einer Backdoor sowie Manipulationswerkzeugen, die sich dieser Backdoor ermächtigen besteht, griffen die IT-Angreifer auch auf den sogenannten Build-Server des Ccleaner zu. Der Build Server wird in der Softwareentwicklung zur Versionskompilierung verwendet, sodass die IT-Angreifer eigene Ccleaner Versionen entwickeln und auf dem Build-Server unbemerkt platzieren konnten. Schließlich wurde ab dem 2. August 2017 von den Angreifern eine eigene manipulierte Version von Ccleaner auf den Servern von Avast zur Verfügung gestellt, welche bis zum3. September 2017, dem Tag der Entdeckung, über 2 Millionen Mal heruntergeladen wurde. /WIR18r01/

Die manipulierten Versionen von Ccleaner waren für Nutzer und Antivirensoftware nicht direkt erkennbar, da die Programmierer für die Schadsoftware die Zertifikate von Ccleaner anwendeten und ihre Schadsoftware so in den Programmcode einpflegten, dass keine Abweichungen zu nicht manipulierten Versionen auffielen. Die Schadsoftware wurde mehrstufig aufgebaut, wobei die ersten zwei Stufen der Systemidentifikation dienten und in den manipulierten Versionen von Ccleaner integriert waren.

Darauf aufbauend wurde dann die dritte Stufe, die Schadsoftwarekomponente Shadowpad, heruntergeladen und ggf. durch die Angreifer aktiviert. Mit Shadowpad werden z. B. sämtliche Eingaben in gängige Programme ausgelesen, um Passwörter in Erfahrung zu bringen. Shadowpad bietet aber auch die Möglichkeit, weitere Schadmodule herunterzuladen und zu nutzen. Die Command-and-Control-Server der Angreifer wurden am 16. September 2017 von der US-amerikanischen Bundespolizei stillgelegt und es wurde in Erfahrung gebracht, dass auf insgesamt 40 PCs Aktivierungsbefehle für höhere Stufen der Schadsoftware eingegangen waren. Die betroffenen IT-Systeme gehörten zu elf verschiedenen Unternehmen wie Google, Cisco, Intel, Samsung oder Gauselmann. /INS18r01/

Bei Ccleaner Hack handelt sich damit um einen sehr spezifischen Supply-Chain-Angriff, der eine weit verbreitete legitime Software nutzte, um gezielt ausgewählte IT-Systeme mit potenter Schadsoftware unerkannt anzugreifen. Ähnliche Vorgehensweisen wurden in weiteren IT-Angriffen unterschiedlichen Ausmaßes angewendet.

So beim Shadowhammer genannten IT-Angriff 2018 (siehe Kapitel B.10.1), bei welchem die Angreifer die Kontrolle über die Updateroutinen der Steuerungssoftware des PC-Herstellers ASUSteK Computer Inc. (ASUS) erlangten und über 600 Systeme, identifiziert mittels der MAC-Adresse, mit mehrstufiger Schadsoftware angriffen. /KAS19r01/ Einen ähnlich aufgebauten IT-Angriff, jedoch mit deutlich größerem Ausmaß und Wirkung, stellt der SolarWinds Angriff im Jahr 2020 dar (siehe Kapitel B.12.4). Bei diesem wurden ebenfalls die Updates einer legitimen Software mit Schadsoftware versehen, jedoch gehören über 18.000 Unternehmen, Behörden, Geheimdienste und weitere kritische Stellen zu den Kunden, welche das mit Schadsoftware versehende Update erhalten haben.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.2 Triton/TriSIS – IT-Angriff auf Petro Rabigh

Überblick

Im Juni und August des Jahres 2017 kam es in einer petrochemischen Anlage in Saudi-Arabien in Folge der Manipulation von Steuerungen von Sicherheits- und Schutzsystemen der Anlage mit der Schadsoftware Triton/TriSIS zu mehreren Schutzabschaltungen von sicherheitsrelevanten verfahrenstechnischen Prozessen /FIR17w01/, /GUT19w01/.

Beschreibung

Bei der breit angelegten forensischen Analyse zu diesem IT-Sicherheitsvorfällen wurde die inzwischen als Triton/TriSIS bekannte Schadsoftware im Image einer dem Safety Instrumented System (SIS) zugeordneten Engineering Workstation gefunden. Zusätzlich wurde unbekannte Software im Speicher aller betroffenen Controller des SIS aufgefunden /GUT19w01/. Ausgehend von der Kompromittierung des SIS und daraus resultierenden potenziellen Auswirkungen auf die Ausführung von Sicherheits-, Sicherungs- und Schutzfunktionen, wurden die rechnerbasierten und programmierbaren Systeme der betroffenen Anlage flächendeckend auf das Vorhandensein weiterer Schadsoftware untersucht /GUT19w01/.

Hierbei wurde festgestellt, dass neben dem SIS auch das industrielle Steuerungssystem zur Steuerung des verfahrenstechnischen Prozesses, das in der betroffenen Anlage im Gegensatz zum SIS nicht von Schneider Electric, sondern von einem anderen Hersteller stammte /SCH18w02/, kompromittiert war /MID18w01/, /CON18w01/.

Insgesamt wurde im Rahmen der Untersuchungen zum IT-Sicherheitsvorfall im August des Jahres 2017 festgestellt, dass die Angreifer bereits im Jahr 2014 Zugriff auf das Anlagennetzwerk erlangt und sich fortan schrittweise langsam und unentdeckt im Anlagennetzwerk ausgebreitet hatten. /MIT19w01/

Aus den der GRS vorliegenden Informationen geht hervor, dass es sich bei Triton/TriSIS um eine hochentwickelte Schadsoftware handelt, die ähnlich wie Stuxnet, Havex, BlackEnergy und Industroyer/Crashoverride auf industrielle Steuerungssysteme (Industrial Control Systems, ICS) von kritischen Infrastrukturen ausgerichtet ist. Im Unterschied zu den genannten Vertretern von ICS-angepasster Schadsoftware, die vor allem auf die

Manipulation industrieller Steuerungssysteme zur Prozesssteuerung ausgerichtet sind, zielt Triton/TriSIS jedoch als bisher einzige bekannt gewordene Schadsoftware auf die Manipulation derjenigen industriellen Steuerungssysteme, die Sicherheits-, Sicherungs- oder Schutzfunktionen ausführen und entsprechende Schutzaktionen auslösen (SIS, Safety Instrumented System). Mit Hilfe von Triton/TriSIS sind daher nicht nur Beschädigungen von Komponenten oder die Abschaltung industrieller Prozesse denkbar, sondern prinzipiell auch die Manipulation von SIS bei gleichzeitiger Herbeiführung von unsicheren Anlagenzuständen. Die Schadsoftware Triton/TriSIS deckt hierbei nicht den gesamten IT-Angriff ab, sondern stellt einen wesentlichen Baustein innerhalb eines komplexen, mehrstufigen IT-Angriffs dar.

Hierbei beschränken sich die Möglichkeiten von Triton/TriSIS nicht auf die Verhinderung des Eingriffs von Systemen, die Sicherheits-, Sicherungs- oder Schutzfunktionen ausführen, oder die Herbeiführung einer Fehlauslösung solcher Funktionen. Die Schadsoftware Triton/TriSIS ist vielmehr auf die Einrichtung einer Backdoor innerhalb von Controllern eines SIS ausgerichtet, welche den Angreifern erlaubt, die uneingeschränkte und unbemerkte Kontrolle über das SIS zu erlangen und heimlich beliebige Manipulationen an Sicherheits-, Sicherungs- oder Schutzfunktionen mit sehr ernsten potenziellen Auswirkungen durchzuführen. /MID18w01/, /FIR19w01/, /DRA19r01/

Zwischenzeitlich wurden ein weiterer IT-Sicherheitsvorfall im Zusammenhang mit Triton/TriSIS (siehe Kapitel B.11.3) und weitere Aktivitäten der Angreifer bekannt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r01/. Zudem wurde die Weiterleitungsnachricht 2021/01 verfasst /GRS21i01/.

B.9.3 Karagany.B und Heriplor – Zweite IT-Angriffswelle durch APT Dragonfly

Übersicht

Bei den IT-Angriffen durch Dragonfly (für weitere Informationen über die APT-Gruppierung siehe Kapitel 3.12.5) handelt es sich um hochentwickelte, mehrstufige Angriffe /BSI20i01/. Die APT-Gruppierung setzt dabei ein breites Spektrum an IT-Angriffswerkzeugen und Schadsoftwarekomponenten ein. Auch verfolgt Dragonfly eine effektive Strategie bei der Kompromittierung von Zielnetzwerken über die Lieferkette einzelner Systeme.

Beschreibung

Bislang werden Dragonfly zwei Angriffswellen zugeordnet. Die zweite Angriffswelle wird ab 2015 ausgemacht und erreichte 2017 einen vorläufigen Höhepunkt, dauert aber nach wie vor an /SYM14r01/, /BSI20i01/ (für Informationen zur ersten Angriffswelle siehe Kapitel B.6.3, für Informationen zur APT-Gruppierung Dragonfly siehe Kapitel 3.12.5). Auch bei diesen Angriffen handelt es sich um mehrstufige, komplexe Angriffe, die anschließend an erste Aufklärungsschritte zunächst Spear Phishing und Watering-Hole-Techniken nutzen. Darauf aufbauend setzen die Angreifer eine Vielzahl an Methoden ein, um Remote Zugriff auf die Zielnetzwerke zu erlangen und sich dort weiter auszubreiten. Berichtet wird hierzu beispielsweise von Man-in-the-Middle Angriffen, Passwort Cracking Methoden, Credential Harvesting und Brute-Force-Angriffen auf Fernwartungsprotokolle. Zur Einschleusung von Schadcode nutzen die Angreifer beispielsweise kompromittierte LNK-Dateien. Auch wird vom unautorisierten Einsatz von Red Team Tools[15] zur weiteren Ausbreitung im Zielnetzwerk, der Manipulation von Firewalls zur Etablierung von dauerhaften Remote-Zugriffen und unautorisierten Änderungen der Konfiguration der Netzwerkkomponenten zur Umleitung des Datenverkehrs über von den Angreifern kontrollierte Systeme berichtet. /BFV18r01/

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

Nach Erlangung und Verfestigung des entsprechenden Zugriffs setzen die Angreifer beispielsweise Schadsoftwarekomponenten zur Etablierung von Backdoors ein, auch mehrere parallel. Konkret genannt werden verschiedene Schadsoftwarekomponenten wie Godoor, Dorshel, Karagany.B und Heriplor /SYM17r01/. Wie bei Havex (siehe Kapitel 3.12.5) handelt es sich bei Heriplor um eine maßgeschneiderte Schadsoftware, die anderen Angreifergruppierungen bislang nicht zugänglich ist. Analysten gehen davon aus, dass Heriplor auf Basis des Codes von Havex entwickelt wurde /SYM17r01/, /SEC19w02/. Bei Karagany.B handelt es sich um eine Weiterentwicklung der bei der ersten Angriffswelle eingesetzten Schadsoftwarekomponente Karagany. Neben diesen Schadsoftwarekomponenten verwendeten die Angreifer für die einzelnen Angriffsschritte noch weitere, maßgeschneiderte Angriffswerkzeuge sowie frei oder kommerziell verfügbare Werkzeuge /CIS18r01/. Darüber hinaus bedient sich die APT-Gruppierung sogenannter Living-off-the-Land-Techniken, bei denen legitime im Anlagennetzwerk vorhandene Systeme für maliziöse Handlungen eingesetzt werden /BSI20i02/.

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

Bei den eigentlich anvisierten Zielen liegt der Fokus der Angreifer nach bisherigen Erkenntnissen auf dem systematischen Ausforschen der Zielnetzwerke. Hierbei werden gezielt Informationen über Nutzer, Hosts und die Netzwerkumgebung gesammelt und aufgelistet. Auch werden Nutzeraktivitäten erfasst, einschließlich aktueller Bildschirminhalte. Die Angreifer erfassen insbesondere auch Informationen zu den industriellen Steuerungssystemen wie Konfiguration und Zugriffsinformationen sowie Informationen zu deren Bedienung einschließlich der Erfassung von Screenshots während des Betriebs. /CIS18r01/

Im Rahmen der zweiten Angriffswelle werden vornehmlich Unternehmen im Energiesektor einschließlich der kerntechnischen Industrie sowie der Öl- und Gasindustrie angegriffen. Die Angriffe konzentrieren sich auf Unternehmen in Europa und den USA, betroffen sind aber auch einige asiatische Länder /CYC18w01/. Das BSI berichtet, dass es im Rahmen der zweiten Angriffswelle durch Dragonfly auch zur Kompromittierung von Unternehmen in Deutschland gekommen ist /BSI20i01/.

Kerntechnischer Bezug

Im Rahmen der zweiten Angriffswelle kam es auch zu mindestens einem Angriff auf eine kerntechnische Anlage. Betroffen war das US-amerikanische Kernkraftwerk Woolf Creek. In einer ersten Reaktion gab die Anlage an, die möglichen Auswirkungen des Angriffs sei auf administrative und geschäftliche Teile des Anlagennetzwerks beschränkt, die Untersuchungen seien aber noch nicht abgeschlossen /NYT17w01/. Aus Sicht der GRS besteht eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r11/.

B.9.4 WannaCry – Globaler IT-Angriff

Übersicht

Ab dem 12. Mai 2017 infizierte die Ransomware mit dem Namen WannaCry, WCry, WannaDecryptor Computer weltweit. WannaCry ist eine Schadsoftware, die von Erpressern eingesetzt wird, um Computerdateien zu verschlüsseln und für die Entschlüsselung Lösegeld (engl. ransom) in Form von Bitcoins zu fordern /CIS17i02/.

Beschreibung

WannaCry greift Rechner mit dem Windows Betriebssystem an, wobei die Malware eine Schwachstelle im Windows Server Protokoll nutzt. Dabei waren in der überwiegenden Mehrheit (98 %) Computer mit dem Betriebssystem Windows 7 betroffen, die das wenige Wochen zuvor zur Verfügung gestellte Patch der Schwachstelle noch nicht eingespielt hatten /HEI17w01/. Zum damaligen Zeitpunkt war Windows 7 das am meisten genutzte Betriebssystem noch vor Windows 10. Etwa 0,1 % der Infektionen betrafen das veraltete Betriebssystem Windows XP. Laut Microsoft wurden keine Windows 10 Rechner von WannaCry infiziert /MIC17r01/.

Zunächst wurde angenommen, dass die initiale Infektion eines Computernetzwerkes über E−Mails mit maliziösem Anhang oder Link erfolgt, wie es für Ransomware typisch ist. Es zeigte sich jedoch, dass die initiale Infektion eines Computers über einen Angriff auf den Server aus dem Internet erfolgt, indem eine Schwachstelle im Windows Server Protokoll SMBv1 (Server Message Block) (CVE-2017-0144 /NVD18w01/) ausgenutzt

wurde. Der Server Message Block ist ein Netzwerkprotokoll von Microsoft für Zugriffe auf Dateien und Serverdienste in Rechnernetzen /BSI17i01/.

Sobald ein Rechner mit der Schadsoftware befallen ist, kann sich WannaCry weiter über lokale Netzwerke ausbreiten, da WannaCry laut Microsoft entsprechende Wurmeigenschaften besitzt. Aufgrund dieser Eigenschaft konnte sich WannaCry sehr schnell verbreiten und durch eine initiale Infektion eines Rechners im Netzwerk das gesamte Netzwerk kompromittieren /MIC17r01, BSI17i01/.

Der erste Schritt bei einer Infektion mit WannaCry erfolgt über eine eigenständig ausführbare Programm Datei (sog. Dropper), welche das Exploit EternalBlue verwendet. EternalBlue nutzt die oben genannte Sicherheitslücke des Protokolls SMBv1, um sich Zugang zum Computersystem zu verschaffen (nähere Informationen s. u.) /CIS17r01/, /MAL17w01/. Dieser Dropper enthält einen sog. Killswitch, der von den Entwicklern als eine Art Notausschalter programmiert wurde, um die Schadsoftware zu stoppen. Dabei schickt der Dropper eine Anfrage an eine Internetseite (www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com). Kann eine Verbindung zu dieser Seite hergestellt werden, wird der Dropper nicht weiter ausgeführt und die Infektion des Computers wird gestoppt /CIS17r01/, /HEI17w03/, /MAL17w01/. Erfolgt keine Verbindung, wird der Computer mit der Schadsoftware infiziert, indem ein Service (mssecsvc2.0) gestartet wird, der alle IP−Adressen des lokalen Netzwerkes des infizierten Computers scannt und versucht, sich mit dem TCP Port 445 (SMB) jeder IP−Adresse zu verbinden. Gelingt es der Malware, unter der Ausnutzung der SMBv1 Schwachstelle auf einen Rechner zu gelangen, wird eine ausführbare Datei auf dem System installiert. Die ausführende Datei tasksche.exe sucht Dateien auf der Festplatte, den Netzlaufwerken und den Wechselspeichergeräten, die dann mit einem kryptographischen Verfahren verschlüsselt werden. Dabei können etwa 120 unterschiedliche Dateiformate verschlüsselt werden, darunter Text-, Audio-, Video- und Bilddateien. Zudem werden durch zwei weitere ausführbare Dateien taskdl.exe und taskse.exe alle temporären Dateien (mit denen eine Wiederherstellung der Dateien möglich wäre) gelöscht und eine Bildschirmanzeige mit der Lösegelderpressung angezeigt /CIS17r01/. Die von WannaCry ausgenutzte Sicherheitslücke SMBv1 wurde vom US-amerikanischen Auslandsgeheimdienst (NSA) entdeckt und mit dem Zero-Day-Exploit EternalBlue SMBv1 über drei Jahre lang verwendet ohne Microsoft über die Schwachstelle zu informieren. Erst als dieses Wissen von der Angreifergruppierung Shadow Brockers gestohlen wurde, informierte die NSA Microsoft über die Sicherheitslücke /NYT17w02, HEI17w04/.

Daraufhin wurde am 14. März 2017 ein Patch für Windows Vista, Windows 7, Windows 8.1, Windows 10 sowie Windows Server 2008 zur Verfügung gestellt. Später folgten auch Patches für Windows XP, Windows 8 und Windows Server 2003.

Betroffen von den IT-Angriffen mit der Ransomware WannaCry waren laut Medienberichten Computer unterschiedlicher Organisationen in über 150 Ländern, u. a. Deutschland, Frankreich, Großbritannien, Japan, Russland, Spanien, Taiwan und USA. Darunter sind das Innenministerium in Russland mit 1000 infizierten Rechnern, der National Health Service in Großbritannien (NHS), wodurch in vielen Krankenhäuser die Behandlung von Patienten erheblich beeinträchtigt wurde /BSI17i01/, /HEI17w05/, /MAL17w01/. Die Autohersteller Nissan (in Großbritannien) und Renault (in Frankreich), der Flugzeughersteller Boeing, die Netzbetreiber Telefónica (in Spanien) und Telecom (in Portugal), das Logistikunternehmen FedEx (USA) und sowie die Deutsche Bahn, deren Anzeigetafeln und Fahrscheinautomaten betroffen waren. /HEI17w05/, /HEI17w06/, /SEA17w01/

Laut Forbes /FOR17w01/ waren auch zahlreiche medizinische Einrichtungen in den USA betroffen. Dabei waren nicht nur Bürorechner infiziert, sondern auch medizinische Geräte, auf denen das Microsoft Betriebssystem lief und die sich im Netzwerk befanden. Als Beispiel wurde ein Überwachungssystem zur Injektion von Kontrastmittel bei Magnetresonanztomographie von Bayer genannt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.5 Bad Rabbit – Globaler IT-Angriff

Übersicht

Im Oktober 2017 wurde bekannt, dass osteuropäische Unternehmen und Behörden vor allem in der Ukraine und Russland Opfer einer IT-Angriffswelle mit der Ransomware BadRabbit wurden. Betroffen waren unter anderem eine russische Nachrichtenagentur, die U-Bahn in Kiew und der Flughafen in Odessa. Es folgten außerdem weitere IT-Angriffe auf Ziele in mehreren europäischen Staaten (darunter Deutschland), Japan, den USA und weiteren Staaten.

Die Ransomware gelangte vermutlich über Watering-Hole-Angriffe, bei denen von Zielpersonen besuchte Webseiten mit Schadsoftware infiziert waren, auf die Systeme der Opfer. Dabei wurden die Opfer über ein manipuliertes Skript zur angeblichen Installation bzw. zum Update des Adobe Flash-Players aufgefordert, woraufhin die Schadsoftware auf das System des Opfers gelangte und mit der Verschlüsselung der Daten begann. /AIR17w01/, /TRE17w01/

Beschreibung

Nachdem die Schadsoftware BadRabbit auf das Zielsystem gelangt ist, nutzt sie das frei verfügbare IT-Angriffswerkzeug Mimikatz, um die lokalen Anmeldeinformationen der Benutzer oder Administratoren zu extrahieren. Dabei handelt es sich um ein für IT-Angriffe oftmals verwendetes Programm, welches verwendet werden kann, um bei Windows-Systemen unter Ausnutzung einer Schwachstelle an zwischengespeicherte Anmeldeinformationen zu gelangen. Mimikatz wurde u. a. beispielsweise beim NotPeyta-Angriff im Jahr 2017 eingesetzt. BadRabbit nutzt anschließend das frei verfügbare Programm DiskCryptor, um die Daten des infizierten Systems zu verschlüsseln. Die Verschlüsselung umfasst die meisten gängigen Dateitypen wie beispielsweise Microsoft Office Dateien, PDF-Dateien und Bilddateien. Außerdem wird der Master Boot Record (MBR) verschlüsselt, der das Startprogramm für BIOS-basierte Computer enthält. Nachdem die Daten verschlüsselt wurden, startet BadRabbit das System neu und das Opfer bekommt eine Lösegeldforderung angezeigt, indem eine Zahlung in Bitcoins verlangt wird, um die Daten entschlüsseln zu können. Die Schadsoftware ist in der Lage, sich über das Netzwerk im System des Opfers zu verbreiten und so weitere Computer zu infizieren. Dabei wird unter anderem eine modifizierte Version des Exploits Eternal-Romance genutzt. /AIR17w01/, /TRE17w02/

Die Behörde für nationale Cybersecurity des Vereinigten Königreichs, das National Cyber Security Centre (NCSC), vermutet, dass die APT-Gruppierung Sandworm (siehe Kapitel 3.12.11) für die IT-Angriffe mit der Ransomware BadRabbit verantwortlich ist /NCS18i02/.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.9.6 NotPetya – IT-Angriffe auf ukrainische Behörden, Infrastruktur und weltweite Unternehmen

Übersicht

Am 27. Juni 2017 waren weltweit Unternehmen und Organisationen von einem massiven Ausfall ihrer Informationsinfrastruktur betroffen, nachdem unbekannte Angreifer bereits im Frühjahr 2017 Zugriff auf die Server des Unternehmens Linkos Group erlangt und unbemerkt die Kontrolle über die Updateserver für das Programm M.E.Doc des Unternehmens übernommen hatten. M.E.Doc ist eine in der Ukraine weit verbreitete Software zur Unterstützung der Erstellung von Steuerabrechnungen und -erklärungen, welche von vielen in der Ukraine tätigen ausländischen Unternehmen und Konzerntöchtern verwendet wird. Der NotPetya-Angriff erfolgte somit über die Lieferkette. Hauptsächlich galt der Angriff Firmen und Regierungsbehörden in der Ukraine, darunter die Post, das Metrosystem in Kiew, ukrainische Banken und das ukrainische Stromnetzunternehmen Kievenergo. Das Kernkraftwerk Tschernobyl war ebenfalls betroffen, bei dem infolge des IT-Angriffs die Strahlungsüberwachung manuell durchgeführt werden musste. Besonders betroffen von dem IT-Angriff war außerdem das dänische Logistikunternehmen Maersk. /CNN17w01/, /NYT17w03/, /GUA17w01/

Beschreibung

Die Angreifer luden auf die betroffenen Systeme per Softwareupdate die Schadsoftware NotPetya hoch und aktivierten diese zeitgleich am 27. Juni 2017. Diese Schadsoftware, auch unter dem Namen Wiper geführt, wird teilweise der Schadsoftware Petya, einem klassischen Verschlüsselungstrojaner, zugeordnet, unterscheidet sich aber in wesentlichen Punkten fundamental von diesem.

Beispielsweise ist das Ziel beim NotPetya-Angriff keine Lösegeldzahlung der Opfer, sondern die Verschlüsselung der Daten der Opfer ohne Möglichkeiten der Entschlüsselung, sodass die betroffenen Daten verloren und die Systeme unzugänglich sind. Die Schadsoftware NotPetya breitete sich in den betroffenen IT-Netzwerken aus, vernichtete sämtliche gespeicherte Daten der betroffenen Systeme und versuchte, weitere IT-Systeme zu infizieren. IT-Analysten rechnen den Angriff dem russischen Militär zu, mit dem Ziel, Schadsoftware auf den Computern der ukrainischen Regierung und Unternehmen zu installieren. Durch die Aktivitäten internationaler Unternehmen in der Ukraine, konnte sich die Schadsoftware dann verbreiten.

Innerhalb weniger Tage entstand weltweit ein wirtschaftlicher Schaden von mehreren Milliarden Dollar. Die Schadsoftware verwendet das aus dem Arsenal der National Security Agency (NSA) der USA gestohlene IT-Angriffswerkzeug EternalBlue, welches eine Microsoft Windows Schwachstelle ausnutzt. /CNN17w01/, /NYT17w03/, /BUS17w01/, /CNE18w01/

Ein umfassendes Beispiel der Schadwirkung von NotPetya ist die Zerstörung des Firmennetzwerkes bei dem Logistikunternehmen Maersk. Eine Niederlassung von Maersk in der Ukraine nutzte die Software M.E.Doc für ihre Abrechnungen. Von dort ausgehend verbreitete sich NotPetya im gesamten Netzwerk des Unternehmens, das aus über 80.000 IT-Systemen besteht. Jedes IT-System wurde infiziert und dessen gespeicherte Dateien unwiderruflich zerstört. Die weitere Ausbreitung der Schadsoftware umfasste u. a. das französische Baustoffunternehmen Saint-Gobain, die britische Werbeagentur WPPGY, die russischen Unternehmen Rosneft (Öl und Gas), Gazprom (Gasunternehmen) und die Bank Home Credit, das Stahl- und Bergbauunternehmen Evraz, das Gesundheitsunternehmen Heritage Valley Health Systems in Pennsylvania, die globale Transportfirma FedEx, das Pharmaunternehmen Merck, das Unternehmen Mondelez (MDLZ) (dem weltweit Unternehmen zur Herstellung von Süßwaren wie Oreos und Cadbory angehören) und die Anwaltskanzlei DLA Piper. /CNN17w01/, /NYT17w03/

Kerntechnischer Bezug

Mit dem Ausfall der Strahlungsüberwachung im Kernkraftwerk Tschernobyl, welche daraufhin manuell durchgeführt werden musste, hat der IT-Angriff einen direkten Bezug zu kerntechnischen Anlagen. /PRV17r01/

B.10 2018

B.10.1 Shadowhammer – IT-Angriff über schadsoftwarebehaftete ASUS Steuerungssoftware

Übersicht

Bei dem als Operation Shadowhammer genannten IT-Angriff handelt es sich um einen typverwandten oder womöglich Nachfolgeangriff zum beschriebenen Ccleaner IT-Angriff (siehe Kapitel B.9.1).

Im März 2019 veröffentlichte Kaspersky Labs zu einem bis dahin unbekannten Supply-Chain-Angriff einen umfassenden Bericht, welcher das unter dem Markennamen ASUS auftretende Unternehmen ASUSTeK Computer Inc. betraf.

Beschreibung

Im Verlauf des Jahres 2018 sicherten sich die IT-Angreifer Zugriff auf die Webseite von ASUS, auf welcher dieser eine Steuerungssoftware für seine Kunden zum Herunterladen anbietet. Die IT-Angreifer platzierten beginnend im Juni 2018 unbemerkt eine mit Schadcode versehende Version auf der Webseite. Diese manipulierte Version wurde mit legitimen Zertifikaten ausgestattet und so an Kunden des Unternehmens verteilt. Nach bisherigen Erkenntnissen lief der IT-Angriff vom Juni 2018 bis November 2018 und wurde dann am 29. Januar 2019 entdeckt. /SEN19r01/

Ähnlich zum Ccleaner IT-Angriff diente die initiale Schadsoftwarekomponente ausschließlich der Identifizierung der betroffenen IT-Systeme. Die IT-Angreifer nutzen eine Liste von insgesamt 600 eindeutig zu identifizierenden MAC Adressen unbekannter Herkunft zur Erkennung von IT-Systemen, bei welchen die zweite Schadsoftwarekomponente zum Einsatz kommen sollte. Diese zweite Schadsoftwarekomponente ähnelte der beim Ccleaner Hack eingesetzten Shadowpad Schadsoftware. Zu den Opfern gehören neben ASUS selbst insbesondere IT-Unternehmen aus der Republik China und den USA. /SEN19r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.2 IT-Angriff auf den französischen Baukonzern Ingérop

Übersicht

Im November 2018 wurde bekannt, dass Daten des französischen Baudienstleisters Ingérop, der für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo arbeitet, zunächst teilweise im Internet aufzufinden waren und anschließend ein aus 11.000 Dateien bestehendes Archiv im Darknet angeboten wurde.

Darunter befinden sich nach aktuellem Kenntnisstand auch Daten über französische kerntechnische Anlagen. Nach bisherigen Erkenntnissen wurde Ingérop im ersten Halbjahr 2018 Opfer eines Phishing-Angriffs, bei welchem ein oder mehrere Mitarbeiter des Konzerns mittels fingierter Emails zur Installation einer bisher nicht bekannten Schadsoftware verleitet wurden.

Kerntechnischer Bezug

Der französische Baudienstleister Ingérop, der Opfer des Phishing-Angriffs wurde, arbeitet für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo.

B.10.3 Emotet – Globale IT-Angriffe auf Behörden und Infrastruktur

Übersicht

Bei Emotet handelt es sich um eine erstmalig 2014 beschriebene Schadsoftware des Typs Ransomware mit hohem Schadpotenzial. Emotet zielt hierbei jedoch nicht auf Privatanwender, sondern wurde von seinen Entwicklern immer weiter spezialisiert, um große Firmennetzwerke gezielt angreifen zu können. Aufgrund der rasant gestiegenen Schadwirkung und Fähigkeiten der Emotet-Schadsoftware veröffentlichte das BSI im Jahr 2018 eine Warnmeldung bezüglich Emotet /BSI20r04/. Betroffen waren Krankenhäuser, Stadtverwaltungen, das Medienunternehmen Heise Gruppe, das Berliner Kammergericht, der BwFuhrparkservice und damit der Fahrdienst des Deutschen Bundestages und viele weitere Unternehmen, Institutionen und Verwaltungen in Deutschland und anderen Nationen. /SOP19r01/, /TON20r01/

Beschreibung

Die Gefährlichkeit der Emotet-Schadsoftware nahm im Jahr 2018 insbesondere durch neuere Emotet-Versionen zu, welche in der Lage waren, Emails betroffener IT-Systeme auszulesen und unter Hilfe der ausgelesenen Emails täuschend echte Emails mit kompromittiertem Anhang zu versenden oder gar auf bestehende Emails zu antworten. Empfänger solcher Emails wurden häufig durch die legitimen Titel, Absender, Inhalte und Bezeichnung des Anhangs dazu geführt die zur Installation von Emotet notwendigen

Schritte (Herunterladen der Word-Datei im Anhang, Erlaubnis von Word-Makros) durchzuführen.

Wird Emotet auf einem IT-System ausgeführt, beginnt Emotet umfassende Auswertungen von Eingaben, Auslesung von Emails sowie die eigene Weiterverbreitung über angeschlossene Netzwerke und Emailversendungen. Emotets Kernfunktion ist hierbei die Verschlüsselung sämtlicher angeschlossener Massenspeicher aller betroffener IT-Systeme. Hierdurch kommt es zum Teil zu vollständigen Ausfällen der Netzwerkinfrastruktur oder gar aller vernetzter IT-Systeme der betroffenen Opfer. Einen Schlüssel zur Entschlüsselung erhielten die Opfer nur nach Zahlung einer hohen Geldsumme an die IT-Angreifer. Emotet wurde konstant weiterentwickelt und wurde mit hoher Schadwirkung bis Ende 2020 eingesetzt. /SOP19r01/

Anfang 2021 gelang den deutschen Sicherheitsbehörden BSI und BKA die vollständige Übernahme der Command-and-Control-Server von Emotet. Hierdurch war es den Behörden möglich, die Tätigkeiten von Emotet zunächst zu unterbinden. So wurde über die Command-and-Control-Server ein spezielles Update an alle aktiven Emotet-Versionen versendet, welches zum einen die Emotet-Schadsoftware „quarantänisiert“ und damit inaktiviert, zum anderen aber auch für Antivirensoftware einfach erkennbar macht. Weiterhin wurde die Kommunikation zu einem direkt von den Strafverfolgungsbehörden kontrollierten Server umgeleitet und die Besitzer mit Emotet infizierter Systeme wurden aktiv kontaktiert. Nach Übernahme der Command-and-Control Server von Emotet wurde davon auszugegangen, dass die Aktivitäten von Emotet stark zurückgehen werden und immer mehr Systeme von der Schadsoftware bereinigt werden. /BSI21r01/, /BIT22w02/

Tatsächlich wurden zwischen Januar 2021 und November 2021 keine Emotet Aktivitäten mehr entdeckt. Seit dem vierten Quartal 2021 sind wieder große Angriffswellen unter Nutzung oder Beteiligung der Schadsoftware Emotet und der ihr zugehörigen Emotet-Gruppe entdeckt worden. Hierbei wurden Emotet Funktionen zum einen in die Malware Trickbot übernommen und zum anderen kommt es seit November 2021 zu wiederholten schwerwiegenden Angriffsserien durch Emotet, wobei wieder Emails mit manipulierten Anhängen oder Weblinks zur Verbreitung von Emotet eingesetzt werden. Basierte die Übertragung früher zumeist auf der Nutzung von Macro-Funktionen von MS Office Produkten, hat sich der Angriffsvektor vermehrt zur Ausführung von gefälschten Apps verschoben, z. B. PDF-Lesern sowie Java-Archiven und für Webseitenfunktionen wichtige Javascripts. Die aktuellen weltweiten Infektionswellen mit Emotet zeigen, dass aktuell durch Emotet insbesondere der Abfluss verwertbarer Informationen wie

E-Mail-Passwörter, Kontakte und andere Zugangsdaten als Kernfunktion durchgeführt wird und damit von den betroffenen IT-Systemen neuer glaubwürdiger E-Mail Spam verschickt wird. Einige Emotet-Versionen besitzen die Möglichkeit zum Nachladen von weiteren Schadsoftwares. Gemäß einer Auswertung des IT-Systemherstellers und Dienstleisters HP Inc. ist im ersten Quartal 2022 zu einer 27-fachen Steigerung der Anzahl an Emotet Identifikationen gegenüber dem letzten Quartal 2021 gekommen, womit Emotet zur häufigsten identifizierten Schadsoftware durch HP wurde. /HPW22w01/, /BIT22w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.4 Operation Sharpshooter – Globale IT-Angriffe auf Behörden und Infrastruktur

Übersicht

Operation Sharpshooter wird eine große, international wirkende IT-Angriffsserie professioneller Art genannt, welche von McAfee Global Threat Intelligence 2018 der Öffentlichkeit vorgestellt wurde und im Rahmen eines großen Berichts näher beleuchtet wurde /MCA18r01/. Die Kampagne zielte auf Unternehmen und Behörden im Bereich der kritischen Infrastruktur sowie im Verteidigungsbereich ab. Dabei nutzten die Angreifer beim Cloudspeicheranbieter Dropbox hinterlegte Worddokumente mit Schadcode, welcher mittels Word Macros ausgeführt wurde. Über die Macros wurden dann Alibi-Worddokumente erzeugt, welche zum Herunterladen der eigentlichen Schadsoftware mit dem Namen Rising Sun verwendet wurden. Rising Sun wird zum einen zum Ausspähen von Netzwerken, Computernamen, Nutzernamen, IP-Adressen, Systeminformationen und anderen Informationen verwendet und zusätzlich ist die Schadsoftware in der Lage die gesammelten Daten an einen Command-and-Control-Server zu übertragen und damit zu entwenden. /MCA18r01/

Die beim Angriff hinterlassenen Spuren deuten darauf hin, dass die ATP Lazarus in dieser IT-Angriffsserie involviert ist. Dies ist jedoch keine sichere Erkenntnis, sondern basiert auf Indizien, die auch für die Verwischung der Spuren von IT-Angreifern absichtlich platziert sein könnten. /MCA18r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.10.5 Shamoon v3 – IT-Angriff auf Saipem

Übersicht

Ende des Jahres 2018 wurde eine weitere Variante der Shamoon Schadsoftwarefamilie, Shamoon v3, entdeckt.

Beschreibung

Ziel des Angriffs mit Shamoon v3 war das italienische Öl- und Gasunternehmen Saipem. Angaben von ZDNet zufolge waren etwa 10 % der gesamten Rechnerinfrastruktur von Saipem betroffen, Infektionen wurden sowohl im Mittleren Osten, als auch in Italien, Indien und Spanien vermeldet. Im Gegensatz zu den ersten beiden Angriffen mit Shamoon 2012 und 2016 wurden die Daten auf den betroffenen Rechnern diesmal nicht mit Bilddaten, sondern mit zufälligen, nicht zusammenhängenden Daten überschrieben. /ZDN18w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11 2019

B.11.1 IT-Sicherheitsvorfall durch Cryptomining in KKW Südukraine

Übersicht

Wie die ukrainische Nachrichtenplattform InternetUA im August 2019 berichtete, wurde am 10. Juli 2019 vom ukrainischen Geheimdienst SBU der Verwaltungstrakt des Kernkraftwerks Südukraine durchsucht. Dabei wurden mehrere IT-Systeme beschlagnahmt,

welche für die Generierung (sogenanntes Mining) von digitalen Währungen wie Bitcoins verwendet wurden.

Beschreibung

Digitale Währungen (auch Kryptowährungen genannt) wie Bitcoin oder Dogecoin basieren bei ihrer Generierung auf hochkomplexen Gleichungen, welche mittels stromintensiver Grafikkarten gelöst werden. Die Stromkosten sind daher eine der einflussreichsten Grenzkosten des Minings, wodurch es bereits zu wiederholten Strom- und Rechenzeitdiebstählen in wissenschaftlichen und technischen Einrichtungen kam. /ZDN19r02/

Mitarbeiter des Kernkraftwerks brachten eigene IT-Systeme, sogenannte Miningracks mit mehreren stromintensiven Grafikkarten in den Verwaltungstrakt ein, schlossen diese Systeme an das interne Netzwerk des Verwaltungstrakts und dieses interne Netzwerk wiederum an das Internet an. Es bestand zu keiner Zeit eine Verbindung zwischen dem Netzwerk des Verwaltungstraktes und dem leittechnischen Netzwerk des Kraftwerkes. Nach Berichten wurde weiteres Equipment für die Generierung von digitalen Währungen in den auf dem Kraftwerksgelände befindlichen militärischen Kasernen gefunden. Die militärischen Kasernen werden von der ukrainischen Nationalgarde genutzt, da die Nationalgarde mit dem Schutz des Kraftwerks beauftragt ist. Es ist nicht bekannt, ob Mitglieder der Nationalgarde direkt an dem IT-Ereignis beteiligt waren. /ZDN19r02/

Kerntechnischer Bezug

Der IT-Sicherheitsvorfall ereignete sich in einem Verwaltungstrakt des KKW Südukraine.

B.11.2 IT-Angriff auf KKW Kudankulam

Übersicht

Im September 2019 wurde die Öffentlichkeit durch einen Tweet eines früheren Sicherheitsforschers der indischen nationalen technisch Forschungsorganisation (NTRO) auf einen aktiven IT-Angriff auf das indische Kernkraftwerk Kudankulam (2 russische DWR-Reaktoren) informiert /PUS19w01/.

Beschreibung

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

Der initiale IT-Angriff wurde mit der Verteilung manipulierter Emails durchgeführt. Die IT-Angreifer, welche nach bisherigen Kenntnissen seit mehreren Jahren Informationen zu wichtigen Personen des indischen zivilen nuklearen Programms ausforschten, nutzten ihre Informationen um sich in Emails als Regierungsmitarbeiter auszugeben und per Email Schadcode an Unternehmen und Privatpersonen des indischen zivilen nuklearen Sektors zu verteilen.

Als Schadcode wurde in Folge der Trojaner Dtrack eingesetzt; ein Trojaner für die Aufklärung und das Nachladen weiteren Schadcodes. Dtrack ist zum Auslesen von Tastatureingaben, Browserhistorien, Systeminformationen, Netzwerkinformationen und allen gespeicherten Daten fähig. Die eingesetzte Dtrack-Version basiert auf einem Bankingtrojaner, welcher im Jahr 2016 gegen indische Finanzinstitute angewendet wurde. Die Herkunft des Trojaners und des gesamten IT-Angriffes auf das Kernkraftwerk wird wegen verschiedener Indizien der ATP Lazarus zugeschrieben. /PKM20r01/

Nach bisherigen Informationen erreichten die IT-Angreifer vollumfänglich ihr Ziel. Mit in der Schadsoftware fest eingepflegten, gültigen Zugriffsinformationen konnten sie umfassend auf das administrative Netzwerk zugreifen und Daten aus diesem Netzwerk entwenden. Es wird davon ausgegangen, dass große Datenmengen, die in dem Netzwerk verfügbar waren, entwendet wurden. Es kam zu keinem Angriff oder Zugriff auf die leittechnischen Systeme des Kraftwerks, die Schadsoftware war nicht für solche Zugriffe ausgelegt. /PKM20r01/

Kerntechnischer Bezug

Das Kernkraftwerk Kudankulam war direkt von dem IT-Angriff betroffen und das administrative Netzwerk des Kraftwerks wurde von den Angreifern kompromittiert.

B.11.3 Weiterer IT-Sicherheitsvorfall in Zusammenhang mit Triton/Trisis

Übersicht

Über den in Kapitel B.5.1 beschriebenen IT-Angriff unter Einsatz der Schadsoftware Triton/TriSIS auf eine petrochemische Anlage in Saudi-Arabien hinaus, wurde im April 2019 ein weiterer IT-Sicherheitsvorfall bekannt, bei dem es denselben Angreifern gelungen war, in eine weitere kritische Infrastruktur in Saudi-Arabien einzudringen /FIR19w01/.

Beschreibung

Details zu diesem weiteren IT-Sicherheitsvorfall in Zusammenhang mit der Schadsoftware Triton/TriSIS werden nach wie vor geheim gehalten. Bestätigt ist jedoch, dass es den Angreifern auch hier gelang, sich Zugriff auf das SIS zu verschaffen. Auf Basis der Untersuchung dieses IT-Sicherheitsvorfalls wurden Erkenntnisse zu den IT-Angriffswerkzeugen veröffentlicht, mit denen die APT-Gruppierung in das Netzwerk der betroffenen Anlage eindrang, sich in diesem Netzwerk bewegte und den Einsatz der Schadsoftware Triton/TriSIS vorbereitete /FIR19w01/. Die entdeckten Angriffswerkzeuge sind im Rahmen eines komplexen und mehrstufigen IT-Angriffs, der sich typischerweise über Monate oder Jahre erstreckt, Angriffsschritten zuzuordnen, die zeitlich deutlich früher erfolgt sind als der Einsatz der Schadsoftware Triton/TriSIS selbst. Bemerkenswert ist, dass dabei eine ganze Reihe von Angriffswerkzeugen, darunter auch neue, von den Angreifern maßgeschneiderte Angriffswerkzeuge gefunden wurden.

Die von der IT-Sicherheitsfirma FireEye durchgeführte Analyse /FIR19w01/ dieses IT-Sicherheitsvorfalls zeigt, dass sich die Angreifer fast ein Jahr im Netzwerk der angegriffenen Anlage bewegten, bevor sie Zugriff auf industrielle Steuerungssysteme zur Ausführung von Sicherheits-, Sicherungs- oder Schutzfunktionen erlangten. Nach dem ersten Eindringen ins IT-Netzwerk der Anlage und einer Verfestigung des Zugriffs auf das Anlagennetzwerk lag der Fokus der Angreifer darauf, Zugriff auf die industriellen Steuerungssysteme zu erlangen. Hierzu setzten sie vor allem Werkzeuge zur Ausforschung des Anlagennetzwerks, für die laterale Ausbreitung im Anlagennetzwerk und für die Etablierung dauerhafter Präsenz im Anlagennetzwerk ein.

Zusätzlich nutzten sie eine Reihe von Techniken um ihre Aktivitäten zu verbergen und wie legitime Aktionen erscheinen zu lassen.

Mittels dieser Techniken gelang es ihnen, ihre Spuren zu verwischen, die Identifikation der mit Schadcode behafteten Dateien zu verhindern, sowie eine potenzielle forensische Untersuchung ihrer Werkzeuge zu erschweren. Beispielsweise erlangten die Angreifer zwar Zugriff auf das industrielle Steuerungssystem zur Prozesssteuerung, nutzten diesen zunächst aber weder zur Manipulation der entsprechenden Controller noch zu Spionagezwecken. Nachdem sie Zugriff auf die anvisierten Controller des SIS erlangt hatten, lag der Fokus der Angreifer insbesondere darauf, diesen Zugriff dauerhaft zu erhalten und dort die Schadsoftware Triton/TriSIS einzusetzen. /FIR19w01/

Bisher ist jedoch nicht bekannt, ob es in der Folge zu Manipulationen oder Störungen von Sicherheits-, Sicherungs- oder Schutzfunktionen in der betroffenen Anlage gekommen ist.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS20r01/. Zudem wurde die Weiterleitungsnachricht 2021/01 verfasst.

B.11.4 ZeroCleare – IT-Angriffe auf den Energiesektor im mittleren Osten

Übersicht

Im Jahr 2019 gaben IT-Sicherheitsanalysten von IBM Security die Entdeckung einer neuen Wiper-Schadsoftware bekannt, die in der ersten Jahreshälfte 2019 bei mehreren Angriffen auf den Energiesektor im Mittleren Osten eingesetzt worden war. Die Schadsoftware wird als ZeroCleare bezeichnet.

Beschreibung

Bei ZeroCleare handelt es sich um einen klassischen Wiper, der versucht, auf den infizierten Systemen so viele Daten wie möglich zu löschen, wie sie auch in früheren

Angriffen bereits eingesetzt wurden (siehe Kapitel 3.6). ZeroCleare weist dabei Parallelen zur Schadsoftware Shamoon (siehe Kapitel B.5.1) auf.

So versucht ZeroCleare, genau wie Shamoon, in Windows-basierten Systemen den Master Boot Record (MBR) zu überschreiben und Partitionen zu beschädigen. /IBM20i01/, /ZDN19w01/

Die beschriebenen Angriffe mit ZeroCleare begannen typischerweise mit einem Brute-Force-Angriff, um einen Erstzugriff auf einen Server zu erlangen. Anschließend nutzten die Angreifer eine Schwachstelle in SharePoint aus, um Schadsoftwarekomponenten wie beispielsweise China Chopper und Tunna zu installieren. Nach erfolgreicher lateraler Ausbreitung im Zielnetzwerk setzten die Angreifer im letzten Angriffsschritt die Schadsoftware ZeroCleare ein. Wie schon die bislang aufgefundenen Versionen von Shamoon /SEC12w04/ setzt ZeroCleare das von sich aus nicht schädliche Werkzeug EldoS RawDisk auf maliziöse Weise ein, um mit Dateien, Laufwerken und Partitionen zu interagieren und diese letztlich zu zerstören. EldoS RawDisk erlaubt das direkte Ändern von Daten unter Umgehung von Security Features des Windows-Betriebssystems. /IBM20i01/

Nach eingehender Untersuchung der Schadsoftware äußert IBM die Vermutung, dass die Angriffe von iranischen, staatlich geförderten Angreifern durchgeführt wurden. Die Rede ist hierbei von APT34/OilRig sowie mindestens einer weiteren Gruppierung. /IBM20i01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.5 IT-Angriff mit LockerGoga auf Norsk Hydro

Übersicht

Im März 2019 wurde bekannt, dass der norwegische Konzern Norsk Hydro, einer der größten Aluminiumproduzenten der Welt, am 19.03.2020 Opfer eines großangelegten IT-Angriffs mit der Ransomware LockerGoga wurde. Nachdem ursprünglich Unternehmensnetzwerke in den USA betroffen waren, verbreitete sich die Schadsoftware innerhalb von Stunden und betraf auch andere Niederlassungen des Unternehmens, welches in 40 Ländern agiert /GOO19w01/. Norsk Hydro stoppte daraufhin die Produktion in einigen Anlagen oder stellte in betroffenen Anlagen auf manuellen Betrieb um.

Insgesamt waren alle 35.000 Mitarbeiter des Unternehmens betroffen, wobei Daten auf über 1.000 PCs und Servern verschlüsselt wurden und sowohl die Produktion als auch Büro-Netzwerke betroffen waren. Der Vorfall verursachte finanzielle Schäden in Höhe von etwa 71 Millionen Dollar und hatte Auswirkungen auf den weltweiten Aluminium-markt. /BRI19w01/

Beschreibung

Die Schadsoftware LockerGoga wurde erstmals Anfang 2019 bei einem IT-Angriff auf das französische Unternehmen Altran Technologies, das vor allem in der Technologieberatung tätig ist, beobachtet. Altran Technologies veröffentlichte am 28.01.2019 eine Pressemitteilung in der angegeben wird, dass nach ihren Erkenntnissen keine Daten gestohlen wurden und dass sich die Schadsoftware nicht zu ihren Kunden verbreitet hat /ALT19i01/. Neben den Angriffen auf Altran Technologies und Norsk Hydro wurden auch zwei IT-Angriffe auf die europäischen bzw. US-amerikanischen Chemieunternehmen Hexicon und Momentive in 2019 bekannt, bei der die Schadsoftware LockerGoga verwendet wurde /WIE19w01/.

Im Fall von Norsk Hydro verschafften sich die Angreifer bereits Monate vor der Aktivierung der Schadsoftware durch eine mit Schadsoftware behaftete E-Mail an einen Mitarbeiter, die von einem vertrauenswürdigen Kunden des Unternehmens abgesendet wurde, Zugriff auf das Unternehmensnetzwerk. /BRI19w01/ In den folgenden Monaten breiteten die Angreifer sich lateral im Netzwerk aus, wobei u. a. Tools verwendet wurden, die Zugangsdaten erfordern, sodass davon auszugehen ist, dass die Angreifer diese Daten im Verlauf des IT-Angriffs über Spear-Phishing oder Brute-Force-Angriffe bzw.

über den ursprünglichen IT-Angriff der schadsoftwarebehafteten E-Mail erlangten. Das auf den Bereich IT-Sicherheit spezialisierte japanische Unternehmen Trend Micro geht davon aus, dass der Angriff mit der entsprechenden Vorbereitung sehr gezielt und mit der Absicht der Beeinträchtigung der Produktion von Norsk Hydro erfolgte. /TRE19w01/

Nach der Installation modifiziert LockerGoga die Accounts der Benutzer des Systems, indem es die Passwörter ändert. Die Schadsoftware versucht dabei, eingeloggte Benutzer auszuloggen. Daten auf den betroffenen Systemen (Laptops, Server, Desktop-PCs) werden anschließend verschlüsselt und auf dem Desktop eine Textdatei mit der Lösegeldforderung erstellt. Das Opfer wird darin aufgefordert, Kontakt mit den Angreifern aufzunehmen und Lösegeld in Form von Bitcoins zu zahlen.

Die verschlüsselten Daten umfassen dabei u. a. Dokumente wie PDF-Dateien, Tabellen, PowerPoint-Dateien, Datenbanken, Videos, sowie Python-Dateien und Java-Skripte. Je nach Version der Schadsoftware kann die Verschlüsselung spezifischer Dateien oder aller Daten sowie auch die Löschung von Daten von LockerGoga durchgeführt werden. In einigen von Trend Micro untersuchten Fällen war auch der Windows Boot Manager betroffen, sodass die betroffenen Systeme nicht mehr gestartet werden konnten. Bei allen von Trend Micro untersuchten Fällen waren die Systeme so stark beeinträchtigt, dass weder ein Entschlüsselungsprogramm genutzt werden noch eine Lösegeldforderung hätte erfüllt werden können, da die Opfer keinen Zugang zum System hatten. /TRE19w01/

Nach der Verschlüsselung der Daten versucht LockerGoga alle Netzwerkverbindungen des betroffenen Systems zu deaktivieren. Die Schadsoftware besitzt nach derzeitigen Informationen nicht die Fähigkeit, sich selbstständig auszubreiten wie beispielsweise WannaCry (siehe Kapitel B.9.4) oder NotPetya (siehe Kapitel B.9.6). Dagegen ist LockerGoga darauf ausgelegt, bis zur Ausführung möglichst unerkannt zu bleiben. Dazu ist die Schadsoftware beispielsweise mit verschiedenen gültigen Zertifikaten (Alisa Ltd., Kitty’s Ltd., and Mikl Limited) ausgestattet, die mittlerweile widerrufen wurden. Außerdem erzeugt die Schadsoftware keinen Netzwerk-Traffic, sodass diese Erkennungsmöglichkeit umgangen wird. Dazu werden weitere Techniken angewandt, um unerkannt zu bleiben. /TRE19w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.6 IT-Angriffe über VPN-Schwachstellen

Übersicht

Auf der BlackHat 2019, einer jährlichen Konferenz zu Informationssicherheit und IT-Angriffen, wurde ein umfassender Vortrag über IT-Angriffe auf VPN-Clients und VPN-zugängliche Netzwerke vorgestellt, welcher nach Einschätzung der Experten auf iranische IT-Angreifer zurückgeht. Die Erkenntnisse des Vortrages wurden Anfang 2020 in einem umfangreichen Bericht weiter dargelegt. /BLH20r01/

Beschreibung

Im Jahr 2019 sind eine Reihe von schwerwiegenden Schwachstellen in VPN-Clients bekannt geworden (CVE-2019-11510, CVE-2019-13379, CVE-2019-1579 usw.) welche von den im Vortag und zugehörigen Bericht genannten IT-Angreifern teilweise innerhalb von Stunden nach Veröffentlichung genutzt wurden, um IT-Angriffe durchzuführen.

Ziel der Angreifer waren nach bisherigen Erkenntnissen Netzwerke von Unternehmen und Behörden, welche VPN-Software für die datentechnischen Verbindungen ihrer Mitarbeiter benötigen, die außerhalb der Niederlassungen arbeiteten.

Wenn die Angreifer Zugriff auf die VPN-Verbindungen der Unternehmen bzw. Behörden erreichten, nutzten sie eine Reihe weiterer Schadsoftwarekomponenten und IT-Werkzeuge, um sich im betroffenen Netzwerk auszubreiten und immer mehr IT-Systeme zu kompromittieren. Nach bisherigen Erkenntnissen dienten die bisher erkannten IT-Angriffe über VPN-Schwachstellen durch mehrere iranische APT-Gruppen ausschließlich der Aufklärung, dem Abfließen von Informationen und der sicheren Installation von Hintertüren für die IT-Angreifer. Langfristig können solche Aufklärungs- und Zugriffsmöglichkeiten jedoch auch direkte Schadwirkung entfalten, z. B. wenn die IT-Angreifer Zugriff auf die Updateverteilsysteme von Softwarefirmen erhalten oder mit Datenlöschsoftware die Netzwerke und gespeicherten Daten unwiderruflich zerstören. /BLH20r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.11.7 IT-Angriff auf Windkraftanlage in den USA

Übersicht

Am 5. März 2019 wurde der u. a. in Utah (USA) ansässige Betreiber von Windkraft- und Solarenergieanlagen sPower, der über 130 Stromerzeugungsanlagen verteilt über die Vereinigten Staaten betreibt, Opfer eines IT-Angriffs. Das Unternehmen verzeichnete eine Reihe von Verbindungsabbrüchen zwischen dem Hauptkontrollzentrum und entfernten Stromerzeugungsstandorten, die jeweils kurz und intermittierend auftraten.

Die Ausfallzeiten, die als Loss-of-View bezeichnet werden, wurden durch Denial-of-Service-Angriffe (DoS) verursacht und beeinträchtigten die Fähigkeit des Unternehmens, den aktuellen Status der betroffenen Anlagen zu überwachen. Die Stromerzeugung der betroffenen Anlagen war nicht beeinträchtigt. /SEA19w01/

Beschreibung

Die Angreifer nutzten für die DoS-Angriffe eine ungepatchte Sicherheitslücke in der Firewall der betroffenen Anlagen aus, die es unautorisierten Benutzern erlaubte, betroffene Geräte wiederholt neu zu starten. Dies führte zu mehreren kurzen (im Bereich weniger Minuten) Kommunikationsausfällen zwischen Geräten vor Ort in den Anlagen, sowie zwischen den Stromerzeugungsstandorten und dem Hauptkontrollzentrum. Die betroffenen Geräte sind Firewalls der amerikanischen Firma Cisco Systems, die als Sicherheitseinrichtungen gegen IT-Angriffe bzw. unerlaubte Zugriffe von außerhalb dienen. Bei den Standorten und dem Kontrollzentrum handelt es sich um Einrichtungen mit geringem Einfluss auf das Stromnetz. Die durchgeführten Untersuchungen des IT-Sicherheitsvorfalls ergaben, dass der extern initiierte Neustart der Firewalls über einen Zeitraum von 10 Stunden auftrat und in den jeweiligen Einzelfällen für weniger als fünf Minuten vorlag. Cisco Systems stellte nach diesem Vorfall dem Unternehmen einen Firmware-Patch bereit, der anschließend von sPower im System aufgespielt wurde. Die Schwachstelle war bereits vor dem Ereignis bekannt und Cisco Systems hatte den Firmware-Patch bereits veröffentlicht, jedoch hatte der Betreiber sPower diesen nicht installiert. /NER19r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12 2020

B.12.1 IT-Angriff auf US-amerikanischen Pipeline Betreiber

Übersicht

Am 18. Februar 2020 veröffentlichte die Cybersecurity and Infrastructure Security Agency (CISA) der USA einen Bericht zu einem bis dahin unbekannten IT-Angriff auf einen nicht genannten Pipelinebetreiber. Im Rahmen des IT-Angriffes wurde neben dem administrativen Netzwerk auch das die Pipeline steuernde leittechnische Netzwerk beeinflusst, sodass es zur Beeinflussung des Betriebsablaufes kam. /CIS20r05/

Beschreibung

Die IT-Angreifer nutzten Spear-Phishing- und Watering-Hole-Techniken für den initialen Einbruch in die IT-Systeme des Pipelinebetreibers. Zielgenau erstellte Links auf manipulierte Webseiten wurden hierbei genutzt, um an Nutzer in der Zielorganisation, welche die manipulierten Webseiten für legitime Webseiten hielten, Schadsoftware zu verteilen. Die so in das IT-Netzwerk des Pipelinebetreibers eingebrachte Schadsoftware verbreitete sich dann über Netzwerkverbindungen an jedes weitere angebundene IT-System innerhalb des betroffenen Pipelinekontrollzentrums. Da keine spezifische Barriere zwischen dem IT-Netzwerk und dem leittechnischen Netzwerk des Pipelinebetreibers bestand, breitete sich die Schadsoftware auch im leittechnischen Netzwerk aus. Als Schadsoftware kam ein Erpressertrojaner für Windowssysteme zum Einsatz, sodass alle betroffenen Windows-PCs und Server von den IT-Angreifern verschlüsselt wurden und damit nicht mehr nutzbar waren. Im leittechnischen Netzwerk waren hierdurch Mensch-Maschine-Schnittstellen, Server und Datenarchivierungssysteme betroffen, jedoch keine leittechnischen Steuereinheiten mit Einfluss auf die Pipeline. /CIS20r05/

Aufgrund der verschlüsselten IT-Systeme kam es bei dem Betreiber der Pipeline zu Ausfällen von Anzeigen im Pipelinekontrollzentrum, jedoch konnte der Pipelinebetrieb weiterhin gesteuert werden. Aufgrund der Ausfälle wurde die Pipeline für zwei Tage abgeschaltet, die betroffenen IT-Systeme wurden getauscht und der Betrieb anschließend wieder aufgenommen.

Der IT-Angriff und seine Auswirkungen auf das leittechnische Netzwerk waren insbesondere dadurch möglich, dass der Betreiber der Pipeline kein IT-Sicherheitskonzept etabliert hatte und IT-Angriffe nicht in potenzielle Notfall- und Sicherungspläne aufnahm. Die fehlende Trennung der administrativen und leittechnischen Netzwerke ist auf fehlendes Verständnis für die Bedeutung der Informationssicherheit und dem vorrangigen Ziel den täglichen Betrieb zu erleichtern zurückgeführt worden. CISA beschreibt umfassende Maßnahmen des Pipelinebetreibers zur Erhöhung der Informationssicherheit nach dem Vorfall. /CIS20r05/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12.2 SNAKE/EKANS – IT-Angriffe auf weltweite Unternehmen

Übersicht

Im Januar 2020 veröffentlichten Forscher mehrerer IT-Sicherheitsunternehmen wie Dragos und SentinelLABS Informationen zu der im Dezember 2019 erstmals entdeckten Schadsoftware Snake (auch als EKANS bezeichnet, Bezeichnung taucht bei den Angriffen als String auf; Snake rückwärts und im weiteren Verlauf als Snake bezeichnet), bei der es sich um Ransomware handelt /DRA20w02, WAL20w01/. Neben der für Ransomware üblichen Verschlüsselung von Daten und der angezeigten Lösegeldforderung ist nach /DRA20w02/ die Besonderheit bei Snake, dass die Schadsoftware verschiedene Prozesse beeinflussen bzw. stoppen kann, die unter anderem im Zusammenhang mit industriellen Steuerungen (ICS) stehen. Im Verlauf des Jahres 2020 wurden Angriffe auf verschiedene Unternehmen mit der Schadsoftware beobachtet.

Beschreibung

Die Schadsoftware Snake ist – wie es häufig bei Ransomware der Fall ist – in der opensource Programmiersprache Golang geschrieben, die durch ihre Unterstützung multipler Plattformen auf den drei großen Betriebssystemen Windows, macOS und Linux Anwendung findet. Nach der Infektion überprüft Snake zunächst, ob das System bereits von der Schadsoftware betroffen ist. Bevor im weiteren Verlauf die Verschlüsselung gestartet wird, erzwingt Snake das Stoppen von Prozessen, die in der Schadsoftware als Liste

codiert sind und neben mit industriellen Steuerungssystemen in Zusammenhang stehenden Prozessen hauptsächlich Datenbanken (beispielsweise Microsoft SQL-Server) oder Backup-Systeme für Daten beinhalten. Nach /DRA20w02/ sind im ICS-Bereich unter anderem die Firmen Honeywell und GE Digital betroffen. Außer dem erzwungenen Stopp der betroffenen Prozesse und der bei Ransomware üblichen Verschlüsselung der Daten, führt die Malware keine weiteren Aktionen aus und beeinflusst entsprechend ICS-zugehörige Prozesse nicht weiter.

Nach der Verschlüsselung betroffener Dateien werden die Dateinamen abgeändert, indem eine zufällige fünfstellige Buchstabenfolge an den Dateityp angehängt wird. Im Gegensatz zu einer uniformen Umbenennung erschwert dieses Vorgehen die Identifikation der Ransomware. Nach dem Stoppen der Prozesse und der Verschlüsselung der Daten wird im Root-Verzeichnis und auf dem Desktop eine Datei mit der Lösegeldforderung und einer E-Mail-Adresse als Kontaktmöglichkeit erstellt. Kritische Systemdateien oder -ordner sind nicht von der Verschlüsselung betroffen, sodass das System beispielsweise nicht heruntergefahren oder gesperrt wird, was dem Opfer Zugriff auf die verschlüsselten Daten erlaubt. Dies unterscheidet Snake von disruptiveren Vertretern von Ransomware wie beispielsweise LockerGoga (siehe Kapitel B.11.5).

Die Schadsoftware Snake besitzt nach derzeitigen Informationen keinen Mechanismus zur Ausbreitung über ein infiziertes Netzwerk hinaus, sondern ist darauf angewiesen, dass sie aktiv gestartet oder innerhalb von Skripten ausgeführt wird, um ein Zielsystem zu infizieren. Innerhalb des Netzwerks breitet sich Snake über Skripte oder weitere Mechanismen aus, beispielsweise durch die Kompromittierung des Verzeichnisdienstes Active Directory. /DRA20w02/, /WAL20w01/

Im Verlauf des Jahres 2020 wurden vermehrt IT-Angriffe mit der Schadsoftware Snake beobachtet. Laut /ABR20w01/ startete am 4. Mai 2020 eine weltweite Kampagne von IT-Angriffen, bei der diverse Firmen, unter anderem im Gesundheitssektor, betroffen waren. Dabei wurde berichtet, dass Snake vor der Verschlüsselung der Daten außerdem Datendiebstahl betreibt und mit der Veröffentlichung der verwendeten Daten droht. Es ist unklar, ob dies tatsächlich der Fall ist, sich die Angreifer anderweitig Zugang zu Daten beschafft haben oder die Drohung tatsächlich in die Tat umgesetzt werden könnte. Eines der Opfer dieser Kampagne ist das deutsche Unternehmen Fresenius, ein Medizintechnik- und Gesundheitskonzern. Weiterhin ist Fresenius einer der größten privaten Krankenhausbetreiber Deutschlands und im Pharma- und Gesundheitsdienstleistungsbereich tätig. Ein Unternehmenssprecher bestätigte den IT-Angriff und gab an, dass es

dadurch bzw. durch entsprechende Gegenmaßnahmen zwar zu Einschränkungen einiger Funktionen innerhalb des Unternehmens kam, die Patientenversorgung jedoch sichergestellt und fortgesetzt werde. /KRE20w01/

Generell sind die Opfer von Snake nach derzeitigen Informationen gezielt ausgesucht. Die Schadsoftware gleicht dazu das Netzwerk der Opfer mit eigenen IP-Listen ab. /JUN20w01/ Die Ziele sind weltweit verteilt und umfassen ein breites Spektrum. Neben Angriffen auf Unternehmen und Organisationen der kritischen Infrastruktur (wie beispielsweise Fresenius in Deutschland) stellt in diesem Zusammenhang der IT-Angriff auf das Unternehmen Honda, einem japanischen Konzern, der hauptsächlich im Bereich Motoren und Automobil tätig ist, im Sommer 2020 einen weiteren IT-Sicherheitsvorfall dar. Betroffen waren Netzwerke von Unternehmensniederlassungen in Europa und Japan. Die entsprechenden Honda-Domains wurden in der Ziel-Abfrage der Schadsoftware gefunden. /ILA20w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.12.3 IT-Angriff auf die Stromversorgung von Mumbai

Übersicht

Am 13. Oktober 2020 waren etwa 20 Millionen Menschen in Mumbai von einem Stromausfall betroffen. Dem Ereignis waren politische Spannungen zwischen Indien und China vorrausgegangen. Bis heute ist jedoch unklar, ob es sich bei dem Stromausfall um einen IT-Angriff Chinas oder um technisches bzw. menschliches Versagen gehandelt hat.

Beschreibung

Am 13. Oktober 2020 kam es zu einem Stromausfall in Mumbai, von dem etwa 20 Millionen Menschen betroffen waren. Vermutlich war der Stromausfall die Folge eines chinesischen IT-Angriffs auf ein nahe gelegenes Stromlastmanagementzentrum. Dem Ereignis waren politische Spannungen zwischen Indien und China vorausgegangen. Seit Anfang 2020 sind indische Organisationen, darunter auch solche aus dem Energiesektor, das Ziel chinesischer IT-Angriffe /ECT21w01/.

Im Februar 2020 führten indische IT-Angreifer eine Kampagne gegen chinesische Organisationen in Wuhan durch, bei denen sie Phishing-E-Mails verwendeten, die das Corona Virus thematisierten. Im Juni 2020 kam es zu Auseinandersetzungen zwischen indischen und chinesischen Truppen im Galwan-Tal, an der Grenze zwischen beiden Ländern /ECT21w01/.

Vier Monate später startete China IT-Angriffe auf die indische Technologie- und Bankeninfrastruktur. Dabei wurde auch Schadsoftware in die Leittechniksysteme und Knotenpunkte des indischen Stromnetzes eingeschleust, wobei ein Großteil der Schadsoftware jedoch nicht aktiviert wurde. Unter den Zielen befanden sich ein Umspannwerk und ein Kohlekraftwerk. /NYT21w02, REC21w03, WSJ21w02/

Das US-amerikanische IT-Sicherheitsunternehmen Recorded Future, das das Internet auf Aktivitäten staatlicher Akteure untersucht, entdeckte zwar den Datenfluss der Schadsoftwarekomponenten, war aber nicht in der Lage deren Programmcode zu untersuchen, da die indischen Behörden keine Auskunft darüber geben /WSJ21w02/. Recorded Future sendete seine Ergebnisse an das indische Computer Emergency Response Team CERT. Vermutlich ist für die Einschleusung der Schadsoftware in das indische Stromnetz die chinesische APT-Gruppierung Red Echo verantwortlich. Indische Militärexperten haben dazu geraten, in China gefertigte Hardware, welche im indischen Energiesektor eingesetzt wird, auszutauschen. /NYT21w02, REC21w03, WSJ21w02/

Kerntechnischer Bezug

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

B.12.4 SolarWinds – IT-Angriffe über schadsoftwarebehaftete SolarWinds Produkte

Übersicht

Anfang Dezember 2020 wurde eine breit angelegte Angriffswelle von Supply-Chain-Angriffen über manipulierte, schadsoftwarebehaftete SolarWinds-Produkte bekannt /FIR20r01/.

Von den IT-Angriffen ist hierbei die Software-Plattform SolarWinds Orion betroffen, die unter anderem Monitoring und Management von IT-Netzwerken, -Systemen und -Anwendungen ermöglicht und von 33.000 Solar Winds Kunden genutzt wird.

Beschreibung

Den IT-Angreifern gelang es, unbemerkt eine Reihe von SolarWinds Orion Versionen (2019.4 HF5 bis 2020.2.1) mit einem Trojaner zu infizieren, welche dann digital signiert und ab März 2020 über den offiziellen Update-Server von SolarWinds verteilt wurden. Hierbei ist konkret die Programmbibliothek SolarWinds.Orion.Core.BusinessLayer.dll betroffen /BSI20i04/. Diese Programmbibliothek ist ebenfalls digital signiert. Die inzwischen als Sunburst betitelte Schadsoftware etabliert eine Backdoor mit weitreichenden Handlungsoptionen für die Angreifer /FIR20r01/. Es wurde bekannt, dass etwa 18.000 Kunden von SolarWinds die schadsoftwarebehafteten Updates heruntergeladen haben /DAR21w01/.

Entdeckt wurde die Schadsoftware von der IT-Sicherheitsfirma FireEye, welche am 13.12.2020 von einer sektor- und länderübergreifenden Angriffskampagne mit Schadsoftware berichtet, einschließlich eines Angriffs auf FireEye selbst /FIR20r01/. Darüber hinaus werden immer weitere Berichte über nach dem Download der schadsoftwarebehafteten Solar Winds Updates weiterführende Kompromittierungen mit Sunburst bekannt. Unter anderem bei einer Reihe von US-Ministerien und Behörden (bspw. die US-Department of Homeland Security, Justice, Energy, Commerce und Treasury ebenso wie das US-Department of State und die National Institutes of Health) sowie unter anderem die Federal Energy Regulatory Commission (FERC), das Los Alamos National Laboratory und die Sandia National Laboratories /BUS20w01, POL20w01/. Auch Microsoft, VMware, CrowdStrike und Cisco haben inzwischen bestätigt, Ziel des Angriffs mit Sunburst geworden zu sein /NYT20w02, REU20w01, WSJ20w01/.

Bereits Anfang Januar 2020 wurde von mehr als 250 kompromittierten Angriffszielen ausgegangen /SEC21w05/. Es ist zu erwarten, dass es darüber hinaus noch weitere Opfer der Angriffswelle gibt, welche den Angriff bislang noch nicht entdeckt oder nicht öffentlich gemacht haben. Welche und wie viele Daten bei den bisherigen Angriffen gestohlen oder manipuliert wurden, lässt sich bislang noch nicht abschätzen, die Analyse und Aufarbeitung wird sich vermutlich über Jahre hinziehen. Auch ist derzeit noch keine Aussage dazu möglich, wie viele kompromittierte oder manipulierte Daten und Informationen von den direkt mit Sunburst angegriffenen Opfern an Dritte weitergegeben

wurden. Darüber hinaus handelt es sich bei den IT-Angriffen nicht um eine vergangene, sondern eine aktuelle, derzeit noch andauernde Angriffskampagne. Dies schließt weitere Angriffsziele als auch die weitergehende Kompromittierung oder Ausschleusung und Manipulation von Daten und Informationen bisheriger Angriffsziele ein.

Kerntechnischer Bezug

Zu den von den Angriffen mit schadsoftwarebehafteten SolarWinds Produkten betroffenen Organisationen zählen auch das Los Alamos National Laboratory, welches sich mit der Forschung und Entwicklung hinsichtlich Nuklearwaffen und Kernfusion beschäftigt. Ein weiteres Opfer sind die Sandia National Laboratories, in welchen hauptsächlich die nicht-nuklearen Komponenten von Nuklearwaffen entwickelt und hergestellt werden. Aus Sicht der GRS besteht allerdings eine Relevanz auch für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Stellungnahme detailliert ausgewertet /GRS21r05/.

B.13 2021

B.13.1 Oldsmar Attack – IT-Angriff auf Wasserwiederaufbereitungsanlage in Tampa, Florida

Übersicht

Im Februar 2021 wurde von der amerikanischen Bundespolizei FBI ein Bericht veröffentlicht, wie im Rahmen eines IT-Angriffes auf eine Wasserwiederaufbereitungsanlage nördlich von Tampa die Trinkwasserversorgung vergiftet wurde. Die Angreifer nutzten hierbei einen Fernwartungszugriff, welcher auch von Mitarbeitern insbesondere in der Pandemiezeit genutzt wird.

Beschreibung

Die Angreifer nutzten den Fernzugriff, um den Regler für die Steuerung des Anteils von Natriumhydroxid im Wasser zu manipulieren und den Anteil von 100 ppm auf 11.000 ppm anzuheben. Dem schichthabenden Mitarbeiter fiel auf, wie sich der Mauszeiger von selbst bewegte und am Regler der Anteil des Natriumhydroxids erhöht wurde. Die Angreifer beendeten umgehend nach dem Eingriff ihre Verbindung.

Gemäß der Anlage wäre ohne Entdeckung durch den Mitarbeiter der Angriff durch die eingesetzten pH Scanner der Anlage aufgefallen, was dann jedoch zu einer Unterbrechung der Wasserversorgung geführt hätte.

Der Fernwartungszugriff wurde auf den IT-Angriff folgend deaktiviert und es sollen Upgrades der Systeme durchgeführt werden. /NPR21r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.2 DarkSide – IT-Angriff auf brasilianischen Energiesektor

Übersicht

Die Nachrichtenagentur Reuters veröffentlichte im Februar 2021 eine kurze Meldung, dass nach Angaben des brasilianischen Betreibers Eletrobras sich ein Informationssicherheitsvorfall im Kernkraftwerk Angra ereignete. Dabei wurde der Betrieb des Kraftwerkes nicht beeinflusst, ein nicht näher beschriebenes Netzwerk des Kraftwerkes wurde von einer Ransomware infiziert. Die Nutzung eines Teils der administrativen Systeme wurde daraufhin untersagt und eine Untersuchung angeordnet.

Gemäß den vorliegenden Informationen wurde neben dem KKW Angra auch Eletrobras selbst sowie der Energiekonzern Copel angegriffen, mit nach Information von Reuters der neuartigen Ransomware Darkside, welche auch Informationen vom Unternehmen Copel entwendete. Weitere Informationen sind bisher nicht verfügbar. /REU21r01/

Kerntechnischer Bezug

Das Kernkraftwerk Angra war direkt von diesem IT-Angriff betroffen.

B.13.3 Codecov – IT-Angriff über Bash Uploader Dev Tool

Übersicht

Im April 2021 wurde ein Supply-Chain-Angriff über eine Kompromittierung des IT-Werkzeugs Codecov Bash Uploader entdeckt, der seit Ende Januar 2021 unentdeckt geblieben war. Beim Codecov Bash Uploader handelt es sich um ein Werkzeug, das im Rahmen einer Analyse der sogenannten Code Coverage (Testabdeckung von Programmcode im Zuge des Entwicklungsprozesses) zum Einsatz kommt.

Konkret dient das von der Manipulation betroffene Bash Uploader-Skript dazu, aus verschiedenen Entwicklungsplattformen heraus Code Coverage-Reports zur weiteren Auswertung an den Server von Codecov zu übermitteln. Von den Manipulationen betroffen sind nach Aussage des Unternehmens auch die verwandten Bash Uploader-Skripte für GitHub, CircleCI und Bitrise Step. Die manipulierte Version des Bash Uploaders verschaffte den IT-Angreifern unter bestimmten Voraussetzungen Zugangsdaten und andere Informationen aus Continuous-Integration-Umgebungen von Codecov-Kunden, die das kompromittierte Skript für ihre Repositories verwenden. /HEI21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.4 Kaseya – Globaler IT-Angriff

Übersicht

Am 2. Juli 2021 ereignete sich ein IT-Angriff auf VSA-Server verschiedener weltweit verteilter Unternehmen, wobei über 1000 Firmen betroffen waren. Die betroffene Software VSA (Virtual System Administrator) des amerikanischen IT-Dienstleisters Kaseya ist ein Remote-Monitoring und -Management-Tool, mit dem Dienstleistungen wie beispielsweise Fernwartung o. ä. durchgeführt werden können. Unter anderem wird VSA häufig zum Ausführen von Softwareupdates verwendet. Die Angreifer nutzten dabei eine Sicherheitslücke aus und verschlüsselten infolgedessen im Rahmen eines Ransomware-Angriffs die Daten der Kunden des IT-Dienstleisters, um Lösegeld für die Entschlüsselung der Daten zu erpressen. Kaseya hat weltweit mehr als 36.000 Kunden,

wobei die Zahl der von dem Angriff betroffenen Unternehmen nach Angaben der IT-Sicherheitsfirma Huntress bei mehr als 1.000 liegt. Kaseya selbst spricht von weniger als 40 betroffenen Kunden, wobei sich darunter wiederum auch IT-Dienstleister mit mehreren Kunden befanden, sodass eine Verbreitung über mehrere Schritte wahrscheinlich ist.

Bei den Tätern handelt es sich mutmaßlich um die russische Gruppierung REvil, die bereits durch Ransomware-Angriffe auf US-Unternehmen sowie Cyberangriffe gegen verschiedene Ministerien und Behörden insbesondere in der jüngeren Vergangenheit aufgefallen ist.

Es wurden bei diesem IT-Angriff mit Hilfe von Ransomware Daten auf den betroffenen VSA-Servern verschlüsselt. Insgesamt handelt es sich um 50 Server, die durch den Angriff betroffen waren. Über ein Softwareupdate wurde die Schadsoftware an tausende Firmenrechner verteilt, wobei die Angreifer für diesen Lieferkettenangriff einen Zero-Day-Exploit ausnutzten. Am 5. Juli 2021 folgte eine Lösegeldforderung im Darknet über 70 Millionen US-Dollar in Form von Kryptowährung (Monero) für die Entschlüsselung der Daten. Betroffen war neben überwiegend Unternehmen in den USA und Großbritannien sowie die schwedische Supermarktkette Coop, deren Zahlungsdienstleister die Software von Kaseya nutzt. Coop musste in der Folge am 3. Juli 2021 alle 800 Filialen schließen, da die Kassensysteme blockiert waren. Dem Bundesamt für Sicherheit in der Informationstechnik zufolge waren auch in Deutschland Unternehmen betroffen. Insgesamt spricht das BSI von einigen tausend betroffenen Computern und unter anderem einem betroffenen IT-Dienstleister. /HEI21w06/, /CIO21w01/, /BSI21i10/

Beschreibung

Am Abend des 2. Juli 2021 startete der IT-Angriff zunächst in den Vereinigten Staaten und hatte zeitnah bereits Auswirkungen in Europa. Kaseya berichtete am selben Tag von einem potenziellen Angriff auf die Fernwartungssoftware VSA und empfahl den Kunden, vorsorgliche ihre VSA-Server abzuschalten. Die Kunden wurden per E-Mail, Telefon und Online-Benachrichtigungen informiert, dies schnellstmöglich durchzuführen, da einer der ersten Schritte der Angreifer die Sperrung des administrativen Zugriffs auf diese Systeme beinhaltet. Bei dem Ransomware-Angriff über Kaseyas Software VSA handelte es sich um einen der bisher größten IT-Angriffe über die Lieferkette. Neben den über 1.000 direkt betroffenen Firmen, die mit Kaseya in Verbindung standen, und den entsprechend tausenden von der Verschlüsselung betroffenen Computern waren auch

Firmen betroffen, die selbst keinen direkten Bezug zu Kaseya haben, sondern deren IT-Dienstleister oder Zulieferer VSA nutzten.

Die Angreifer nutzten mehrere Sicherheitslücken und Zero-Day-Exploits aus, um die VSA-Server zu manipulieren und so ein schadsoftwarebehaftetes Update zu platzieren, welches entsprechend von den Servern an die Clients weitergegeben wurde. Dieses Update führte zur Verschlüsselung sämtlicher Daten betroffener Systeme und forderte zu einer Lösegeldzahlung auf. Einzelne Anwender erhielten Forderungen im Bereich von ca. 50.000 US-Dollar (in Form der Kryptowährung Monero), im Verlauf des Angriffs ergaben sich Lösegeldforderungen der Angreifer von bis zu umgerechnet 70 Millionen US-Dollar für die Entschlüsselung aller betroffenen Systeme.

Nach bisherigem Kenntnisstand war von dem Angriff lediglich der Update-Server von Kaseya betroffen und nicht die Infrastruktur, wie es beispielsweise bei SolarWinds der Fall war, wo Angreifer Zugriff auf den Build-Server des Unternehmens erlangt hatten.

Die Einschleusung der Schadsoftware bzw. das Einfallstor für diesen Lieferkettenabgriff waren mehrere Zero-Day-Exploits in der Software VSA von Kaseya. Die Existenz dieser Sicherheitslücken war bereits teilweise vor dem Angriff bekannt. Mitarbeiter des Dutch Institute for Vulnerability Disclosure (DVID) hatten vor dem Angriff mehrere Zero-Day Vulnerabilities entdeckt und die Erkenntnisse bereits an Kaseya weitergegeben. Nachdem Kaseya von den Schwachstellen erfahren hatte, trat sie in Kontakt mit dem DIVD und arbeitete zusammen an Lösungen, unter anderem indem intern erste Patches zur Behebung getestet wurden. Der IT-Angriff auf die VSA-Server erfolgte, bevor Kaseya die Sicherheitslücken patchen und die Patches einer breiten Öffentlichkeit zur Verfügung stellen konnte. /HEI21w07/, /DIV21w01/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.13.5 DarkSide – IT-Angriff auf Colonial Pipeline

Übersicht

Am 7. Mai 2021 bemerkte der US-amerikanische Pipeline-Betreiber „Colonial“, dass die IT-Systeme der Firma Ziel eines IT-Angriffs mit Ransomware waren. Die

Colonial-Pipeline ist mit ca. 8.850 km Länge die größte Pipeline für Erdölderivate (Diesel, Heizöl, Treibstoff für Flugzeuge uvm.) in den USA, wobei täglich mehrere 100 Millionen Liter an der Ostküste der USA von Texas bis an den Hafen von New York und New Jersey befördert werden. Um den IT-Angriff schnellstmöglich zu begrenzen und da zunächst unklar war, inwieweit IT- und OT-Systeme betroffen waren, stellte der Betreiber den Betrieb der Pipeline innerhalb weniger Stunden nach der Erkennung des Angriffs ein. Neben dem Einsatz von Ransomware gelang es den Angreifern vor der Verschlüsselung etwa 100 GB Daten zu stehlen. Als Gegenleistung für die Entschlüsselungstools und zur Verhinderung der Veröffentlichung der Daten verlangten die Angreifer Lösegeld in Höhe von ca. 4,4 Millionen Dollar in Form von Bitcoins.

Der Betreiber zahlte das Lösegeld am 8. Mai 2021, woraufhin ein Tool zur Entschlüsselung zur Verfügung gestellt wurde und am 12. Mai 2021 der Betrieb der Pipeline wieder aufgenommen wurde. Es handelte sich hierbei lediglich um einen rudimentären Grundbetrieb. Es dauerte Wochen bzw. Monate bis alle Auswirkungen des IT-Angriffs behoben waren. Am 7. Juni 2021 gab das amerikanische Justizministerium bekannt, dass 63,7 Bitcoins (ca. 2,3 Millionen Dollar) die für die Lösegeldzahlung verwendet wurden, zurückerlangt werden konnten. Im Rahmen der unmittelbaren Auswirkungen des Ausfalls der Pipeline kam es zu Lieferengpässen, sodass aufgrund der Treibstoffknappheit der Flugverkehr u. a. am Charlotte Douglas International Airport beeinträchtigt wurde, die Preise für Benzin rasant anstiegen und es zu Panikkäufen von Benzin kam, da in einzelnen Gebieten bis zu 80 % der Tankstellen kein Benzin mehr vorrätig hatten. Für die betroffenen Gebiete wurde der Notstand ausgerufen. /SEC21w07/, /SEC21w08/

Beschreibung

Die Colonial Pipeline Company gab am 07.05.2021 bekannt, Opfer eines IT-Angriffs mit Ransomware zu sein und stellte am gleichen Tag den Betrieb ein. Offen blieb zunächst, ob neben der Informationstechnik auch OT bzw. industrielle Steuerungssysteme vom Angriff direkt betroffen waren. Der Betreiber der Pipeline nahm vorsorglich auch bis zu dem Zeitpunkt nicht betroffene IT-Systeme, einschließlich Büro-IT und industriellen Steuerungssystemen, außer Betrieb, da Umfang und Zielsetzung des Angriffs zunächst nicht bekannt waren. Es ist nicht bekannt, ob in der Systemarchitektur des Betreibers eine klare Trennung zwischen IT und OT vorliegt, sodass ggf. durch den Angriff auf IT-Systeme auch OT-Systeme bis hin zu industriellen Steuerungssystemen beeinflusst werden konnten.

Nach derzeitigem Kenntnisstand betraf der IT-Angriff jedoch ausschließlich IT-Systeme und zielte auf die Abrechnungsinfrastruktur ab. /CON21w02/, /CNN21w01/, /CIS21w08/

Die Angreifer setzten dem FBI zufolge eine Ransomware ein, die unter dem Namen DarkSide bekannt ist und von der gleichnamigen Gruppierung, die mutmaßlich Verbindungen nach Russland aufweist, eingesetzt wird /FBI21w01/. Außer der Verschlüsselung von Daten betreibt DarkSide gleichzeitig Spionage und Datendiebstahl, um die Opfer mit Androhung einer Veröffentlichung dieser Daten noch stärker unter Druck zu setzen. Die Gruppierung hinter DarkSide bietet im DarkNet mit Hilfe von Cloud Computing Ransomware-as-a-Service (RaaS) an, d. h. sie bietet auch Dritten, die selbst über keinerlei Programmierkenntnisse verfügen, eine maßgeschneiderte Version ihrer Ransomware gegen Bezahlung an.

Die eigentliche Erpressung wird dann von den Cyberkriminellen durchgeführt, welche die RaaS-Dienste in Anspruch nehmen. /DIG20w01/

Den Zugriff auf das Netzwerk von Colonial Pipeline erlangten die Angreifer nach Angaben des Geschäftsführers über einen veralteten, nicht mehr genutzten VPN-Zugang. Dieser war mit einem komplexen Passwort geschützt, jedoch nicht wie viele andere aktuelle Systeme des Betreibers weiter gesichert, beispielsweise mit einer Multi-Faktor-Authentifizierung. Es ist unklar, wie die Angreifer die Anmeldeinformationen (credentials) erlangten. /CYB21w01/ Die eigentliche Schadsoftware ist eine komprimierte ausführbare Datei mit komprimierten Konfigurationsdateien und nutzt hybride Verschlüsselungstools. DarkSide prüft im Verlauf der Ausführung, ob die Schadsoftware mit erhöhten Rechten ausgeführt wird. Wenn der mit dem Prozess verbundene Benutzer kein Administrator ist, verwendet DarkSide Techniken zur Erhöhung der Benutzerrechte, um sich selbst mit höheren Rechten neu zu starten. Es werden vorbereitende Schritte zur Verschlüsselung der Daten durchgeführt, die Kommunikation mit dem für den Angriff vorgesehenen Command & Control (C&C)-Server hergestellt und geprüft, ob die Systemsprache des Systems Russisch ist, wobei sich die Schadsoftware beendet, wenn dies der Fall ist. Zur Identifizierung der Opfersysteme werden systemspezifische Informationen verschlüsselt gespeichert und an den C&C-Server übertragen. Der Hauptangriff besteht anschließend darin, die Kopien jedes Datenträgers mithilfe eines PowerShell-Skripts zu löschen, damit das Opfer die Daten nicht wiederherstellen kann. Außerdem werden Windows-Dienste und verschiedene Prozesse beendet. Anschließend verschlüsselt die Malware rekursiv Dateien, bis alle lokalen und Netzwerkspeicher verschlüsselt sind. Der Dateiname, die Daten und der Hash des Opfers werden an jede Datei angehängt, bevor sie an den

entsprechenden C&C-Server des Angreifers übermittelt werden. In einem letzten Schritt löscht die Malware sich selbst. /VIR21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Darkside veröffentlichte nach dem IT-Angriff auf die Pipeline eine Meldung, dass ihre Ziele rein wirtschaftlicher Natur seien und dass direkte Auswirkungen für die Gesellschaft vermieden werden sollten. Demnach sollen u. a. die Angriffsziele nach eigenen Angaben, insbesondere auch im Rahmen der RaaS-Dienste, zukünftig abseits von Krankenhäusern, Schulen, Universitäten, Non-Profit-Organisationen und staatlichen Einrichtungen liegen. /CNB21w01/

Eigenen Angaben zufolge hat die Gruppierung aufgrund der Aktivitäten und des Drucks der Behörden der Vereinigten Staaten die Aktivitäten eingestellt, wobei der Gruppierung unter anderem der Zugang zu Teilen ihrer Infrastruktur nicht mehr möglich sei. Da es sich hierbei um eigene Angaben einer kriminellen Organisation mutmaßlich mit russischen Verbindungen handelt, ist die Glaubwürdigkeit zumindest fraglich. Für derartige Gruppierungen ist es zudem durchaus üblich, unter einem neuen Namen zu agieren. Nach Informationen der CISA operiert die Gruppierung neuerdings möglicherweise unter der Bezeichnung „BlackMatter“ (siehe Kapitel B.13.7). /WSJ21w01, CIS21i07/

B.13.6 IT-Angriff auf Kisters AG

Übersicht

Am 12.11.2021 meldete das deutsche IT-Unternehmen Kisters AG, dass es in der Nacht vom 10. auf den 11. November 2021 Opfer eines IT-Angriffs geworden ist, wobei die Angreifer Ransomware einsetzten. Das Unternehmen arbeitet als IT-Dienstleister unter anderem im Bereich der kritischen Infrastrukturen und versorgt dabei beispielsweise Energieerzeuger, Netzbetreiber und Messstellenbetreiber mit Softwareprodukten. Die Dienstleistungen umfassen dabei unter anderem die Steuerung von Regelleistungen. Die Kisters AG hat nach eigenen Angaben zunächst das komplette System heruntergefahren, um weiteren Schaden zu vermeiden und war vorübergehen weder per E-Mail noch über das Festnetztelefon erreichbar. Bis zum März 2022 konnte in fast allen Bereichen wieder der Normalbetrieb eingerichtet werden.

Die Kriminalpolizei und das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden umgehend eingeschaltet und die zuständigen Aufsichtsbehörden informiert. /KIS21w01/

Beschreibung

Das BSI schätzt den erfolgreichen Angriff auf die Kisters AG in ihren Meldungen zur IT-Bedrohungslage vom 16. bzw. 19.11.2021 unter anderem für Betreiber kritischer Infrastrukturen als potenziell kritisch ein, da zu diesem Zeitpunkt nach Aussage des Unternehmens nicht ausgeschlossen werden konnte, dass Kunden- oder Lieferantendaten kompromittiert wurden, was auch entsprechende Einwahldaten der Fernwartungszugänge betreffen könnte.

Nach Angaben der Kisters AG haben sich die Angreifer bei dem durchgeführten Ransomware-Angriff Zugang zu Daten des Unternehmens gesichert, diese verschlüsselt und damit gedroht, die erbeuteten Daten zu veröffentlichen. Bei einer Weigerung, entsprechende Lösegeldforderungen zu erfüllen, war demnach unter anderem mit einer Veröffentlichung der erbeuteten Daten zu rechnen. Am 21.11.2021 meldete die Kisters AG, dass nach den bisherigen forensischen Analysen keine Anzeichen gebe, dass ausgelieferte Softwareprodukte kompromittiert sind /ENE21w01/. Allerdings geht das Unternehmen davon aus, dass Daten abgeflossen sein könnten, welche Informationen zu kritischen Infrastrukturen beinhalten, beispielsweise Netzpläne oder weitere sensible Daten. (BSI-Meldung)

Hinsichtlich der Frage, wie sich die Angreifer Zugriff zum Netzwerk der Kisters AG verschafft haben, gibt es bisher keine Informationen. Das Unternehmen veröffentlichte am 31. März 2022 eine Pressemitteilung, nach der in fast allen Bereichen wieder ein Normalbetrieb eingerichtet wurde, wobei über vier Monate Anstrengungen zur Wiederherstellung und Verbesserung der IT-Infrastruktur, wie beispielsweise eine technische Entkopplung der E-Mail-Server von der internen Infrastruktur, unternommen wurden. Zudem wurde durch weitere Sicherheitsvorkehrungen, wie umfangreiche Viren-Scans, Passwortänderungen und Prozessbeobachtungen die Sicherheit weiter erhöht. /ENE21w01/, /KIS22w01/, /ENE22w01/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.13.7 Black Matter – IT-Angriffe auf kritische Infrastrukturen

Übersicht

Am 18. Oktober 2021 wurde von der CISA, dem FBI und der NSA eine Warnmeldung bezüglich Ransomware-Angriffen von der Gruppierung „BlackMatter“ bzw. mit der gleichnamigen Ransomware veröffentlicht /CIS21i07/. Darin sind Informationen über die bei den IT-Angriffen verwendeten Taktiken, Techniken und Prozeduren (TTPs) enthalten.

Nach Angaben der CISA handelt es sich bei BlackMatter um eine Ransomware einsetzende und Ransomware-as-a-Service (RaaS) anbietende, russisch-sprachige Gruppierung, die erstmals im Juli 2021 in Erscheinung getreten ist und seitdem diverse Ziele der amerikanischen kritischen Infrastruktur angegriffen hat. Darunter zwei Organisationen des US-amerikanischen Lebensmittel- und Landwirtschaftssektors. Der Hersteller für Antivirensoftware Emsisoft berichtet in der Zeit von Juli bis September 2021 von 44 IT-Angriffen mit der Ransomware BlackMatter und schätzt aufgrund einer erwarteten Dunkelziffer die Aktivitäten der Gruppierung auf über 100 Angriffe in dieser Zeit, wobei die Ziele neben den USA, dem Vereinten Königreich und Kanada weltweit verteilt sind. Hervorzuheben ist dabei ein Angriff auf den japanischen Konzern Olympus, der weltweit Produkte im Bereich Optik und Fotografie im Privatbereich und für die Medizin, Wissenschaft und Industrie anbietet. Nachdem verdächtige Aktivitäten in den Firmennetzwerken in Europa, Afrika und dem mittleren Osten beobachtet wurden, stellte Olympus den Datentransfer in die Systeme der betroffenen Regionen vorbeugend ein. /EMS21w01/

Beschreibung

Die Ransomware BlackMatter wird von der gleichnamigen Gruppierung eingesetzt und auch als RaaS angeboten, d. h. sie ist auch für Dritte, die selbst über keinerlei Programmierkenntnisse verfügen, in Form einer maßgeschneiderten Version der Ransomware gegen Bezahlung verfügbar. Die eigentliche Erpressung wird dann von den Cyberkriminellen durchgeführt, welche die RaaS-Dienste in Anspruch nehmen. Bei einem entsprechenden IT-Angriff werden die Daten der Opfer verschlüsselt, woraufhin eine Lösegeldforderung zwischen in der Regel 80.000 $ und 15.000.000 $ in Kryptowährungen (Bitcoin oder Monero) und ggf. die Drohung der Veröffentlichung gestohlener Daten erfolgt.

Bevor die Daten im Verlauf des IT-Angriffs mit Hilfe kryptographischer Tools (Salsa20 bzw. RSA 1024-bit) verschlüsselt werden, werden Daten vom kompromittierten System extrahiert und zur weiteren Erpressung der Opfer hinsichtlich einer möglichen Veröffentlichung missbraucht. Neben einer Version für Windows-Systeme existiert auch eine für Linux-Systeme entwickelte Version von BlackMatter. /EMS21w01/

Der IT-Angriff beginnt mit dem Eindringen in das Netzwerk des Opfers, was in der Regel über ein kompromittiertes Remote-Desktop-Protokoll, Phishing-Kampagnen, das Ausnutzen bekannter Schwachstellen oder gestohlene Anmeldedaten erfolgt. Nach der Ausführung der Schadsoftware überprüft BlackMatter zunächst die Nutzerrechte, um ggf. durch eine Rechteeskalation die Nutzerrechte zu erhöhen.

BlackMatter nutzt das Lightweight Directory Access Protocol (LDAP) und das Server Message Block (SMB) Protokoll, um auf das Active Directory (AD) zuzugreifen und alle Geräte im Netzwerk zu erkennen. Laufende Prozesse und Services werden gestoppt. BlackMatter verschlüsselt dann die gefundenen Systeme und freigegebenen Laufwerke per Fernzugriff, wobei neben den lokal und auf Netzwerklaufwerken gespeicherten Daten auch Wechseldatenträger verschlüsselt werden. Spezifische Verzeichnisse und Daten, die zum Betrieb des Systems benötigt werden, werden nicht verschlüsselt, sodass das Opfer weiterhin Zugriff auf das grundlegende System hat. /CIS21i07, EMS21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Nach eigenen Angaben verzichtet die Gruppierung auf Angriffe auf Ziele kritischer Infrastruktur, staatliche Behörden, Krankenhäuser und gemeinnützige Organisationen und hat lediglich monetäre Interessen. Diese Aussagen erscheinen, da es sich um eine kriminelle Gruppierung handelt unglaubwürdig und wurden durch die Meldung der CISA, des FBI und der NSA, die Angriffe auf kritische Infrastruktur der USA melden, bereits widerlegt. Generell befinden sich unter den Opfern große, über weitreichende (finanzielle) Ressourcen verfügende Organisationen /CIS21i07/, /EMS21w01/. Eigenen Angaben zufolge hat die Gruppierung aufgrund des Drucks der Behörden die Aktivitäten eingestellt /CPO21w03/. Auch diese Aussagen sind vor dem kriminellen Hintergrund der Gruppierung zu betrachten, wobei es zudem für derartige Gruppierungen nicht unüblich ist, immer wieder unter einem neuen Namen zu agieren, wie es für BlackMatter hinsichtlich DarkSide bereits vermutet wurde.

B.13.8 APT28 – IT-Angriff auf Google

Übersicht

Die vom russischen Staat unterstützte APT-Gruppierung APT28, auch Fancy Bear genannt, führte einen Spear-Phishing Angriff auf die E-Mail-Postfächer von 1.4000 Gmail-Nutzern aus verschiedenen Geschäftsfeldern durch /VER21w01/. Der Angriff wurde Ende September 2021 entdeckt. Das Ziel der Angreifer bestand darin die Postfächer zu übernehmen und Zugriff auf vertrauliche Dokumente und Kommunikationen zu erhalten. Alle E-Mails, die von APT28 gesendet wurden, wurden von Google bereits blockiert. /BSI21i06/

Beschreibung

Ende September 2021 informierte Google 1.4000 Nutzer seines E-Mail-Servers Gmail, dass die APT-Gruppierung APT28 / Fancy Bear einen Spear-Phishing-Angriff auf ihre E-Mail-Postfächer durchgeführt hat mit dem Ziel deren Passwörter zu stehlen, um so Zugriff auf die Postfächer zu erhalten und an die darin enthaltenen Informationen zu gelangen. Nach der üblichen Vorgehensweise von APT28 wären diese Informationen dann genutzt worden, um auf die Postfächer weiterer Personen und die darin enthaltenen Informationen zuzugreifen. Alle schadhaften E-Mails wurden von Gmail jedoch automatisch als Spam-Nachrichten klassifiziert und blockiert. Der Angriff war zwar global, richtete sich aber gegen einen ausgewählten Personenkreis von Aktivisten, Journalisten, Regierungsmitarbeitern, Menschenrechtlern, Rechtsanwälten und Angestellten im Bereich der Nationalen Sicherheit. Insgesamt waren nur 0,1% der Gmail-Nutzer betroffen. /BSI21i06/, /MAL21w03/, /MOT21w01/

Google empfiehlt Personen, aus den oben genannten Bereichen ihre Gmail-Konten durch die zusätzliche Aktivierung der Schutzmaßnahmen seines Advanced Protection Program (APP) abzusichern. Das APP bietet Schutz gegen Phishing-Angriffe und Malware. Es sieht die Verwendung von physischen USB-Sicherheitsschlüsseln vor, welche häufig in Kombination mit einer weiteren Sicherheitsinformation wie z. B. einem Passwort eingesetzt werden, d. h. einer Zwei-Faktor-Authentifizierung. Zusätzlich scannt der Google Chrome Browser im APP alle Dateien, die heruntergeladen werden sollen. Dabei werden Dateien abgelehnt, die von unseriösen oder unbekannten Quellen stammen. /BSI21i06/, /VER21w01/, /ZDN21w02/, /MAL21w03/

Die APT-Gruppierung APT28 ist spätestens seit 2004 aktiv. Sie gehört zu Russlands militärischem Geheimdienst und ist Teil des Hauptnachrichtendienstes des russischen Generalstabes (GRU), 85. Haupt-Sonderdienstleistungszentrum (GTsSS), militärische Einheit 26165. APT28 führte 2016 die IT-Angriffe auf die Wahlkampagne von Hillary Clinton und das Nationale Komitee der Demokraten in den USA durch. /BAN21w01/, /REC21w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.9 APT28 – IT-Angriffe im Rahmen einer Brute Force Kampagne

Übersicht

Am 01.07.2021 veröffentlichten die NSA, CISA, das FBI und das britische National Cyber Security Center (NCSC) Advisories zu einer Spionagekampagne der APT-Gruppierung APT28, welche gegen US-amerikanische und europäische Organisationen gerichtet ist. Die Kampagne soll bereits 2019 begonnen haben. /BSI21i08/

Beschreibung

Im Sommer 2020 berichtete die Sicherheitsfirma TrendMicro bereits über die IT-Angriffe, die nach den oben genannten Advisories von 2021 der APT-Gruppierung APT28 zugeordnet werden, welche u. a. unter dem Namen Fancy Bear bekannt ist. Die APT-Gruppierung APT28 ist mindestens seit 2004 aktiv. Die Angriffe richten sich gegen Regierungen und Parteien, das Militär und Verteidigungsunternehmen, Energie- und Logistikkonzerne, Universitäten und Medien sowie Anwaltskanzleien und Medienunternehmen in den USA und Europa /NCS21i01/. Die Angriffe erfolgen über Microsoft Office 365 Cloud-Dienste und E-Mail-Server, die eine Vielzahl verschiedener Protokolle verwenden /NCS21i01/. Dabei setzen die Angreifer Brute-Force-Techniken ein und nutzen bekannte Schwachstellen aus, um sich Zugriff auf die Systeme zu verschaffen. /BSI21i08/

Bei einem Brute-Force-Angriff wird von einem Angreifer versucht ein Passwort, einen Benutzernamen, die Adresse einer verborgenen Webseite oder einen Schlüssel nach

dem Versuch-und-Irrtum-Prinzip zu erraten. Je nach Komplexität des Passwortes kann dieser Versuch wenige Sekunden bis zu mehreren Jahren dauern. Die Brute-Force-Angriffe von APT28 sind auf geschützte Daten wie E-Mails und die Identifizierung von Kontenanmeldeinformationen ausgerichtet. Diese Informationen werden dann genutzt, um den Erstzugriff auf das Netzwerk, eine persistente Verbindung und eine Privilegien-Eskalation zu erreichen, sowie Schutzfunktionen zu umgehen. /KAS21w02/, /NCS21i01/

Im Zuge der Brute-Force-Kampagne verwendeten die Angreifer das Framework Kubernetes, um die Effektivität der Angriffe zu erhöhen. Ein solches Vorgehen ist zuvor noch nicht beobachtet worden. Das Kubernetes-Cluster, das bei den Angriffen eingesetzt wird, dient dazu Brute-Force-Authentifizierungsversuche zu verschleiern und sie über Tor- und kommerzielle VPN-Dienste weiterzuleiten. /BSI21i08/, /THR21w02/

Darüber hinaus nutzen die Angreifer die Schwachstellen CVE 2020-0688 und CVE 2020-17144 des Microsoft Exchange E-Mail-Servers aus, um per Fernzugriff Programmcode auszuführen und um den Zugriff auf das Zielnetzwerk zu erhöhen. /NCS21i01/

Da die Angriffe auf Default- oder schwache Passwörter abzielen, sind sie leicht zu verhindern, indem starke Passwörter, eine Zwei-Faktor-Authentifizierung (2FA), Sperrungen bei Fehlversuchen oder das Blockieren von VPN- und Tor-Verbindungen verwendet werden. Schutz bietet auch die Umsetzung des Zero Trust Security-Modells. /BSI21i08/, /NCS21i01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.10 REvil – IT-Angriff auf US-Fleischkonzern JBS

Übersicht

Nach einem IT-Angriff auf den weltgrößten Fleischkonzern JBS mit Hauptsitz in Brasilien und Aktivitäten vor allem in Australien, Nord- und Südamerika, der am 30.05.2021 entdeckt wurde, wurden große Teile des Betriebs in den USA, aber auch einige Betriebe in Australien und Kanada vorübergehend stillgelegt. /HEI21w08/, /BLO21w01/, /TEC21w01/

Beschreibung

JBS gab Anfang Juni 2021 bekannt, Opfer eines IT-Angriffs mit Ransomware zu sein. Der weltweit größte Produzent von Rind- und Schweinefleisch wurde dabei Ziel eines organisierten IT-Angriffs, der einige Server der nordamerikanischen und australischen IT-Systeme von JBS betraf. Unmittelbar nach dem Entdecken des Angriffs wurden nordamerikanische und australische IT-Systeme außer Betrieb gesetzt, um das weitere Eindringen zu verhindern, eine mögliche Infektion zu begrenzen und die Kernsysteme zu schützen. Alle Schlachtbetriebe in den USA wurden geschlossen, die Behörden informiert und Fachleute zu Rate gezogen. /SEN21w02/, /BLO21w01/, /TEC21w01/

Da die verschlüsselten Backup-Server von JBS nicht infiziert wurden, erfolgte eine relativ schnelle Wiederherstellung der Systeme und die Rückkehr zum Betrieb innerhalb weniger Tage. / BLO21w01/, /TEC21w01/ Nachdem die Anlagen wieder in Betrieb waren, erfolgte eine Zahlung von umgerechnet 11 Millionen Dollar Lösegeld in Form von Bitcoins. Die Bezahlung erfolgte, um weitere Störungen durch die Angreifer zu verhindern und den reibungslosen Betrieb wiederherstellen zu können. Es kam laut JBS zu keiner Kompromittierung von Unternehmens-, Kunden- und Mitarbeiterdaten. /BBC21w01/, /TAG21w02/

Laut Berichten mehrerer Medien unter Berufung auf das FBI wurde der IT-Angriff von der Gruppe REvil/Sodinokibi ausgeführt, die aus Russland agiert. /HEI21w09/, /SEC21w13/ Dabei wurde Ransomware eingesetzt, wobei neben der Verschlüsselung von Daten gleichzeitig Spionage und Datendiebstahl betrieben werden sollte, um JBS mit der Androhung einer Veröffentlichung der Daten noch stärker unter Druck zu setzen. Die Gruppe REvil bietet so genannten Ransomware-as-a-Service (RaaS) an, d. h. sie bietet auch Dritten, die über keinerlei Programmierkenntnisse verfügen, Ransomware gegen Bezahlung an. /SEC21w13/ Der Angriff auf JBS basierte vermutlich auf QBot-Malware, eine modulare Malware, die in der Lage ist, sensible Daten zu kompromittieren. Es wurden Hinweise entdeckt, dass bereits Mitte April 2021 eine QBot-Infektion bei JBS vorlag. /WTW21w01/ Der Zugang zu den IT-Systemen von JBS wurde über ein altes, nicht mehr genutztes Konto erreicht, welches mit einem schwachen Passwort geschützt und nicht deaktiviert worden war. /HIL21w01l/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.11 Conti - IT-Angriff auf den irischen Gesundheitsdienst

Übersicht

Am 14.05.2021 kam es zu einem IT-Angriff auf den irischen Gesundheitsdienst HSE (Health Service Executive), welcher diverse Dienste für alle Krankenhäuser und Gemeinden in ganz Irland bereitstellt. Aufgrund des Angriffs wurde das gesamte Computersystem des irischen Gesundheitsdienstes abgeschaltet, wodurch zahlreiche Krankenhäuser ihren Betrieb einschränken mussten.

Routinetermine wurden vielerorts abgesagt, der Betrieb in den Notaufnahmen lief weiter, war aber beeinträchtigt. /AER21w01, FAZ21w03, TAZ21w01/

Beschreibung

HSE wurde Ziel eines organisierten IT-Angriffs mit der Ransomware Conti, bei dem die IT-Systeme infiltriert wurden. Unmittelbar nach Entdecken des Angriffs wurde von der HSE der Prozess für die Reaktion auf IT-Angriffe in Gang gesetzt, wobei entschieden wurde, alle IT-Systeme abzuschalten und das „National Healthcare Network“ vom Internet zu trennen, um zu versuchen, die Auswirkungen des Angriffs einzugrenzen und zu bewerten. Dies führte dazu, dass alle Mitarbeiter im Gesundheitswesen keinen Zugang mehr zu allen von der HSE bereitgestellten IT-Systemen hatten. Dadurch kam es zu schweren Störungen der Gesundheitsdienste im ganzen Land. /HSE21r01/

Bei dem Angriff sind Dateien verschlüsselt und gestohlen worden und es wurde mit der Veröffentlichung der gestohlenen Patientendaten gedroht. Es wurde ein Lösegeld von 20 Millionen Euro für die Entschlüsselung und Nicht-Veröffentlichung der Daten gefordert, welches nicht gezahlt wurde. Später wurden vertrauliche medizinische Daten von über 500 Patienten sowie Unternehmensdokumente im Internet veröffentlicht. Am 23.06.2021, also mehr als einen Monat nach dem Angriff, waren lediglich 75 % der Daten entschlüsselt und 70 % der IT-Systeme wieder in Betrieb. Es dauerte noch bis Ende September 2021, bis nahezu alle Systeme wieder in Betrieb waren /TAZ21w01/, /IRT21w01/, /RTE21w01/, /BLE21w01/, /HSE21r01/

Laut Berichten mehrerer Medien wurde der IT-Angriff von der Gruppe Conti ausgeführt, die aus Russland agiert. /TAZ21w01/, /IRT21w02/ Mittels der eingesetzten Ransomware wurde neben der Verschlüsselung von Daten gleichzeitig Spionage und Datendiebstahl betrieben, um HSE mit der Androhung einer Veröffentlichung der Daten stärker unter Druck zu setzen. /BLO21w02/ Am 16.03.2021 wurde der Angriff mit dem Senden einer maliziösen Phishing-E-Mail an einen Arbeitsplatz begonnen. Dabei wurde eine maliziöse Excel-Datei geöffnet, über welche von den Angreifern der Zugriff auf die Systeme geschaffen wurde. In den darauffolgenden Wochen wurde der Zugriff auf weitere Systeme ausgeweitet. Bereits vor der Ausführung der Ransomware wurden Aktivitäten von einer Antivirensoftware entdeckt. Da diese allerdings nur im Überwachungsmodus arbeitete, wurden die Aktivitäten nicht blockiert. Begünstigt wurde der IT-Angriff durch die IT-Systeme der HSE, die veraltet und nicht gegen IT-Angriffe gewappnet waren. /HSE21r01/

Das National Cyber Security Center stellte fest, dass beim Angriff das käuflich zu erwerbende Penetrationstest-Tool Cobalt Strike verwendet wurde. Mit diesem konnten sich die Angreifer durch die Systeme von HSE bewegen, um diese zu infizieren, ausführbare Dateien zu installieren und eine Variante der Conti-Ransomware zu installieren. /NCS21r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.12 IT-Angriffe mit SparrowDoor

Übersicht

Seit August 2019 greift die APT-Gruppierung FamousSparrow hauptsächlich Hotels aber auch andere Organisationen und Unternehmen (z. B. aus dem Ingenieurwesen) auf der ganzen Welt mit der Backdoor SparrowDoor an. Das Ziel der Angriffe ist vermutlich die Durchführung von Spionageaktivitäten.

Beschreibung

Seit August 2019 nutzt die APT-Gruppierung FamousSparrow Schwachstellen im Microsoft Exchange E-Mail-Server, in Microsoft SharePoint und in Oracle Opera (Software für

das Hotelmanagement), um initialen Zugriff auf IT-Netzwerke zu erhalten und dort die Backdoor SparrowDoor zu verbreiten. Die Angriffe richten sich hauptsächlich gegen Hotels aber auch gegen Regierungen, internationale Organisationen, Ingenieurunternehmen, Anwaltsfirmen und private Organisationen auf der ganzen Welt, vermutlich mit dem Ziel der Spionage. Von den bisherigen Angriffen waren Kanada, Brasilien, Burkina Faso, Israel, Frankreich, Großbritannien, Guatemala, Litauen, Saudi-Arabien, Südafrika, Taiwan und Thailand betroffen. Am 2. März 2021 veröffentlichte Microsoft Patches für den Exchange Server, um vier unter dem Namen ProxyLogon bekannte Schwachstellen zu schließen /BOR21w01/, /ESE21w01/. Sie ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware, wobei Exchange-Online jedoch nicht von den Schwachstellen betroffen ist /BSI21i03/. Bereits einen Tag nach Veröffentlichung der Patches, wurden die Schwachstellen von FamousSparrow für die Verbreitung von SparrowDoor ausgenutzt. /ESE21w02/, /THP21w01/

Haben die Angreifer sich initialen Zugriff auf das Netzwerk einer Organisation verschafft, installieren sie eine Vielzahl von Schadsoftware-Werkzeugen: Eine Variante von Mimikatz für die laterale Bewegung im Netzwerk, eine Komponente, die die Befehlszeilenanwendung ProcDump installiert und diese vermutlich nutzt, um Zugangsdaten aus Speichern auszulesen, den NetBIOS-Scanner Nbtscan, um Dateien und Drucker in einem LAN-Netzwerk zu identifizieren und schließlich einen Loader für die Backdoor SparrowDoor. Der Loader wiederum installiert dann die Backdoor, wobei ein Eintrag in der Registry von Windows erzeugt wird, um eine persistente Verbindung herzustellen. SparrowDoor verbindet sich mit dem Command-and-Control-Server (C&C) der Angreifer über Port 443 (HTTPS) und stellt verschiedene Funktionen bereit. Über SparrowDoor können Dateien umbenannt oder gelöscht werden. Weitere Funktionen sind das Erstellen von Ordnern, das Beenden von Prozessen, das Senden von Dateiinformationen (Attribute, Größe und Erstellzeitpunkt) sowie das Auslesen von Dateien und das Schreiben von Daten in Dateien. Darüber hinaus besitzt die Backdoor einen Kill-Switch, um die Einstellungen für die persistente Verbindung und die Backdoor selbst löschen zu können. /ESE21w02/, /THP21w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.13 IT-Angriff auf WestRock

Übersicht

Am 23.01.2021 kam es zu einem IT-Angriff auf WestRock, dem zweitgrößten Unternehmen zur Produktion von Verpackungen wie beispielsweise Kartons in den USA. Der Angriff hatte sowohl Auswirkungen auf das IT-Netzwerk (Büro-Netzwerk) als auch auf das OT-Netzwerk). Aufgrund des Angriffs wurden diverse Systeme proaktiv abgeschaltet, um eine weitere Ausbreitung zu verhindern. Durch den Angriff wurden mehrere Produktionsprozesse außer Betrieb gesetzt. /SEC21w14/, /THR21w03/, /SEC21w15/, /DAR21w03/

Beschreibung

WestRock wurde Ziel eines IT-Angriffs mit Ransomware, bei dem sowohl IT- als auch OT-Systeme betroffen waren.

Durch den Angriff wurden einige der wichtigsten OT-Systeme von WestRock beeinträchtigt, wodurch es zu Auswirkungen auf die Produktion kam. Hinsichtlich der eingesetzten Ransomware und der Fragen, ob ein Lösegeld gezahlt wurde, ggf. wie und von wem der Angriff eingeleitet wurde, liegen keine Informationen vor. /HEI21w10/, /SEC21w14/

Unmittelbar nach der Entdeckung des Angriffs wurde mit Untersuchungen zu dem Angriff und dessen Auswirkungen begonnen. Mit Unterstützung von externen Experten zur Informationssicherheit wurden Maßnahmen zur Eingrenzung der Auswirkungen getroffen. Außerdem wurden sofort Bemühungen aufgenommen, die Systeme wiederherzustellen und den Geschäftsbetrieb aufrechtzuerhalten und die Auswirkungen auf Kunden und Mitarbeiter zu minimieren. Es gibt keine Hinweise darauf, dass durch den Angriff Daten von Kunden oder Mitarbeitern kompromittiert wurden. /SEC21w14/, /THR21w03/

Trotz der sofortigen Aufnahme von Maßnahmen zur Eingrenzung der Auswirkungen und zur Wiederherstellung der Systeme waren auch mehr als zwei Wochen nach dem Angriff noch nicht alle Systeme wiederhergestellt. Dies führte zu Verzögerungen im Geschäftsbetrieb und bei der Warenproduktion, die um 85.000 Tonnen niedriger lag als geplant, was in etwa einem Produktionsausfall von zwei kompletten Tagen entspricht. Der Angriff hatte Auswirkungen auf den Nettoumsatz von etwa 189 Millionen US-Dollar und auf das Quartalsergebnis von etwa 80 Millionen US-Dollar. Zusätzlich entstanden Kosten von

etwa 20-Millionen US-Dollar für die Wiederherstellung der Daten, was hauptsächlich auf Ausgaben für externe Experten zurückzuführen ist. /SEC21w14/, /THR21w03/, /CSO22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.14 Cuba – IT- Angriffe auf kritische Infrastruktur

Übersicht

Eine russische APT-Gruppierung kompromittierte mit Hilfe der Cuba-Ransomware mindestens 49 Einrichtungen im Bereich der kritischen Infrastrukturen und erbeutete dabei 43,9 Millionen Dollar an Lösegeld für die Wiederherstellung der von ihnen verschlüsselten Daten. Bei den Angriffen kam eine Vielzahl an Schadsoftware-Komponenten und Angriffstechniken zum Einsatz.

Beschreibung

Bei den Angreifern, die die Cuba-Ransomware einsetzen, handelt es sich um eine russische APT-Gruppierung. Sie kompromittierten mindestens 49 Einrichtungen im Bereich der Kritischen Infrastrukturen und erbeuteten dabei 43,9 Millionen Dollar. Ursprünglich hatten die Angreifer sogar 74 Millionen Dollar Lösegeld für die Wiederherstellung der von ihnen verschlüsselten Daten gefordert. Zu den Angriffszielen gehören der Finanzsektor, Behörden und Regierungen, Gesundheitsorganisationen sowie Produktions- und Informationstechnik-Unternehmen in den USA, Südamerika und Europa. /CPO21w02/, /ZDN21w03/

Die Cuba-Ransomware wurde bei den Angriffen unter Zuhilfenahme der Hancitor-Malware verteilt. Diese lädt Diebstahl-Ransomware wie Remote Access Trojaner (RATS) auf die Netzwerke der Opfer. Darüber hinaus verschaffen sich die Angreifer über Phishing-E-Mails, die Ausnutzung von Microsoft Exchange-Schwachstellen und kompromittierte Zugriffsrechte, sowie über Remote-Desktop-Protokolle (RDP) Zugriff auf die Netzwerke. Die Login-Rechte der RDP wurden zuvor durch den Einsatz des Programms Mimikatz gestohlen. Die Angreifer nutzen legitime Windows Systemdienste wie PowerShell und PsExec und Windows Administratorrechte, um die Cuba-Ransomware

auf dem infizierten Netzwerk auszuführen. Diese lädt zwei zusätzliche Payloads, eine zum Diebstahl von Passwörtern und eine zum Aufbau einer Kommunikationsverbindung zum C&C-Server der Angreifer, dessen URL sich in Montenegro befindet. Schließlich verschlüsselt die Cuba-Ransomware Dateien und benennt deren Dateiendung in .cuba um. /CPO21w02/

Die Angreifer verlangen eine Lösegeldzahlung, nach deren Überweisung die Dateien angeblich wiederhergestellt würden. Seit Beginn des Jahres 2021 betreibt die APT-Gruppierung eine Leak-Webseite, auf der sie erbeutete Daten veröffentlicht, sollte das Lösegeld nicht überwiesen werden. Darüber hinaus wurden einige der gestohlenen Daten von den Angreifern verkauft. /PRB21w01, ZDN21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.15 Conti – IT-Angriff auf ONTEC

Übersicht

Am 08.11.2021 wurde festgestellt, dass es zu einem IT-Angriff auf die ONTEC Automation GmbH, einem Unternehmen des Maschinen- und Anlagenbaus und Spezialist für den Bau von Automatisierungssystemen und Sondermaschinen für die industrielle Produktion, gekommen ist. Damit ist durch diesen Angriff ein Unternehmen betroffen, welches industrielle Steuerungssysteme herstellt. Aufgrund des Angriffs kam es zur Verschlüsselung der IT-Infrastruktur des Unternehmens. /UNT21w01/

Beschreibung

Die deutsche ONTEC Automation GmbH wurde Ziel eines IT-Angriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Conti bekannt hat /RED21w01/. Laut /FRA21w01/ mit Bezug auf eine ONTEC Presseerklärung wurde der Angriff frühzeitig erkannt und es umgehend Gegenmaßnahmen eingeleitet. Im Zuge dieser Maßnahmen wurden IT-Systeme abgeschaltet, es kam aber dennoch zu einer Verschlüsselung weiter Teile der IT-Systeme. Dadurch, dass die Daten wiederhergestellt und Systeme neu aufgesetzt werden mussten, kam es möglicherweise zu Verzögerungen in der Geschäftsabwicklung, wobei die Produktion und die Erreichbarkeit laut /UNT21w01/ nicht betroffen

waren. Konkrete Angaben zum Angriffszeitpunkt und zu den detaillierten Auswirkungen liegen nicht vor. Ebenfalls liegen keine Angaben zur Höhe eines möglicherweise geforderten Lösegeldes vor.

Conti ist eine bekannte Ransomware-Gruppierung, die von einer russischen Gruppe betrieben wird und bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. In der Regel verschafft sich Conti Zugang zu einem Unternehmensnetzwerk, nachdem ein Gerät durch einen Phishing-Angriff mit den Schadprogrammen Bazar-Loader oder TrickBot infiziert wurde. Darauffolgend breitet sich Conti lateral im Opfernetzwerk aus und stiehlt Daten, die auf Conti-Server geladen werden. Dann erfolgt die Verschlüsselung der Daten und die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie. Es wird ein Lösegeld für die Entschlüsselung der Daten verlangt. Wird dieses nicht gezahlt, werden die Daten nicht entschlüsselt und außerdem veröffentlicht. /BLE22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.16 Tiny Turla- Globale IT-Angriffe

Übersicht

Im Rahmen der IT-Angriffe der APT-Gruppierung Turla (siehe Kapitel 3.12.13) kam es zum Einsatz der neuen Schadsoftware Tiny Turla. Die Schadsoftware Tiny Turla wurde im September 2021 entdeckt, aber bereits seit 2020 genutzt, um Systeme in den USA, Afghanistan und Deutschland zu kompromittieren. /BSI21r04/

Beschreibung

Tiny Turla soll als heimliche Rückfall-Backdoor genutzt worden sein, um den Zugriff auf das System aufrechtzuhalten, wenn die primär von der APT-Gruppierung Turla genutzte Schadsoftware entfernt wurde. Die Schadsoftware ist dabei nicht aufgefallen, da sie über einen recht einfachen, aber effizienten Code verfügt. Sie ist auf die Nutzung grundlegender Aufgaben beschränkt, wie das Herunterladen, Hochladen und Ausführen von Dateien. /TAL21r01/, /BLE21w02/, /BSI21r04/

Die primäre Schadsoftware ist in Kapitel 3.12.13 zur APT-Gruppierung Turla und in Abschnitt B.6.4 zum IT-Angriff mittels Epic Turla, der als erster Schritt zur Infektion durchgeführt wird, beschrieben.

Tiny Turla wurde als Dienst auf dem infizierten Rechner installiert. Dabei wurde eine .bat-Datei genutzt, um den Dienst als harmlos aussehenden, gefälschten Windows Time-Dienst zu installieren. Um nicht entdeckt zu werden, wurde der Dienst wie ein tatsächlich existierender Windows-Dienst „Windows Time Service“ genannt. Beschreibung und Dateiname lassen ihn wie eine gültige Microsoft-DLL aussehen.

Die Schadsoftware kontaktiert den Command-and-Control-Server der APT-Gruppierung Turla über einen verschlüsselten HTTPS-Kanal alle fünf Sekunden, um zu prüfen, ob neue Befehle vorliegen. /TAL21r01/, /BLE21w02/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor. Laut /BFV16l01/ zeigten die Angreifer bei Epic Turla ein Interesse an Wirtschaft und Forschung in den Bereichen Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung. Aus diesem Grund ist ein kerntechnischer Bezug bei Tiny Turla nicht auszuschließen.

B.13.17 IT-Angriff auf Vestas

Übersicht

Am 19.11.2021 wurde festgestellt, dass es zu einem IT-Angriff auf Vestas Wind Systems A/S, einem der weltweit größten Hersteller von Windenergieanlagen (kritische Infrastruktur) mit Hauptsitz in Dänemark, gekommen ist. Aufgrund des Angriffs wurden vorsorglich diverse IT-Systeme an mehreren Standorten abgeschaltet, um eine weitere Ausbreitung zu verhindern. /BSI21r06/, /BLO21w04/

Beschreibung

Vestas wurde Ziel eines IT-Angriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Lockbit bekannt hat. Nach Entdeckung des Angriffs wurden umgehend Gegenmaßnahmen eingeleitet, wobei als Vorsichtsmaßnahme mehrere

IT-Systeme an mehreren Standorten heruntergefahren wurden. Des Weiteren wurde in Zusammenarbeit mit externen Experten damit begonnen, das Problem einzugrenzen und die Systeme wiederherzustellen. OT-Systeme sind von den Angriffen laut Vestas nicht betroffen gewesen, außerdem sollen keine Daten von Kunden oder Lieferketten entwendet worden sein. Aufgrund der Abschaltung der IT-Systeme können allerdings Kunden, Mitarbeiter und andere Interessengruppen betroffen gewesen sein. Auf bereits betriebene Windenergieanlagen oder die Wartung der Anlagen hatte der Angriff laut Vestas keine Auswirkungen. /BSI21r06/, /BLO21w04/

Trotz der sofort eingeleiteten Maßnahmen zur Eingrenzung der Auswirkungen und Wiederherstellung der Systeme, waren laut /ITD21w01/ am 06.12.2021 zwar die meisten, aber noch nicht alle Systeme wieder betriebsbereit.

Bei dem Angriff wurden von der Ransomware-Gruppierung Lockbit unrechtmäßig Daten gestohlen und es wurde mit einer Veröffentlichung dieser Daten gedroht. Bei den gestohlenen Daten handelte es sich auch um personenbezogene Daten, wobei diese vermutlich nicht in erster Linie das Ziel des Angriffs waren. Es handelte sich ausschließlich um Daten, die auf Vestas internen File-Sharing-Systemen gelagert werden.

Bei den gestohlenen personenbezogenen Daten handelte es sich größtenteils um Namen, Adressen, Telefonnummern sowie Details zur Anstellung wie z. B. Gehalt und Lebenslauf von Mitarbeitern von Vestas. In wenigen Fällen wurden aber auch sensiblere Daten von Vestas-Mitarbeitern wie z. B. Pässe oder Bankdaten gestohlen. Es gibt keine Hinweise darauf, dass personenbezogene Daten gestohlen wurden, die nicht Mitarbeiter von Vestas betreffen. Da Vestas nach eigenen Angaben kein Lösegeld gezahlt hat, wurden alle gestohlenen Daten von Lockbit am 08.12.2022 veröffentlicht, wobei es sich um insgesamt mehr als 7.700 Dateien handelte. Über eine Höhe des geforderten Lösegeldes oder weitere Einzelheiten sind keine Informationen bekannt. /ITD21w01/, /WIN21w01/, /INS21w02/, /SEC21w16/

LockBit ist eine Ransomware-Gruppierung, deren erste Angriffe im September 2019 bekannt geworden sind, wobei die Gruppierung zu diesem Zeitpunkt noch ABCD genannt wurde. /FBI22r01/ Bei LockBit handelt es sich um eine Ransomware-as-a-Service-Gruppierung (RaaS), die laut /REC22w01/ eine der produktivsten aktiven Gruppierungen ist und im Jahr 2022 bereits mindestens 650 Organisationen angegriffen hat (Stand: Ende Juni 2022). Die Gruppierung führt zielgerichtete Angriffe auf Unternehmen und Regierungsorganisationen aus, Privatpersonen sind eher keine Angriffsziele. Es werden

Unternehmen weltweit angegriffen, wobei bewusst Unternehmen mit Standort in Russland gemieden werden.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

B.13.18 IT-Angriffe auf die Vereinten Nationen

Übersicht

Von April 2021 bis August 2021 wurden die Computersysteme der Vereinten Nationen (UN) Opfer mehrerer IT-Angriffe, bei denen Angreifer in die Computersysteme der UN eingedrungen sind. Die IT-Angriffe dienten vermutlich dem Sammeln von Informationen. Systeme oder Dateien wurden nach Aussage der UN nicht beschädigt. Wer für die Angriffe verantwortlich ist und ob außer dem Sammeln von Informationen weitere Motive hinter den Angriffen stehen, ist unklar. /BSI21r05/, /Hei21w11/, /BLO21w03/

Beschreibung

Der erste Angriff dieser Angriffswelle (es gab schon frühere Angriffe auf die UN, die hier nicht betrachtet werden) auf die Computersysteme der UN erfolgte vermutlich am 05. April 2021. Dieser Angriff wurde laut UN erkannt und es wurde darauf reagiert, wobei keine detaillierten Angaben zur Reaktion bekannt sind. Auf diesen Angriff folgten weitere Angriffe, die entdeckt und auf die nach Aussage der UN ebenfalls angemessen reagiert wurde. Nach Recherchen der Cyber-Sicherheitsfirma Resecurity, die den Angriff als erste entdeckt hat, waren die Angreifer bis zum 07. August 2021 im Netzwerk der UN aktiv. /BSI21r05/, /Hei21w11/, /BLO21w03/

Laut Aussage der UN haben die Angreifer keine Systeme beschädigt und keine Dateien entwendet oder verschlüsselt. Laut UN haben sie sich lediglich im Netzwerk umgesehen und Screenshots gemacht. Es existieren gegensätzliche Aussagen von Recesurity, denen zufolge es Beweise zu gestohlenen Daten geben soll. Ungeachtet dessen, ob tatsächlich Dateien gestohlen oder ausschließlich Screenshots gemacht wurden, konnten durch den Angriff Informationen über die Computernetzwerke der UN gesammelt werden. Die somit gesammelten Daten könnten von den Angreifern zum Kauf angeboten oder verwendet werden, um weitere Angriffe auf die UN oder andere Organisationen

durchzuführen. In der Zeit von April bis August 2021 wurde mit den gesammelten Daten aus dem ersten Angriff versucht, mindestens 53 weitere Konten von Nutzern des UN-Netzwerks zu kompromittieren, möglicherweise mit dem Motiv langfristig weitere Daten sammeln zu können. /BSI21r05/, /Hei21w11/, /BLO21w03/

Der Zugriff auf das Computersystem der UN durch die Angreifer erfolgte über die Projektmanagement-Software Umoja, einer proprietären, UN-eigenen Software. Es ist keine Sicherheitslücke in der Software bekannt, der Zugriff auf die Software erfolgte über einen gestohlenen Benutzernamen und das Passwort eines UN-Mitarbeiters, die von den Angreifern im Darknet erworben wurden. Die Zugangsdaten wurden im Darknet von mehreren russischsprachigen Personen angeboten und waren Teil eines Paketes mit Dutzenden Benutzernamen und Passwörtern von verschiedenen Organisationen, welches für 1.000 US-Dollar verkauft wurde. Der Zugriff über die Software Umoja ermöglichte einen tieferen Zugang zum Computersystem der UN und die Auskundschaftung des Netzwerkes. Es wurde der Versuch unternommen, die Rechte zu erweitern. Zum Zeitpunkt der ersten Angriffe verfügte die Software Umoja nicht über eine Multifaktor-Authentifizierung beim Login, welche den Angriff möglicherweise hätte verhindern können. Erst im Juli 2022 gab das Entwicklungsunternehmen von Umoja bekannt, dass eine Multifaktor-Authentifizierung beim Login implementiert wurde. /BSI21r05/, /Hei21w11/, /BLO21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.13.19 Ransomware – IT-Angriff auf Sogin

Übersicht

Im Dezember 2021 bestätigte das italienische Unternehmen Sogin, Opfer eines IT-Angriffs geworden zu sein. Bei Sogin handelt es sich um eine staatliche Firma, die vom italienischen Wirtschafts- und Finanzministerium finanziert wird und die sich um den Rückbau der italienischen Kernkraftwerke und nukleare Entsorgung einschließlich sonstiger radioaktiver Stoffe kümmert. Parallel dazu wurden bei diesem Angriff mutmaßlich gestohlene Unterlagen im Darknet zum Verkauf angeboten.

Beschreibung

Am 13.12.2022 gab das italienische Unternehmen Sogin bekannt, Opfer eines Cyberangriffs geworden zu sein. Sogin betonte dabei, dass die konventionelle und die nukleare Sicherheit der betreuten Anlagen und ihres Betriebes zu jeder Zeit gewährleistet gewesen seien. Details zum Angriff gab Sogin nicht bekannt. Gleichzeitig tauchten aber im Darknet mutmaßlich bei Sogin entwendete Daten zum Verkauf auf. Betroffen waren sensible Dokumente verschiedener Art. Darunter befanden sich beispielsweise Passwörter im Klartext, Ausschreibungen, technische Zeichnungen von Maschinen und Anlagen, Kostenvoranschläge, eine Karte eines von Sogin verwalteten Standorts, eine Liste der angeforderten Software- und Hardware-Updates, Lebensläufe von Mitarbeitern, Reiseberichte, Fotos von Besprechungen sowie Informationen zum Betrieb eines Arbeitsplatzes, der auf industrieller Ebene zur Anlagenüberwachung eingesetzt wird. Zusätzlich enthielten die angebotenen Daten auch persönliche Inhalte, was darauf hindeutet, dass das Material durch das Eindringen in einen Firmencomputer gestohlen worden sein könnte, der gleichzeitig für private Zwecke genutzt wurde. Es wird vermutet, dass die Angreifer über diese private Nutzung Zugang zu dem betroffenen Rechner erhielten. Eine offizielle Bestätigung hierfür liegt aber nicht vor. /WOR21w01/

Kerntechnischer Bezug

Da es sich bei Sogin um ein Unternehmen handelt, das für den Rückbau kerntechnischer Anlagen und die Entsorgung bzw. Lagerung radioaktiver Stoffe verantwortlich ist, besteht ein klarer kerntechnischer Bezug.

B.13.20 SquirrelWaffle-Loader

Übersicht

Im September 2021 wurde der Schadsoftwareloader SquirrelWaffle-Loader von IT-Sicherheitsforschern entdeckt, analysiert und veröffentlicht. SquirrelWaffle ist ein weiterer auf E-Mail Spam basierter Loader, welcher die Erstinfektion eines IT-Systems erreichen soll. Die hierzu genutzten E-Mails enthalten mit Makros versehene Microsoft Word oder Excel Dokumente und ermöglichen bei Ausführung der Makros eine vollautomatische Installation der Schadsoftware. /SEN21w03/

Beschreibung

Moderne Schadsoftwares sind zumeist modular aufgebaut, wobei bestimmte Aufgaben von verschiedenen Schadsoftwares übernommen werden. So übernimmt ein Modul die Verbreitung innerhalb eines Netzwerkes, ein anderes Modul die Ausspähung von wichtigen Daten auf betroffenen Systemen, ein weiteres Modul führt die Verschlüsselung aus und schließlich übernehmen Loader die Aufgabe der erstmaligen Infektion. Die Ansprüche an Schadsoftwareloader sind daher stetig mit steigenden Sicherungsmaßnahmen gewachsen. Ein und derselbe Schadsoftwareloader wird zum Teil bei völlig unterschiedlicher Schadsoftware, z. B. Ransomware oder Bankingtrojaner eingesetzt. Die Loader werden von den Entwicklern verkauft, vermietet oder zur freien Benutzung bereitgestellt. /SEN21w03/

Im September 2021 wurde eine neue Kampagne der Schadsoftwares Cobalt Strike und QakBot, zwei multifunktionalen Schadsoftwares, entdeckt. Beide nutzten für die Verbreitung sogenannte E-Mail-Antwortkettenangriffe, wobei bestehende Emailkorrespondenzen übernommen werden oder neue Emails den Anschein einer längeren Korrespondenz erzeugen sollen.

Werden die mitversendeten Word oder Excel Dateien des E-Mail Anhangs von den Nutzern ausgeführt, wird mittels Makro-Kette die Schadsoftware initialisiert. /SEN21w03/

Die Infektion findet dabei über ein PowerShell Skript statt, mit welchem die Daten des SquirrelWaffle Loaders auf dem betroffenen System festgeschrieben werden. Der Loader nutzt hierbei zur Verschleierung z. B. zufällige Dateinamen und besitzt damit Fähigkeiten zur Nichterkennung durch Sicherungssoftwares.

Nach erstmaliger Installation des SquirrelWaffle Loaders kontaktiert der Loader die C&C Infrastruktur, um Schadsoftware nachzuladen. Die Kommunikation zur C&C Infrastruktur wird dabei so weit wie möglich verschleiert. Konkrete Schadwirkungen werden über die als .txt Dateien nachgeladenen Schadsoftwares Cobalt Strike und Qakbot erreicht. /SEN21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14 2022

B.14.1 WhisperGate – IT-Angriffe auf ukrainische Einrichtungen

Übersicht

Mitte Januar 2022 wurde eine neue Schadsoftware bekannt, die Berichten zufolge vornehmlich gegen Ziele in der Ukraine – darunter Regierungseinrichtungen, Non-profit-Organisationen und IT-Organisationen – eingesetzt wurde und wird. Dabei handelt es sich um einen Wiper, der unter dem Deckmantel eines Ransomware-Angriffs den Master Boot Record des angegriffenen Systems zerstört. Die Schadsoftware wurde unter dem Namen WhisperGate bekannt.

Beschreibung

Bei WhisperGate handelt es sich um einen sogenannten 3-stufigen MBR (Master Boot Record) Wiper. In Schritt 1 wird der Master Boot Record überschrieben, ebenso Teile aller verbundenen Laufwerke. In Schritt 2 wird die Schadsoftware für Schritt 3 heruntergeladen und ausgeführt. In Schritt 3 werden alle Dateien mit einer Liste von 191 Dateiendungen abgeglichen und bei Übereinstimmung der Dateiendungen gelöscht.

Insgesamt beschädigt WhisperGate ein Windows-System so weit, dass Dateien und Laufwerke nicht mehr funktionsfähig und auch nicht wiederherstellbar sind. In Schritt 1 gibt WhisperGate Meldungen heraus, wie sie üblicherweise im Rahmen eines Ransomware-Angriffs angezeigt werden. So wird nach dem Reboot eine Ransomware-Nachricht angezeigt, die allerdings nur als Maskerade dient. WhisperGate besitzt keinerlei Wiederherstellungsmechanismen und versetzt ein erfolgreich kompromittiertes System in einen nicht wiederherstellbaren Zustand. Zusätzlich zur Maskerade als Ransomware nutzt die Schadsoftware auch Verschleierungsmechanismen, um einer Detektion oder Analyse zu entgehen. /REC22w02/

IT-Sicherheitsforscher sehen Parallelen zwischen WhisperGate und NotPetya (siehe Abschnitt3.12.11, 3.12.12), allerdings gilt WhisperGate als weniger komplex. Ein wesentlicher Unterschied zu NotPetya besteht darin, dass WhisperGate gleichzeitig zum Überschreiben des Master Boot Record auch versucht, die Partition C:/ zu überschreiben. /COM21w01/

Ein weiterer Aspekt, der von IT-Sicherheitsforschern hervorgehoben wird, bezieht sich auf die Einschleusung der Schadsoftware bei den Angriffszielen. Demnach ist es wahrscheinlich, dass die Angreifer über gestohlene Zugangsdaten bereits einige Zeit vor den Angriffen Zugriff auf Systeme bei den Angriffszielen hatten.

WhisperGate ist eine destruktive Schadsoftware, bei der weder Manipulation noch finanzieller Gewinn als Zielsetzung im Vordergrund steht, sondern vielmehr das Ziel, IT-Systeme in einen nicht wiederherstellbaren, funktionsunfähigen Zustand zu versetzen.

Hinter den Angriffen mit WhisperGate wird eine staatlich geförderte Angreifergruppierung vermutet. Bislang konnten die Angriffe keiner bekannten APT-Gruppierung zugeordnet werden, die Aktivitäten werden zunächst unter DEV-0586 weiterverfolgt.

Es wurde festgestellt, dass ein Großteil der angegriffenen Websites – hauptsächlich ukrainische Regierungswebsites – dasselbe Content-Management-Programm benutzen. Daher lag die Vermutung nahe, dass die Angreifer eine Schwachstelle in eben diesem Programm, OctoberCMS, ausnutzten. In der weiteren Folge wurde bekannt, dass die Mehrheit der Websites von ein und derselben ukrainischen Firma erstellt und betreut wurden, welche im Vorfeld kompromittiert worden war.

Dies machte es den Angreifern möglich, die Rechte und Zugangsdaten der betreuenden Firma bei deren Kunden zu missbrauchen. Dies legt den Verdacht nahe, dass WhisperGate in vielen Fällen über die Lieferkette eingebracht wurde.

Kerntechnischer Bezug

Der Fokus der bislang mit WhisperGate durchgeführten Angriffe lag auf ukrainischen Einrichtungen. Momentan ist nicht davon auszugehen, dass deutsche kerntechnische Anlagen derzeit zu den anvisierten Angriffszielen zählen. Bislang gibt es weder einen Bezug zu kerntechnischen Anlagen und Einrichtungen noch zu kritischen Infrastrukturen. Allerdings ist WhisperGate auf die Kompromittierung und Zerstörung von Windows-Systemen ausgerichtet, welche auch in deutschen kerntechnischen Anlagen in großer Anzahl vorhanden sind. Daher muss davon ausgegangen werden, dass die Schadsoftware bei entsprechendem Zugang zu den IT-Systemen, auch in deutschen kerntechnischen Anlagen einsetzbar wäre.

B.14.2 AcidRain – IT-Angriff auf die Satellitenkommunikation via KA-Sat

Übersicht

Am 26.02.2022 informierte Paxex.aero über einen Ausfall der Satelliten-basierten Kommunikation via KA-SAT, der auch Auswirkungen auf die Satelliten-basierte Breitbandversorgung in Europa hat. Vom BMUV wurde am 01.03.2022 eine kurzfristige Ersteinschätzung dieses Sachverhalts erbeten.

Beschreibung

Bei KA-SAT (KASAT Viasat) handelt es sich um einen Kommunikationssatelliten der US-amerikanischen Firma Viasat. Ursprünglich wurde KA-Sat im Auftrag der französischen Firma EUTELSAT Ende 2010 ins All befördert. Im April 2021 erwarb Viasat den Anteil von EUTELSAT an der Euro Broadband Infrastruktur (EBI), seither wird der Satellit auch unter der Bezeichnung KASAT Viasat geführt /VIA21w01/. EUTELSAT betreut derzeit noch die Infrastruktur am Boden, während Viasat die bereitgestellten Dienste betreut. Der Satellit bewegt sich auf einem geostationären Orbit bei 13 Grad Ost. Der Satellit verwendet für den Uplink 28-30 GHz, dieser erfolgt also im Ka-Frequenzband (26 bis 40 GHz), während der Downlink im Bereich 18,4 bis 20,2 GHz und daher im K-Frequenzband (18 bis 26 GHz) erfolgt. Mit 82 Spotbeams erreicht er eine europaweite Abdeckung (siehe Abb. B 1).

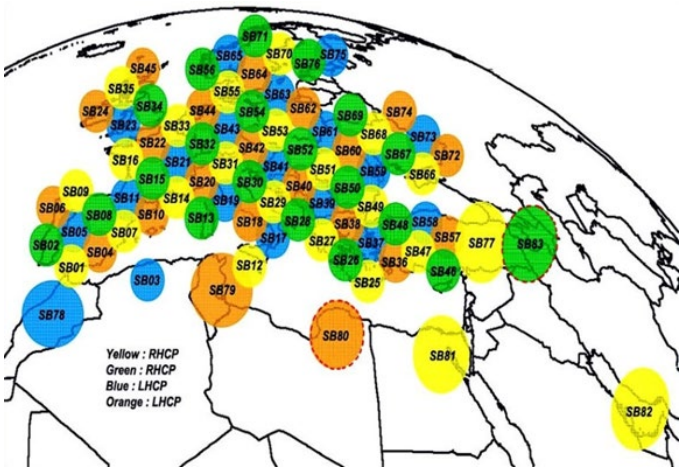

Abb. B 1 Europaweite Abdeckung durch Spotbeams des KA-SAT

Unterschiedliche Farben weisen unterschiedliche Frequenzen bzw. Polarisierungen aus /FRE16w01/

Jeder Spotbeam erlaubt eine Datenübertragung von bis zu 900 Megabit/s, insgesamt erreicht KA-SAT daher eine Gesamtkapazität von etwa 80 Gigabit/s. KA-SAT ist für das Routing des Datenverkehrs mit einem Netzwerk aus Bodenstationen verbunden. Über KA-SAT bietet Viasat Satelliteninternet für Europa und den Mittelmeerraum mit Datenübertragungsraten von bis zu 50 MBit/s im Download. /BSI22r01/, /TEC10w01/

Die Spotbeams werden über acht europaweit verteilte Bodenstationen angebunden, sog. Gateways. Zwar sind die Beams relativ unabhängig voneinander, ein Ausfall eines Gateways wirkt sich aber auf alle damit verbundenen Beams aus. /IDW22w01/

Der Sachverhalt des Ausfalls der Satelliten-basierten Kommunikation via KA-SAT stellt sich auf Basis der bis zum 02.03.2022 vorliegenden Informationen folgendermaßen dar:

Am 24. Februar 2022 erfuhr die Kommunikation über den KA-SAT eine Unterbrechung, welche einen teilweisen Ausfall der Dienste des KA-SAT Satellitennetzwerks über Europa nach sich zog. Der Ausfall betraf sowohl Satelliten-basiertes Internet als auch Satelliten-basierte Telefonie. Der Einbruch der Konnektivität ist in Abb. B 2 dargestellt.

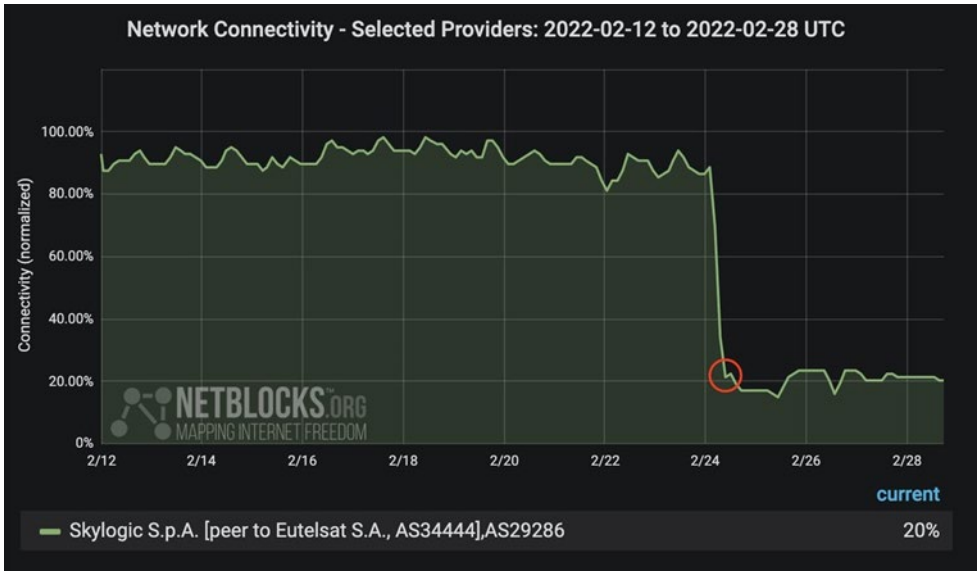

Abb. B 2 Einbruch der Konnektivität von KA-SAT am 24.02.2022

Grafik unverändert übernommen von netblocks.org

Die Störung begann am Donnerstag, den 24.02.2022, um 4 Uhr UTC morgens (entspricht 6 Uhr ukrainischer Zeit) /BSI22r01/, nahezu zeitgleich mit dem Angriff durch russische Streitkräfte auf die Ukraine. Hierbei wird ein Zusammenhang vermutet, Beweise hierzu liegen bisher allerdings nicht vor. Die Störung begann zunächst mit dem KA-SAT

Dienst in der Ukraine und breitete sich anschließend über fast die gesamte KA-SAT-Ausleuchtzone aus /GOL22w01/. Mehrere Internet Service Provider (ISP) melden als Folge des Ausfalls Probleme mit der Satelliten-basierten Breitbandversorgung in Europa. Darunter befinden sich der deutsche ISP EUSANET /BSI22r01/, /PAX22w01/, der tschechische ISP intv.cz /PAX22w01/, ein französischer ISP /PAX22w01/ sowie die schwedische NORDNET /NUM22w01/. Der Betreiber Viasat gab an, dass in Europa „zehntausende“ Kunden von dem Ausfall betroffen waren /REU22w02/.

Der Ausfall von KA-SAT hatte und hat auch Auswirkungen auf kritische Infrastruktur in Deutschland. Hierzu berichtet das BSI: „Der Windkraftanlagenhersteller Enercon berichtet gegenüber der Webseite Golem, dass der KA-SAT-Ausfall auch tausende Windkraftanlagen betreffe. Demnach sei eine Entstörung in Falle eines Fehlers von 5.800 Anlagen mit einer Gesamtleistung von elf Gigawatt aus der Ferne nicht möglich. Die Anlagen laufen jedoch autark weiter und die Steuerung ist weiterhin möglich. Nach Angaben des Bundesverbands Windenergie sei nur der Anbieter Euroskypark betroffen. Der KA-SAT Hersteller Viasat teilte der Webseite ZDNet mit, dass die Untersuchung des Ausfalls noch andauere. Man glaube, dass die Störung durch ein "cyber event" verursacht wurde.“

Das BSI fügt dieser Beschreibung folgende Bewertung des BSI-Fachreferats hinzu: „In Folge des KA-SAT-Ausfalls gingen im BSI mehrere Meldungen ein, da der Dienst u. a. zur Fernwartung von Windenergieanlagen genutzt wird. Der Dienst wird durch Wartungsunternehmen von Windanlagen zur Entstörung aus der Ferne genutzt. Durch den Ausfall des Dienstes ist eine zeitnahe Entstörung der Anlagen nicht mehr gegeben. Eine Entstörung im Fehlerfall kann aber bspw. von vor Ort erfolgen. Die betroffenen Anlagen sind weiterhin in der Lage, Strom zu erzeugen und ins Netz einzuspeisen. Für Netzbetreiber, die u. U. netzstabilisierende Maßnahmen ergreifen müssen, stehen redundante Verbindungsmöglichkeiten zur Verfügung. Daher sind Auswirkungen auf die Stromnetzstabilität nicht zu erwarten.“ /BSI22r02/

Die Dienste von KA-SAT kommen auch in anderen kritischen Infrastrukturen wie beispielsweise bei Einsatzfahrzeugen von Feuerwehren und Rettungsdiensten zum Einsatz. Das BSI bezieht sich hierbei auf eine ihm vorliegende Meldung „die beschreibt, dass von der Störung auch Geräte der Gefahrenabwehr wie beispielsweise Satellitenkommunikationssysteme von Einsatzleitfahrzeugen betroffen sind“ /BSI22r03/. In einer Veröffentlichung, die sich hauptsächlich an Betreiber von Leitstellen zur Gefahrenabwehr wendet, heißt es in einem entsprechenden Bericht: „Immer mehr

Einsatzleitfahrzeuge werden mit einer selbstausrichtenden 77-cm-Sende-Empfangs-Antenne und einem ViaSat-Modem nachgerüstet. Bei der Beschaffung neuer ELW taucht in den Ausschreibungen immer öfter das Ausstattungsmerkmal „Satellitenverbindung“ auf. Viele deutsche Feuerwehren und Rettungsdienste nutzen den schnellen Datensatelliten bereits, so z. B. das BRK Traunstein und Berchtesgadener Land, der Kreisfeuerwehrverband Südpfalz, die Feuerwehren in Paderborn und im Landkreis Darmstadt. In der französischen Region Rhône-Alpes sind die Feuerwachen bereits via KA-SAT miteinander verbunden und sogar die Administration des Service de Secours in Luxemburg hat sich für eine Satellitenlösung entschieden“ /BOS17r01/. Da sich dieser Bericht auf den Stand von 2017 bezieht, ist davon auszugehen, dass die Kommunikation über KA-Sat bei Einsatzfahrzeugen inzwischen breiter verbreitet ist, als hier umrissen. Auf eine Reihe von Anfragen im Rahmen der Informationstransparenz äußerten sich die Kreisverwaltung Südliche Weinstraße und die Kommunalverwaltung Paderborn zur Frage der Betroffenheit durch den KA-SAT Ausfall sowie vorhandene Rückfall-Lösungen. Beide bestätigten die Betroffenheit und gaben an, die Anbindung über KA-SAT nicht standardmäßig, sondern als Rückfallebene zu nutzen. Es wurde angegeben, dass die Primärlösungen im Gegensatz zur Kommunikation über KA-SAT von der Störung nicht betroffen, sondern voll funktionsfähig seien.

Es ist inzwischen bekannt, dass über KA-SAT auch Satellitenkommunikation für die ukrainische Polizei und das ukrainische Militär bereitgestellt wird /REU22w02/. Am 15.03.2022 sprach der stellvertretende Leiter der ukrainischen Behörde für Sonderkommunikation und Informationsschutz, Victor Zhora, in diesem Zusammenhang von einen „sehr großen Verlust an Kommunikation gleich zu Beginn des Krieges". /REU22w03/

Da Viasat KA-SAT erst 2021 erworben hat, war dessen Netzwerk zum Zeitpunkt der Störung noch nicht in das Netzwerk von Viasat integriert, sondern operierte nach Aussage von Viasat in einem Stand-Alone-Netzwerk. Daher waren die vier anderen von Viasat betriebenen Satelliten von der Störung nicht betroffen. /SAN22w01/

Die betroffenen ISPs gaben in eigenen – von Seiten des Betreibers unbestätigten – Meldungen bereits frühzeitig erste Informationen zu einer möglichen Ursache bekannt. So berichtete intv.cz von einem nicht näher spezifizierten Angriff auf die Bodeninfrastruktur von KA-SAT während EUSANET angab, derzeit noch keine Ursachen zu kennen, aber einen zeitlichen Zusammenhang mit dem Ereignissen in der Ukraine herstellte. /HEI22w01/, /PAX22w01/ Der Betreiber Viasat beauftragte ein externes Cybersicherheitsunternehmen mit der Untersuchung und gab frühzeitig an „die Untersuchung des

Ausfalls dauert noch an, aber bislang halten wir einen Cyberevent für die Ursache“ /REU22w01/. Der britische Nachrichtensender Sky News stellte unter Berufung auf einen Insider eine Verbindung zwischen dem teilweisen Ausfall von KA-SAT und den DDoS-Angriffen her, die kurz vor Beginn der russischen Invasion auch eine Reihe von Webseiten von Banken und Regierungseinrichtungen lahmlegte /SKY22w01/. Sky News berichtete darüber hinaus, dass bei der Ursachenklärung auch eine russische Beteiligung untersucht werde /SKY22w01/. Das französische Verteidigungsministerium bestätigte schließlich am 3.3.2022, dass der Ausfall von KA-SAT auf einen Cyberangriff zurückgeht /NUM22w01/. Kurz darauf erfolgte auch die Bestätigung von Viasat, dass der Ausfall von KA-SAT auf einen vorsätzlichen Cyberangriff zurückgeht.

Die derzeit öffentlich verfügbaren Informationen legen nahe, dass der Angriff zunächst den KA-SAT SATCOM Terminals (Terminals bestehen aus Antenne und Modem) in der Ukraine galt, sich der Angriff aber schnell in andere Länder ausbreitete. Konkret genannt werden neben der Ukraine, Deutschland, Tschechien und Frankreich auch Griechenland, Polen, Italien und Ungarn. Auch mehren sich die Aussagen dazu, dass eine große Anzahl Terminals nachhaltig beschädigt wurden /HEI22w01/. So berichtet beispielsweise das BSI in seinem Tageslagebericht vom 02.03.2022 von einer Meldung eines Providers, der von der KA-SAT-Störung betroffen ist.

Dieser Provider berichtet nach Angaben des BSI, „dass bei allen aktiven Consumer-Modems ein Update durchgeführt wurde, welches die Modems nachhaltig zerstöre.“ /BSI22r03/

Der Angriff stellt sich auf Basis der aktuell verfügbaren Informationen wie folgt dar:

Viasat selbst beschreibt den Angriff als mehrstufig. Zunächst erfolgte ein DoS-Angriff, der von mehreren SurfBeam2 Modems und anderem in der Ukraine befindlichen Equipment ausging. Aufgrund dieses DoS-Angriffs gingen viele KA-Sat Modems zeitweise offline. Anschließend war zu beobachten, wie zahlreiche Modems nach und nach ihre Verbindung verloren. Die Angreifer erlangten über die Fehlkonfiguration einer VPN Anwendung Zugriff auf das sogenannte Trusted Management Segment des KA-Sat-Netzwerks. Anschließend erfolgte eine laterale Bewegung des Angreifers durch dieses Segment zu einem Segment, das für Management und Betrieb des Netzwerks verwendet wird. Von diesem Segment aus führten die Angreifer zeitgleich bei einer großen Anzahl Modems gezielte Befehle zum Netzwerkmanagement aus. Unter Anwendung von legitimen Befehlen zum Netzwerkmanagement führten die Angreifer eine

ausführbare Schadsoftware auf den Modems aus. Dabei handelte es sich um einen Wiper namens „AcidRain“, der wesentlichen Daten im Flash-Speicher der Modems überschrieb, so dass diese nicht mehr betrieben werden konnten. Eine Wiederherstellung war nur noch durch Reflashing beim Hersteller möglich. /SEN22w02/

Zunächst empfahl Viasat allen Kunden, bei offline befindlichen Modems keinen Versuch der Verbindungsherstellung zu unternehmen, um Schäden von diesen abzuwenden. Ab dem 10.03.2022 konnten Modems laut Viasat wieder in Betrieb genommen werden. Gleichzeitig wurde bekannt gegeben, dass dabei „durch den Angriff in Mitleidenschaft gezogene Modems ersetzt“ werden müssten. Viasat gab an, etwa 30.000 neue Modems an Kunden ausgeliefert zu haben, um eine Wiederherstellung der Dienste zu beschleunigen. Durch den notwendigen Austausch zog sich die Wiederherstellung über Wochen hin. So gab beispielsweise der deutsche Windkraftanlagenhersteller ENERCON am 15.03.2022 bekannt, dass noch 85 % seiner Modems offline seien und die vollständige Wiederherstellung wohl noch Wochen dauern könne /REU22w03/. Am 19.04.2022 gab ENERCON bekannt, dass 95 % der betroffenen Anlagen wieder in die Fernwartung und -überwachung eingebunden seien.

Kerntechnischer Bezug

Satelliten-basierte Kommunikation wird auch in deutschen Kernkraftwerken und anderen kerntechnischen Anlagen eingesetzt, beispielsweise als diversitäre Kommunikationsmöglichkeit im Krisenfall, beispielsweise für die Polizeidirektverbindung. Bislang ist der GRS aus keiner deutschen kerntechnischen Anlage der Einsatz von KA-SAT bekannt. Grundsätzlich ist der Ablauf des Angriffs allerdings auch auf andere Kommunikationssatelliten, wie sie auch in deutschen Kernkraftwerken eingesetzt werden, möglich. Der Einsatz einer vergleichbaren Wiper-Schadsoftware könnte auch Modems anderer Anbieter, unabhängig vom genutzten Kommunikationssatelliten, in ihrer Funktionalität nachhaltig beeinträchtigen. Aus Sicht der GRS besteht eine Relevanz für deutsche kerntechnische Anlagen und Einrichtungen. Daher wurde der Sachverhalt von der GRS bereits im Rahmen einer Ersteinschätzung ausgewertet, eine Stellungnahme wird derzeit erstellt.

B.14.3 Killnet – IT-Angriffe auf Webseiten von Regierungseinrichtungen

B.14.4 IT-Angriff auf Rosneft

Übersicht

Am 11.03.2022 wurde festgestellt, dass es zu einem IT-Angriff auf die deutsche Niederlassung des russischen Ölproduzenten Rosneft gekommen ist. Rosneft ist Russlands größter Ölproduzent und in den vergangenen Jahren für ein Viertel aller Rohölimporte nach Deutschland zuständig und damit ein Unternehmen der kritischen Infrastruktur. Aufgrund des Angriffs wurden vorsorglich alle IT-Systeme heruntergefahren und der E-Mail-Verkehr unterbrochen, der operative Betrieb wurde laut Rosneft Deutschland nicht beeinträchtigt. /HEI22w09/, /SEC22w05/, /HAN22w01/

Beschreibung

Die Rosneft Deutschland GmbH wurde im März 2022 Opfer eines IT-Angriffs, zu dem sich das Hackerkollektiv Anonymus bekannt hat. Nach Angaben von Anonymus konnte sich über zwei Wochen hinweg kontinuierlich und ohne Pause in den Systemen der Rosneft Deutschland GmbH bewegt und Daten kopiert werden. Nachdem der Angriff erkannt wurde, wurden aus Sicherheitsgründen alle IT-Systeme heruntergefahren und der E-Mail-Verkehr unterbrochen. Durch den Angriff wurden verschiedene Prozesse gestört, u. a. die Möglichkeit, Verträge abzuschließen. Trotzdem die IT-Systeme erheblich betroffen waren, wurde das operative Geschäft und der Betrieb von Pipelines und Raffinerien durch den Angriff laut Rosneft Deutschland nicht eingeschränkt; auch hatte der Angriff keine Auswirkungen auf die Versorgungslage. Um die Ursachen des Angriffs zu klären, wurde ein externer IT-Dienstleister hinzugezogen. /HEI22w09/, /SEC22w05/, /HAN22w01/, /SPI22w01/

Bei dem Angriff wurden insgesamt ca. 20 Terabyte an Daten gestohlen, u. a. Festplattenimages von Mitarbeiterrechnern und eines Mailservers, Backups der Laptops von Führungskräften des Unternehmens, Archiv-Dateien, Software-Pakete, Anleitungen und Lizenz-Schlüssel für Software. Außerdem wurden Inhalte Dutzender Geräte gelöscht. Laut Anonymus war man ca. 2 Wochen lang unbemerkt im System der Rosneft Deutschland GmbH und hatte Zugriff auf diverse Dateien in Backup-Ordnern, weiteren Ordnern

mit Dokumenten sowie iPhones und iPads der Mitarbeiter. Anonymus hatte nach eigenen Angaben zu keinem Zeitpunkt Zugriff auf kritische Systemteile oder Steuerungsanlagen, wobei daran laut Anonymus auch kein Interesse bestand. Laut Anonymus wurde bewusst keine kritische Infrastruktur gefährdet und es wurden keine Steuerungssysteme in Mitleidenschaft gezogen. Eine Veröffentlichung der gestohlenen Daten ist laut Anonymus nicht geplant. /HEI22w09/, /SEC22w05/, /SEC22w06/, /SPI22w01/

Laut Anonymus gelang der Zugriff auf die Systeme der Rosneft Deutschland GmbH über die Steuerung und Verwaltung von Druckern, indem Service Accounts von Druckern im Active Directory kompromittiert wurden. Bei dem Angriff konnte weit in interne Systeme vorgedrungen werden und es ist laut Anonymus gelungen, Administratorrechte zu erlangen. Das Kopieren der Daten erfolgte dann über eine einfache FTP-Verbindung. Das Löschen der Inhalte Dutzender Geräte erfolgte dank eines erratenen Security Pins („1234“). /HAN22w01/, /SEC22w05/, /SPI22w01/

Anonymus ist ein Hackerkollektiv, welches vermutlich nicht besonders straff organisiert ist. Es gibt keinen eng umrissenen Mitgliederkreis, jeder kann sich zum Aktivisten erklären. Nach dem Angriff Russlands auf die Ukraine im Februar 2022 hat Anonymus der russischen Regierung offiziell den Cyberkrieg erklärt. Laut Anonymus wurden bereits diverse IT-Angriffe auf russische Einrichtungen durchgeführt, Opfer waren u. a. der Kreml, das Verteidigungsministerium, das Unterhaus der Duma, diverse russische Webseiten, russische Banken und russische TV-Sender. Auch Rosneft wurde bereits früher von Anonymus angegriffen, Ende Februar 2022 wurde beispielsweise die Webseite von Rosneft International durch einen DDos-Angriff blockiert. /SEC22w05/, /SEC22w06/, /SEC22w07/, /HAN22w01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.5 Industroyer-2 – IT-Angriff auf die ukrainische Energieversorgung

Übersicht

Am 12.04.2022 informierten das CERT-UA und die IT-Sicherheitsfirma ESET über einen IT-Angriff auf das ukrainische Stromnetz vom 08.04.2022, bei dem die Schadsoftware Industroyer2 eingesetzt wurde. Der Angriff wurde rechtzeitig entdeckt und Schäden konnten verhindert werden.

Beschreibung

Am 24.02.2022 begann die Invasion der Ukraine durch Russland. Parallel zu den physischen Kampfhandlungen werden auch IT-Angriffe gegen die Ukraine durchgeführt. Am 08.04.2022 sollte durch den Einsatz der Schadsoftware Industroyer2 ein Blackout im ukrainischen Stromnetz hervorgerufen werden. Der Angriff wurde nach ukrainischen Informationen rechtzeitig erkannt und Schäden konnten verhindert werden. Die Schadsoftwarekomponente Industroyer2 basiert auf der Schadsoftware Industroyer/Crashoverride, die 2016 bei einem IT-Angriff gegen das ukrainische Stromnetz eingesetzt wurde, ist aber im Gegensatz zu dieser nicht modular aufgebaut, sondern hart codiert und deutlich schlichter konzipiert.

Während Industroyer die Industrieprotokolle IEC-101, IEC-104, IEC-61850 und OPC DA verwendete, nutzt Industroyer2 ausschließlich das Protokoll IEC-104, um mit industriellen Steuerungssystemen (Industrial Control System, ICS) zu kommunizieren. Dieses Protokoll wird allgemein für die Überwachung und Steuerung von Energienetzen verwendet. Jedes System, in dem das Protokoll IEC-104 zum Einsatz kommt, ist prinzipiell durch die in der Schadsoftware Industroyer2 beinhalteten Methoden und Werkzeuge angreifbar. /BSI22i03/, /BSI22i04/, /ESE22w01/, /HIT22i01/, /MAN22w02/

Eigentliches Ziel des Angriffs war die Sabotage der industriellen Steuerungssysteme in den Hochspannungsumspannwerken, um einen Blackout hervorzurufen. Etwa zwei Millionen Menschen wären in der Ukraine von dem Blackout betroffen gewesen. Der IT-Angriff wird der APT-Gruppierung Sandworm zugeschrieben, welche dem russischen Nachrichtendienst GRU zugeordnet wird. Die Angreifer besitzen weitreichende Kenntnisse bezüglich des Protokolls IEC-104 und des kompromittierten Netzwerks einschließlich IP-Adressen und der Konfiguration des ICS-Netzwerks.

Dass Industroyer2 hart codiert ist spricht dafür, dass die Schadsoftware für den Einsatz in verschiedenen Umgebungen speziell angepasst und jeweils neu kompiliert werden muss. Auf der anderen Seite erschwert dies die Detektion der Schadsoftware, da die Hashes für die Schadsoftware als Indicator of Compromise (IoC) angriffsspezifisch sind. Darüber hinaus verwendet Industroyer2 nur eine geringe Anzahl von Methoden, um die Detektion der Schadsoftware zu erschweren. Dies lässt vermuten, dass die IT-Angreifer über die Sicherheitsmaßnahmen im kompromittierten Netzwerk Bescheid wussten. /BBC22w01/, /BSI22i03/, /ESE22w01/, /HIT22i01/, /MAN22w02/, /NOZ22w01/, /WAT22w01/

Im Zuge des Angriffs wurden zusätzlich Wiper für Windows-, Linux- und Solaris-Betriebssysteme eingesetzt, um Daten zu löschen. Eines der IT-Angriffswerkzeuge, CaddyWiper, löscht Benutzerdaten und Partitionsinformationen von Laufwerken auf Windows- Systemen, indem es diese mit Nullen überschreibt. Auf diese Weise sind die Systeme nicht wiederherstellbar. Die anderen eingesetzten Wiper Orcshred, Soloshred und Awfulshred sollen Schäden an Linux- und Solaris-Servern verursachen. /ESE22w01/, /WAT22w01/

Kerntechnischer Bezug

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

B.14.6 Khouzestan Steel Co. – IT-Angriff auf iranisches Stahlwerk

Übersicht

Die Hackergruppierung Predatory Sparrow gab am 27.06.2022 bekannt, einen IT-Angriff auf die drei größten Stahlwerke des Iran durchgeführt zu haben. Hierzu veröffentlichten sie auch ein Video einer Überwachungskamera aus dem iranischen Stahlwerk Khouzestan Steel Company. Darauf ist zu sehen, wie die Komponenten einer Produktionslinie zunächst noch wie vorgesehen funktionieren, dann Fehlfunktionen auftreten und schließlich ein massives Feuer ausbricht.

Beschreibung

Im Iran ist es parallel zu den wachsenden Spannungen in der Region in den letzten Monaten immer wieder zu IT-Angriffen gekommen. Für einige davon hat die Hackergruppierung Predatory Sparrow (Gonjeshke Darande) die Verantwortung übernommen. Hierzu zählen Angriffe auf die iranische Eisenbahn, den iranischen Rundfunk, zahlreiche Überwachungskameras und iranische Tankstellen /BBC22w01/. Während zwei der am 27.06.2022 angegriffenen Stahlwerke zwar einen IT-Angriff einräumten, aber keine Angaben zu physischen Schäden machten, gab Khouzestan Steel Co. an, aufgrund technischer Probleme wegen eines Cyberangriffs die Produktion bis auf weiteres einzustellen.

Iran ist einer der Hauptproduzenten für Stahl weltweit und führend im Mittleren Osten. Die drei angegriffenen Firmen haben zusammen das Monopol auf Stahlproduktion im Iran. In dem von Predatory Sparrow veröffentlichten Video ist zunächst der normale Ablauf der Produktion zu sehen. Zudem ist sichtbar, wie das Personal nach und nach das Umfeld der Maschinen verlässt. Anschließend kommt es zu Störungen des Produktionsablaufes bis hin zu einem Feuer. Das Video endet mit Beginn der Löscharbeiten. In den Tagen nach der Veröffentlichung dieses Videos sind weitere Videos aus der Anlage auf-getaucht, die dieselbe Szene aus teils anderen Blickwinkeln zeigen. Darin sind Rufe der Arbeiter nach der Feuerwehr sowie Ausrufe zu Schäden an Komponenten zu hören.

Davon ausgehend, dass es sich bei dem veröffentlichten Bildmaterial um authentisches Bildmaterial handelt, stellt sich der Angriff wie folgt dar: Zum einen müssen die Angreifer Zugriff auf die Überwachungskameras gehabt haben. Zum anderen müssen sie es geschafft haben, sich von außen in die industriellen Steuerungssysteme der betroffenen Produktionslinie einzuhacken. Predatory Sparrow gibt an, mit dem Beginn des Angriffs auf einen Moment gewartet zu haben, zu dem sich keine Arbeiter in der Nähe befunden haben. Dies ist nur mit direktem, unverzögertem Zugriff auf die betroffenen Systeme möglich.

Über den tatsächlichen Angriffsvektor ist derzeit nichts bekannt.

Aufgrund ihrer Vorgehensweise sowie der Komplexität und Auswirkung ihrer Angriffe wird vermutet, dass es sich bei Predatory Sparrow entgegen deren eigenen Angaben nicht um eine Hackergruppierung, sondern vielmehr um eine hochentwickeltem staatlich geförderte Angreifergruppierung handelt.

Kerntechnischer Bezug

Zunächst hat dieser IT-Sicherheitsvorfall keinen kerntechnischen Bezug. Da bislang aber keine Informationen über den Angriffsvektor oder über die angegriffenen industriellen Steuerungssysteme vorliegen, kann eine Übertragbarkeit derzeit nicht eingeschätzt werden.

B.14.7 LockBit – IT-Angriff auf Top Aces

Übersicht

Laut /FBI22r01/, /KAS22w02/ ist LockBit eine Ransomware-Gruppierung, deren erste Angriffe im September 2019 bekannt geworden sind. Zu diesem Zeitpunkt wurde die Gruppierung noch ABCD genannt, da diese Dateierweiterung bei verschlüsselten Daten verwendet wurde. Bei LockBit handelt es sich um eine Ransomware-as-a-Service-Gruppierung, die laut /REC22w01/ eine der produktivsten aktiven Gruppierungen ist und im Jahr 2022 bereits mindestens 650 Organisationen angegriffen hat (Stand: Ende Juni 2022). Die Gruppierung führt zielgerichtete Angriffe auf Unternehmen und Regierungsorganisationen aus, Privatpersonen sind eher keine Angriffsziele. Es werden Unternehmen weltweit angegriffen, wobei bewusst Unternehmen mit Standort in Russland gemieden werden. Die Schadsoftware von LockBit ist dabei darauf ausgelegt, den Zugriff zum angegriffenen System zu sperren, Daten zu verschlüsseln und damit eine Lösegeldzahlung zu erzwingen.

Beschreibung

Laut /BSI22r11/, /REC22w01/ kam es im Mai 2022 zu einem IT-Angriff von LockBit auf Top Aces, einem kanadischen Verteidigungsunternehmen und damit einem Unternehmen einer kritischen Infrastruktur. Top Aces bietet luftgestütztes Training für Luftwaffenverbände weltweit an und ist exklusiver Anbieter gegnerischer Flugziele bei Übungen der kanadischen und deutschen Streitkräfte. Neben diversen Ländern weltweit hat Top Aces auch einen Vertrag mit den USA, in dem ausdrücklich die Bereitstellung von Werkzeugen zur Verteidigung gegen russische Waffen erwähnt wird. Bei dem Ransomware-Angriff von LockBit auf Top Aces wurden 44 GB an Daten gestohlen, die am 16.05.2022 bei Nichtzahlung eines Lösegeldes unbekannter Höhe veröffentlicht werden sollten. Da das Lösegeld nicht gezahlt wurde, erfolgte eine Veröffentlichung der Daten,

wobei am 18.05.2022 nur Fragmente der Daten öffentlich zu finden waren. Ob der komplette gestohlene Datensatz veröffentlich wurde, ist nicht bekannt.

Die Ransomware-Angriffe von LockBit laufen laut /KAS22w02/ folgendermaßen ab: In der ersten Angriffsphase wird versucht, Schwachstellen in Unternehmensnetzwerken auszunutzen. Dabei wird gezielt nach attraktiven Zielen gesucht, es werden also keine breit gestreuten Angriffe ausgeführt. Um Zugang zu einem Unternehmensnetzwerk zu erhalten, werden dann Social-Engineering-Techniken angewendet oder es wird versucht, gewaltsam in das Netzwerk einzudringen. In der darauffolgenden Angriffsphase wird die Angriffsstruktur vervollständigt. Ab diesem Zeitpunkt sind keine manuellen Aktionen mehr notwendig, die Ransomware führt alle Aktionen automatisiert aus. Die Lock-Bit-Ransomware ist dabei so programmiert, dass sie von speziell entwickelten automatisierten Prozessen gelenkt wird und hebt sich damit von anderen Ransomware-Versionen ab, bei denen die Ransomware-Gruppierungen mitunter wochen- oder monatelang in Netzwerken verharren, um Aufklärungs- und Überwachungsarbeit durchzuführen. Nach der manuellen Erstinfektion wird automatisch nach anderen zugänglichen Systemen gesucht. Zur Verbreitung der Ransomware werden dann Tools wie Windows PowerShell oder Server Message Block (SMB) genutzt. Des Weiteren werden Tools genutzt, um sich Berechtigungen zu verschaffen und diese weiter zu eskalieren. Die verwendeten Tools werden dabei in Mustern genutzt, die in nahezu allen Windows-Systemen nativ vorzufinden und damit schwer aufzudecken sind. In dieser Phase werden auch Sicherheitsprogramme ausgeschaltet, über die das System wiederhergestellt werden könnte. In der letzten Angriffsphase beginnt die Ransomware, sich über das infiltrierte Netzwerk auszubreiten.

Dazu genügt ein einziges System mit hoher Zugangsberechtigung, um andere Systeme im Netzwerk ebenfalls zu infizieren. Alle Daten werden verschlüsselt, was nur durch einen speziellen Schlüssel rückgängig gemacht werden kann.

Zu Beginn des Auftretens von LockBit erfolgten ausschließlich Verschlüsselungen von Windows-Systemen, wobei die automatische Verschlüsselung über Active-Directory-Gruppenrichtlinien erfolgte. Im Januar 2022 wurde bekannt, dass LockBit auch eine Verschlüsselungssoftware für VMWare ESXi-Linux-Server in sein Toolkit aufgenommen hat. Außerdem versucht LockBit aktiv Innentäter zu rekrutieren, indem Gewinnbeteiligungen an möglichen erpressten Lösegeldern versprochen werden. Die Innentäter sollen über Virtual Private Network (VPN) oder Remote Desktop Protocol (RDP) Zugang zu Unternehmensnetzwerken gewähren. /BLE22w05/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.8 Conti – IT-Angriff auf Regierungsstellen Costa Ricas

Übersicht

Im April 2022 wurden mehrere Regierungsstellen Costa Ricas laut /BSI22r04/ Opfer der Ransomware-Gruppe Conti. Von den Angriffen waren Finanz-, Zoll- und Steuerbehörden, das Ministerium für Arbeit und Soziales sowie eine Universität betroffen. Durch die Angriffe wurden bedeutende Teile von Behörden und Regierungsstellen lahmgelegt, aufgrund dessen wurde in Costa Rica der nationale Cyber-Notstand ausgerufen. /BSI22r04/, /HEI22w05/ Bisher wurden laut /BSI22r04/ keine derart umfangreichen IT-Angriffe auf staatliche Einrichtungen mit Ransomware beobachtet, laut /WIR22w01/ war es sogar das erste Mal, dass eine Ransomware-Gruppe explizit die Regierung eines Landes angegriffen hat. Die Angriffe erfolgten durch Conti, eine pro-russische Ransomware-as-a-Service-Gruppierung, die Verbindungen zur russischsprachigen Gruppe Wizard Spider hat und unter anderem für Angriffe auf HSE in Irland (siehe Abschnitt B.13.11) und Angriffe auf US-amerikanische Unternehmen des Gesundheitswesens und der Rettungsdienste verantwortlich ist. /BLE22w01/

Beschreibung

Laut /WIR22w01/ erfolgten die ersten Angriffe von Mitte April bis Anfang Mai 2022, wobei insgesamt 27 Regierungsstellen betroffen waren. Am 18. April 2022 wurden als erstes Dateien des Finanzministeriums verschlüsselt, in den darauffolgenden Tagen bis zum 02. Mai 2022 wurde nahezu täglich versucht, in verschiedene weitere lokale Behörden sowie zentrale Regierungsorganisationen einzudringen. Digitale Dienste des Finanzministeriums waren daraufhin seit dem 18.04.2022 nicht mehr verfügbar, wodurch der gesamte „produktive“ Sektor des Landes beeinflusst wurde, da staatliche Verfahren zur Vergabe von Unterschriften, Stempeln, etc. nicht mehr ausgeführt werden konnten. /BLE22w01/ Ein zweiter Angriff Ende Mai 2022, der von der Gruppierung HIVE, welche Verbindungen zu Conti haben soll, ausgeführt, betraf Systeme des Sozialversi-cherungsfonds Costa Ricas, durch den auch die Gesundheitsversorgung organisiert wird, womit also auch das Gesundheitssystem Costa Ricas getroffen wurde. /WIR22w01/

Durch diese beiden IT-Angriffe wurden laut /WIR22w01/ viele wichtige Dienste von Costa Rica lahmgelegt, wodurch der internationale Handel Costa Ricas zum Erliegen kam. Die Ein- und Ausfuhren des Landes mussten ausgesetzt werden, was große Auswirkungen auf den Handel hatte. /WIR22w01/ Insgesamt wurden mehr als 30.000 Arzttermine verschoben und es kam zum Ausfall von Millionenbeträgen.

Laut /BSI22r04/, /HEI22w05/, /BLE22w01/ wurden bei dem IT-Angriff Daten gestohlen und verschlüsselt. Zur Freigabe der Daten wurde ein Lösegeld in Höhe von 10 Millionen US-Dollar gefordert, welches aber nicht gezahlt wurde. Daraufhin wurden 97 % der gestohlenen 672 GB an Daten auf der Webseite von Conti veröffentlicht. Die Drohungen gegen Costa Rica wurden von Seiten Contis verschärft und die Summe des verlangten Lösegeldes wurde auf 20 Millionen US-Dollar erhöht. /WIR22w01/, /HEI22w06/

Die genaue Motivation hinter dem Angriff ist unklar. Es könnte sich laut /BSI22r04/ um einen Testlauf gehandelt haben, der gegen Costa Rica gerichtet war, um ein Exempel zu statuieren. Aber auch ein zufälliger Angriff auf eine Einrichtung und eine von dort erfolgte Kompromittierung weiterer Einrichtungen aufgrund von bei dem Erstangriff aufgedeckten Möglichkeiten ist denkbar. Laut /WIR22w01/ führte Conti zur gleichen Zeit, zu der die Angriffe auf Costa Rica ausgeführt wurden, auch Angriffe auf das Finanzministerium und den Geheimdienst Perus durch, wobei über Schäden oder Auswirkungen dieser IT-Angriffe nichts bekannt geworden ist.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.9 IT-Angriff auf israelische Regierungswebseiten

Übersicht

Laut /HEI22w08/, /IND22w02/, /REG22w02/ kam es am 14.03.2022 zu einem IT-Angriff auf den nationalen israelischen Kommunikationsdienstleister Cellcom. Bei dem Angriff handelte es sich um einen DDoS-Angriff (Distributed-Denial-of-Service-Angriff), infolgedessen diverse Internetseiten der israelischen Regierung nicht mehr zu erreichen waren.

Beschreibung

Der nationale israelische Kommunikationsdienstleister Cellcom wurde Opfer eines DDoS-Angriffs, der zu einer Unterbrechung der Dienste auf verschiedenen Regierungswebseiten führte. Betroffen waren dabei alle Seiten unter der Domain „gov.il“, wobei insbesondere Webseiten des Gesundheits-, Innen-, Justiz- und Sozialministeriums betroffen waren. /REG22w02/, /HEI22w08/, /MAL22w02/

Für den Angriff auf die israelischen Regierungswebseiten ist laut /REG22w02/ ein nationalstaatlicher Akteur oder eine große Organisation verantwortlich, wobei nicht geklärt ist, welche Gruppierung den Angriff begangen hat. Laut /MAL22w02/ ist möglicherweise eine iranische Gruppierung für den Angriff verantwortlich.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.10 IT-Angriffe mit Bumblebee

Übersicht

Seit März 2022 wird vermehrt ein neuer Schadsoftwareloader mit dem Namen Bumblebee durch Sicherheitsforscher beobachtet.

Schadsoftwareloader dienen als erste Stufe von Schadsoftwareangriffen, sie öffnen für die Angreifer einen Zugang zum betroffenen IT-System, stellen die Verbindung mit den Befehlsstrukturen (Command & Control Server) her, führen das Nachladen von weiterer Schadsoftware aus und können zur Verbreitung innerhalb des angegriffenen

Netzwerkes beitragen. Bumblebee hat nach bisherigen Angaben von Sicherheitsforschern eine Reihe früherer genutzter Schadsoftwareloader verdrängt und wird insbesondere von verschiedenen Ransomware-Gruppen als erste Stufe eines IT-Angriffes eingesetzt. /BLC22r01/, /MED22r01/

Beschreibung

Moderne Schadsoftwares sind zumeist modular aufgebaut, wobei bestimmte Aufgaben von verschiedenen Schadsoftwares übernommen werden. So übernimmt ein Modul die Ausbreitung innerhalb eines Netzwerkes, ein anderes Modul die Ausspähung von wichtigen Daten auf betroffenen Systemen, ein weiteres Modul führt die Verschlüsselung aus und schließlich übernehmen Loader die Aufgabe der erstmaligen Infektion. Die Ansprüche an Schadsoftwareloader sind mit steigenden Sicherungsmaßnahmen stetig gewachsen. Ein und derselbe Schadsoftwareloader wird zum Teil zur Verbreitung von völlig unterschiedlichen Schadsoftwares, z. B. Ransomware oder Bankingtrojaner eingesetzt, die Loader werden von den Entwicklern verkauft, vermietet oder zur freien Benutzung bereitgestellt. Seit März 2022 ist mit dem Bumblebee-Loader ein neuartiger hochmoderner Schadsoftwareloader entdeckt worden. Ransomwaregruppen wie Conti, Quantum und Mountlocker haben in den Monaten April bis Juni 2022 ihre bisherigen Loader wie BazarLoader oder Trickbot durch Bumblebee ersetzt. Hierdurch erhoffen sich diese Gruppen vermutlich eine höhere Erfolgsquote in der Verbreitung ihrer Schadsoftware. /BLC22r01/, /MED22r01/

Der Bumblebee-Loader wird in den meisten Fällen per E-Mail verteilt u. a. über Archive, dem CD-Abbildformat ISO und manipulierte HTML-Dateien. Diese Dateien sind entweder direkt an die Emails angehangen oder aber als Link z. B. zu Cloud Speichermedien in Emails verknüpft. Werden die entsprechend verteilten Dateien ausgeführt, wird die Bumblebee-DLL ausgeführt und die Infektion des ausführenden IT-Systems startet. Bumblebee verbindet sich mit einer Command & Control Infrastruktur und führt anschließend alle 15 Minuten ein VBS Script aus.

Mit zeitlichem Abstand wird die zweite Stufe des IT-Angriffs, eine von Bumblebee unabhängige Schadsoftware wie die Ransomware Software Quantum heruntergeladen, mit welcher die Dateien des betroffenen IT-Systems verschlüsselt werden und die weitere Ausbreitung der Infektion durchgeführt werden kann. /MED22r01/

Die Besonderheiten des Bumblebee-Loaders sind seine komplexen Fähigkeiten zur Verschleierung der eigenen Entdeckung, der Entdeckung möglicher Virtualisierungsbemühungen von Schutzprogrammen und die Eskalation der Rechte des Loaders zur Ausführung beliebigen Codes. Bumblebee nutzt eine bisher nicht bekannte Routine, um seinen Code erstmalig auszuführen, wozu Bumblebee den Zugriff auf den Speicher des Systems nutzt, eine fiktive DLL Datei lädt und den Ladevorgang dieser DLL Datei zum Ausführen seines Codes nutzt. Bumblebee sucht bei jeder Ausführung nach bestimmten Prozessen, die auf Virenscanner, andere Schutzfunktionen oder Virtualisierungssoftware hinweisen. Die Anzahl der gesuchten Prozesse hat in den Monaten seit Erscheinen im März 2022 stetig zugenommen, was auf eine konsequente Weiterentwicklung des Bumblebee-Loaders hindeutet. Der Bumblebee-Loader zeigt damit die konsequente innovative Weiterentwicklung von Schadsoftware auf und ist daher von Sicherheitsforschern intensiv analysiert worden. /BLC22r01/, /MED22r01/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor

B.14.11 IT-Angriff auf Dienstleister von Okta

Übersicht

Im März 2022 veröffentlichte die Angreifergruppierung „Lapsus$“ Informationen zu Kundenaccounts des amerikanischen Unternehmens „Okta“, welches Cloud-Produkte für Identitäts- und Zugriffsmanagement anbietet. Okta bestätigte am 22. März, dass das Unternehmen Hinweisen auf einen IT-Angriff in der Zeit vom 16. bis zum 21. Januar 2022 über einen Dienstleister nachgeht. Die Angreifer erlangten ihren Zugriff mutmaßlich über den Laptop eines Unterauftragnehmers. /CNN22w01/

Beschreibung

Durch eine forensische Untersuchung eines im Januar 2022 registrierten IT-Sicherheitsvorfalls erkannte das Unternehmen Okta, dass sich die Angreifergruppierung „Lapsus$“ für einen Zeitraum von fünf Tagen Zugang zu einem Laptop eines Support-Ingenieurs der Firma Sitel verschafft hat. Das Unternehmen bietet für seine Kunden unter anderem technischen Support als Dienstleistung an. Okta grenzte den potenziellen Zugriff der Angreifer zunächst auf 2,5 % des Kundenstamms ein, was auf Grundlage der veröffentlichten Quartalszahlen etwa 366 Kunden betreffen würde. Im April 2022 veröffentlichte Okta die finale forensische Analyse des IT-Sicherheitsvorfalls. Demnach wurde festgestellt, dass sich die Angreifer für eine Zeitspanne von 25 Minuten Zugang zum Laptop des Support-Ingenieurs verschafft haben und nur zwei Kunden betroffen waren. Die Angreifer hatten Zugriff auf die Software SuperUser, die für grundsätzliche Managementfunktionen genutzt wird. Außerdem hatten die Angreifer limitierten Zugriff auf Informationen in anderen Programmen wie „Slack“ oder „Jira“, die nicht für Aktionen im Rahmen Oktas Software verwendet werden können. Nach Angaben von Okta konnten die Angreifer weder Änderungen an Konfigurationen durchführen noch eine Multi-Faktor-Authentifizierung bzw. Passwörter zurücksetzen oder sich in irgendeiner Form direkt gegenüber Okta-Accounts authentifizieren.

Der Grad der Kompromittierung ist gemäß Okta signifikant kleiner als ursprünglich befürchtet, wobei dennoch auf die Kritikalität eines solchen Vorfalls hingewiesen wurde. Okta beschreibt in diesem Zusammenhang mehrere Bereiche, in denen das Unternehmen angesichts des IT-Sicherheitsvorfalls Verbesserungspotenzial sieht. Dabei geht es unter anderem um das Thema Third-Party-Riskmanagement, welches angesichts vermehrter IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette von IT-Systemen von großer Bedeutung ist. /BSI22r16/, /OKT22w01/, /OKT22w02/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.14.12 IT-Angriffe im Jahr 2021/2022 auf den VPN Client Pulse Connect Secure

Übersicht

Bei Pulse Connect Secure handelt es sich um eine als besonders sicher beworbene VPN-Softwarelösung, welche an Geschäftskunden vertrieben wird und von Pulse Secure, einem Tochterunternehmen von Ivanti betrieben wird. Vormals als Juniper SSL VPN bekannt, wird Pulse Connect Secure insbesondere mit seinen Sicherheitsfeatures beworben, wozu unter anderem die Nutzung von Secure Sockets Layer (SSL) gehört, welches ein Netzwerkprotokoll für die sichere Übertragung von Daten ist. Weiterhin verfügt der Pulse Connect Secure VPN gemäß Anbieter über verschiedene Verifizierungsmaßnahmen für den sicheren Zugriff und eine Ende-zu-Ende-Sicherheitsfunktion, welche die Nutzung von Sicherungsmaßnahmen auf den Endgeräten prüft. Am 23.04.2021 wurde die kritische Schwachstelle CVE-2021-22893 der Pulse Connect Secure Software bekannt. /PUL22w01/, /FOR20w02/

Beschreibung

Pulse Connect Secure gilt als sichere VPN-Anwendung zur Anbindung von Fernzugriffen, Unternehmensnetzwerken und ähnlichen über räumliche Distanzen und ist in Unternehmen und Behörden im westlichen Raum weit verbreitet. Insbesondere durch die Pandemie 2020/2021 kam es zu einer weiten Verbreitung von Anwendungen für Fernzugriffe in Unternehmen und Behörden, um das isolierte mobile Arbeiten zu ermöglichen. So stieg Pulse Connects Umsatz im ersten Quartal 2020 um 300 %, insbesondere auch weil Pulse Connect durch den Einsatz von Verschlüsselungstechnologien und Authentifizierungstechnologien als sicher beworben wird. /PUL22w01/, /FOR20w02/

Am 23.04.2021 wurde die Schwachstelle CVE-2021-22893 für Pulse Connect Secure bekannt, wobei erstmalig am 20.04.2021 vom IT-Sicherheitsdienstleister Mandiant bezüglich laufender IT-Angriffe berichtet wurde. Für die sogenannte Zero-Day Schwachstelle stand zu diesem Zeitpunkt kein Sicherheitsupdate zur Verfügung, während IT-Angreifer die Schwachstelle bereits vor der Bekanntwerdung ausnutzten. Zu den Opfern zählen gemäß AP der Telekommunikationskonzern Verizon, die kalifornische Wasserbehörde, die New Yorker U-Bahn sowie nicht spezifizierte dutzende weiterer hochwertiger Ziele der USA. Die Schwachstelle erhielt einen CVSS Base Score von 10 von 10 Punkten und gilt damit als überaus kritisch.

Mittels der Schwachstelle können Angreifer über die Webschnittstelle der Pulse Connect Secure Software beliebigen Code ohne Authentifizierung ausführen und somit die betroffenen IT-Systeme vollständig kontrollieren. Es gibt eindeutige Hinweise, dass die Schwachstelle durch APT Gruppen vor Alarmierung der Öffentlichkeit in Europa und den USA ausgenutzt wurde. Betroffen sind kritische Infrastrukturen, Verteidigungsunternehmen, Regierungsbehörden und Telekommunikation. Für die Schwachstelle wurde am 03.05.2021 ein Sicherheitsupdate veröffentlicht, welches die Schwachstelle behob. /BSI21w08/, /MAN21r01/

Für weitere Schwachstellen wie CVE-2021-22908, die anschließend bekannt, und mit einem CVSS Base Score von bis zu 8,5 von 10 Punkten bewertet wurden, erfolgte die Veröffentlichung von Sicherheitsupdates durch den Hersteller erst mit Verzögerungen von einigen Wochen nach Bekanntwerden. Der Hersteller veröffentlichte darüber hinaus mögliche Mitigationsmaßnahmen, welche vom BSI auch weiterhin insbesondere für solche IT-Systeme empfohlen werden, die kein Update erhalten haben oder erhalten können. /BSI21w08/, /MAN21r01/

Die auf der Schwachstelle CVE-2021-22893 basierenden IT-Angriffe wurden den APT Gruppen UNC2630 und UNC2717 zugeordnet. Mit der Veröffentlichung der Schwachstellen von Pulse Connect Secure kam es zu weiteren IT-Angriffen unter Ausnutzung der Schwachstellen. Es besteht bisher keine vollständige Übersicht, welche Unternehmen sowie staatlichen Stellen und Bereiche der kritischen Infrastruktur tatsächlich vom IT-Angriff betroffen waren, insbesondere dutzende „Hochwert“ Ziele, die betroffen sein sollen, wurden nicht namentlich veröffentlicht. Mittels der Schwachstelle konnten betroffene IT-Systeme vollständig von den IT-Angreifern kontrolliert werden. Von hier aus konnte auf angeschlossene IT-Netzwerke je nach Umständen zugegriffen werden, wobei die Entwendung von Daten und Informationen Ziel der Angriffe gewesen sein soll. /MAN21r01/

Am 15. März 2022 wurde die Schwachstelle CVE-2022-0778 bekannt, welche die Software OpenSSL betrifft. OpenSSL wird von Pulse Connect Secure für die SSL Verschlüsselung angewendet und ist in die Software integriert. Die Schwachstelle mit einem CVSS Base Score von 7,5 von 10 ermöglicht Angreifern die Überführung betroffener IT-Systeme in einen Denial-of-Service Zustand. /PUL22w02/

Kerntechnischer Bezug

Derzeit sind keine Auswirkungen mit kerntechnischem Bezug bekannt.

B.14.13 IT-Angriff auf T-Mobile US und folgende SIM-Swaps

Übersicht

T-Mobile US ist die amerikanische Tochtergesellschaft der deutschen Telekom und mit über 100 Millionen Kunden der größte Mobiltelekommunikationsanbieter der USA. T-Mobile US veröffentlichte seit 2018 insgesamt sieben verschiedene Datenabflüsse durch IT-Angriffe, wovon mehrere als schwerwiegend anzusehen sind. Im Rahmen der Datenabflüsse wurden Millionen Kundendaten verschiedener Kundenkategorien durch IT-Angreifer entwendet. Die so entwendeten Zugangsdaten der Mitarbeiteremailaccounts und die IT-Angriffe ermöglichten im Jahr 2021 auf zwei unterschiedliche Arten sogenannte SIM Swap Attacks. Bei diesen Angriffen erhalten die Angreifer eine funktionierende SIM-Karte, der die Telefonnummern und Telefonverträge der Opfer zugeordnet sind. Damit können Angreifer die Mobilkommunikation der Kunden vollständig übernehmen. /BLE21w03/

Beschreibung

Der bekannteste IT-Angriff auf T-Mobile US wurde im August 2021 bekannt. IT-Angreifer erlangten Zugriff auf das IT-Netzwerk des Telekommunikationskonzerns und erbeuteten laut T-Mobile US Datensätze zu 7,8 Millionen Vertragskunden, 40 Millionen früheren oder potenziellen Kunden und 850.000 Kunden mit Prepaid-Konten. Gemäß T-Mobile US wurden hierbei Namen, Sozialversicherungsnummern, Geburts- und Führerscheindaten entwendet, jedoch keine finanziellen Daten oder Passwörter. Die Angreifer selbst gaben an, dass Sie Daten von mehr als 100 Millionen Kunden erlangten und forderten für den Kauf eines Datensatzes mit Millionen Führerscheindaten und Sozialversicherungsnummern insgesamt 285.000 Dollar. Gemäß T-Mobile US erlangten die Angreifer Zugang zu einer Testumgebung und nutzten von hier aus Brute Force-Angriffe, um auf das IT-Netzwerk des Konzerns zuzugreifen. Der Angriff reiht sich in eine Reihe von Datendiebstählen bei T-Mobile US ein, im Jahr 2018, 2019 und 2020 kam es zu weiteren Datendiebstählen durch IT-Angriffe.

Dazu wurden die Zugangsdaten der Mitarbeiter durch einen IT-Angriff auf einen externen Dienstleister im Jahr 2020 entwendet. /BLE21w03/

Besondere Aufmerksamkeit erhielten insbesondere zwei IT-Angriffe, bei welchen sogenannte SIM-Swaps durch IT-Angreifer durchgeführt wurden. SIM-Karten dienen in Telefonen und anderen IT-Systemen als Identifikationsobjekte der Nutzer und werden zur Bereitstellung von mobilen Telekommunikations- und Datenanschlüssen von Telekommunikationsunternehmen genutzt. SIM-Karten werden durch PINs und PUKs vor unbefugten Zugriffen geschützt. Falls SIM-Karten verloren gehen, bieten Telekommunikationsdienstleister verschiedene Formen an, neue SIM-Karten zu beantragen, ebenso gibt es die Möglichkeit mehrere gleiche SIM-Karten für verschiedene Endgeräte zu erhalten. Im Rahmen der SIM-Swap Angriffe können die Verfahren zum Erlangen von Ersatz-SIM-Karten, welche entweder durch menschliche Bediener betrieben werden oder vollautomatisiert sind, beeinflusst werden, um die neuen SIM-Karten zu erhalten. Mit den SIM-Karten haben die IT-Angreifer Zugriff auf alle eingehenden SMS sowie Telefonanrufe der Opfer und können selbst SMS verschicken bzw. Telefonanrufe mittels der Telefonnummer der Opfer durchführen. Die Opfer erhalten bis auf den Ausfall der eigenen Telekommunikation zum Teil keinen Hinweis auf durchgeführte SIM-Swaps. /ZDN21w05/

Im Rahmen von Multi-Faktor-Authentifizierungen werden häufig SMS zur Zweifaktorprüfung von Anmeldungen auf IT-Systemen, Fernzugriffe und IT-Services wie Emailaccounts, Onlinebanking oder soziale Medien genutzt. Zusammen mit Passwörtern erhalten die IT-Angreifer mittels SIM-Swaps somit einen umfassenden Zugriff auf entsprechende Services und IT-Systeme der Opfer. Zumeist bieten IT-Services sogenannte Accountwiederherstellung an, falls Passwörter vergessen wurden. So kann auch ohne Kenntnis der Passwörter der Opfer mittels SIM-Swap ein Zugriff erreicht werden. Mit dem Zugriff auf zentrale Emailaccounts können zumeist weitere Accounts, die den Emailaccount zur Wiederherstellung nutzen, übernommen werden. /ZDN21w05/

Im Februar 2021 gab T-Mobile US bekannt, dass insgesamt 400 Kunden von einer Form von Informationsdiebstahl betroffen waren. Zu den Informationen gehörten PINs, Sicherheitsfragen und -antworten, Kundeninformationen und persönliche Informationen, wodurch es zu SIM-Swaps kam. Die Angreifer nutzten die von T-Mobile US angebotene Möglichkeit zur Beschaffung von Ersatz-SIM-Karten.

Im Dezember 2021 kam es zu einem weiteren Vorfall, bei welchem T-Mobile US bekannt gab, dass es nicht autorisierte Aktivitäten in den von den Kunden einsehbaren Nutzerinformationen gab. Mittels dieser Daten ist es zum SIM-Swap durch die IT-Angreifer gekommen. /BLE21w03/

Nach bisherigen Erkenntnissen wurden die SIM-Swaps nicht spezifisch durchgeführt, führten bei Betroffenen jedoch zum Teil zu erheblichen finanziellen Schäden. So wurde eine Klage eingereicht, weil ein Kunde von T-Mobile US insgesamt mehr als 8,7 Millionen Dollar in Form von Kryptowährungen verlor, nachdem durch einen SIM-Swap Zugriff auf Handelsplattformen von Kryptowährungen durch die Angreifer erlangt wurde. /BLE21w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.14 IT-Angriffe mit DeadBolt

Übersicht

Im Januar 2022 kam es zu einem breiten IT-Angriff mittels Ransomware auf NAS-Systeme des Anbieters QNAP. Im Rahmen dieses IT-Angriffs wurden die betroffenen NAS-Systeme durch die Schadsoftware verschlüsselt, wodurch gespeicherte Daten nicht mehr abrufbar waren, und anschließend ein Lösegeld verlangt. /QNA22r01/

Beschreibung

QNAP ist ein taiwanesischer Anbieter für NAS-Systeme und vertreibt diese weltweit. Die NAS-Systeme des Herstellers bieten umfassende Funktionalitäten an, um einen Zugriff auf die NAS-Systeme aus dem Internet zu ermöglichen. Am 25. Januar 2022 kam es zu einer IT-Angriffsserie auf NAS-Systeme von QNAP, bei welchen die Angreifer eine hohe Anzahl an NAS-Systemen, welche über das Internet ansteuerbar waren, mit Ransomware angriffen. Die Ransomware verschlüsselte sämtliche gespeicherte Dateien und fügte diesen anschließend die Endung „.Deadbolt“ an. Die Angreifer nutzten schließlich die HTML-basierten Zugriffsmöglichkeiten auf die NAS-Systeme um den Opfern eine Aufforderung zur Überweisung von 0,03 Bitcoin (zum damaligen Zeitpunkt ca. 1.100 US Dollar) anzuzeigen.

Nach eingegangener Überweisung wurde den Opfern ein Entschlüsselungscode zugeschickt. Insgesamt 5.000 von 130.000 Online identifizierbaren NAS-Systemen von QNAP wiesen Anzeichen auf eine Infektion mit Deadbolt auf. Es bestand für Betroffene kein direkter Kontakt zu den IT-Angreifern, die Übersendung der Entschlüsselungscodes erfolgte vollautomatisch mittels in Bitcoin-Transaktionen inkludierter Informationen. /QNA22r01, ENI22r01/

Bekanntheit erlangte der IT-Angriff insbesondere durch die Aussagen der Angreifer, dass diese eine bis dahin unerkannte Zero-Day-Schwachstelle ausnutzen würden und für 5 Bitcoin (zum damaligen Zeitpunkt ca. 117.000 US Dollar) die Informationen über diese Schwachstelle sowie für 50 Bitcoin (zum damaligen Zeitpunkt ca. 1,7 Millionen US Dollar) den Hauptschlüssel zur Entschlüsselung aller betroffenen IT-Systeme zum Kauf anboten. QNAP reagierte auf die IT-Angriffe durch Deadbolt am 02. Februar 2022 mit dem Hinweis, dass eine Schwachstelle ausgenutzt wurde, welche am 13. Januar 2022 durch QNAP in einem Security Advisory bekanntgemacht wurde und für welche ein Update für alle betroffenen QNAP Systeme seit dem 13. Januar 2022 bereitsteht. Weiterhin wies QNAP die Nutzer daraufhin besondere Sicherungsmaßnahmen für die eigenen NAS-Systeme zu treffen, z. B. die direkte Konnektivität zum Internet für die Systeme abzuschalten oder aber spezielle VPN-Verbindungen für Zugriffe zu etablieren. /ENI22r01/

Im Mai 2022 kam es zu einer weiteren Welle an Deadbolt Ransomware-Angriffen auf NAS-Systeme von QNAP. Gemäß eines Security Advisorys von QNAP vom 17. Juni 2022 waren ausschließlich nicht aktualisierte Versionen der NAS-Systeme betroffen. Weiterhin kam es zu Ransomware-Angriffen mit der Schadsoftware ECh0raix (auch SunCrypt genannt) sowie weiteren Ransomwares. NAS-Systeme wurden in den letzten Jahren zu einem typischen Ziel für IT-Angreifer, besonders für Ransomware-Angriffe. NAS-Systeme werden vielfach mit Anbindungen ans Internet genutzt, als Speichersysteme werden sie für eine hohe Onlinezeit selten aktualisiert und insbesondere im Fall von QNAP meiden Nutzer aktiv die Updates aufgrund von früheren und aktuellen Komptabilitätsproblemen und Systemfehlfunktionen nach Updates. /TRE22r01, QNA22r02/

Da NAS-Systeme neben Privatanwendern insbesondere von Unternehmen und Behörden angewendet werden, werden diese häufig insbesondere aufgrund ihrer konstanten Verfügbarkeit eingesetzt, sodass Updates verzögert oder überhaupt nicht aufgespielt werden.

NAS-Systeme werden zudem häufig „out of the box“ in Betrieb genommen ohne umfassende IT-Sicherungsmaßnahmen oder Konfigurationen, sodass diese, aber auch andere typische IoT-Systeme vermehrt von Angreifenden als Ziel genommen werden. Neben Ransomware-Angriffen sind so auch Angriffe zum Erlangen der gespeicherten Daten sowie zur Etablierung in Netzwerkstrukturen bekannt geworden. QNAP alleine hat für die eigenen vom Januar 2022 bis zum Juni 2022 insgesamt 22 Security Advisories veröffentlicht oder aktualisiert.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.15 IT-Angriff über USB-Sticks

Übersicht

Seit August 2021 kam es in den USA laut /FBI22l01/, /HEI22w03/ zum Verschicken von USB-Sticks, welche Ransomware enthalten. Diese werden getarnt als Geschenkbox oder Covid-19-Leitlinien an diverse US-Firmen, insbesondere aus der Transport-, Versicherungs- und Rüstungsbranche (kritische Infrastrukturen) verschickt. Welche Auswirkungen diese Attacke bisher hatte, wurde von /FBI22l01/, /HEI22w03/ nicht genannt. Die Angriffe erfolgten durch eine bereits seit dem Jahr 2013 bekannte Gruppierung namens FIN7 (auch bekannt als Carbanak), welche bekannt ist für Phishing Attacken sowie Schadsoftware in Bankservern, Geldautomaten und Bezahlterminals mit dem Ziel, finanziellen Gewinn damit zu erzielen. Die Gruppierung FIN7 hat laut /HEI22w04/ bereits einen Schaden von mehr als einer Milliarde US-Dollar verursacht und mehrere hundert US-Unternehmen angegriffen.

Beschreibung

Die USB-Sticks wurden seit August 2021 verschickt, wobei die Lieferung über den US Postal Service oder UPS erfolgte. Die USB-Sticks wurden in zwei Varianten verschickt: Bei der ersten Variante ist der Absender das US Department of Health and Human Services (Gesundheitsministerium) und das Paket enthält den USB-Stick und Briefe, die sich auf Covid-19-Leitlinien beziehen. Bei der zweiten Variante enthält das

Paket eine Geschenkbox von Amazon mit dem USB-Stick und einem gefälschten Dankesschreiben.

Durch die falsche Vorspiegelung, die USB-Sticks stammten von den genannten Institutionen, sollen die Empfänger in Sicherheit gewogen und dazu verleitet werden, diese tatsächlich zu nutzen. Es wird somit gezielt der Faktor Mensch ausgenutzt, um als Schwachstelle zu fungieren und Zugriff auf interne Netzwerke zu erhalten. /FBI22l01, HEI22w03, WIN22w01/

In beiden verschickten Varianten enthielten die Pakete USB-Sticks der Marke LilyGO, welche die Malware BadUSB oder Bad Beetle USB enthalten, die im Internet käuflich zu erwerben sind. Diese Malware ermöglicht die Ausführung von Programmen aus der Ferne oder das Einschleusen von Malware in den betroffenen PC. Nach dem Einstecken der USB-Sticks wird durch die enthaltene Malware BadUSB bzw. Bad Beetle USB eine inhärente Schwachstelle der USB-Firmware ausgenutzt, welche es ermöglicht, die USB-Sticks so zu programmieren, dass sie als menschliche Schnittstellengeräte fungieren. Dabei registriert sich der USB-Stick beim Einstecken als Tastatur, womit eine mögliche Einstellung, dass externe Speichermedien nicht automatisch ausgeführt werden, umgangen wird. Bei einem Einstecken des USB-Sticks in einen privaten oder dienstliches PC werden diese mit Malware infiziert, worauf weitere Erpressungen oder IT-Angriffe erfolgen können. /FBI22l01/, /HEI22w03/

Nach dem Einstecken der USB-Sticks werden Programmroutinen ausgeführt, die vorkonfigurierte, automatische Tastatureingaben ablaufen lassen, um einen PowerShell-Befehl namens KillACK auszuführen, welcher dem dauerhaften Zugriff auf das Zielsystem und dem Diebstahl von Informationen dienen soll. Außerdem wird Malware von einem von FIN7 kontrollieren Server heruntergeladen und ausgeführt. Daran anschließend wird seitens der Täter der Versuch unternommen, administrativen Zugang zu erhalten und anschließend durch Seitwärtsbewegungen im betroffenen Netzwerk auf andere lokale Systeme überzugreifen. Die verwendete Malware ist dabei z. B. Metasploit, Cobalt Strike, PowerShell-Skripte, Carbanak, Griffon, Diceloader und Trion sowie Ransomware wie BlackMatter oder REvil. /FBI22l01/, /HEI22w03/, /ZDN22w02/

Ähnliche Attacken wurden von FIN7 bereits im Jahr 2020 durchgeführt, damals im Namen des Elektronikhändlers BestBuy. Ziel der Attacken waren Hotels, Restaurants und Einzelhandelsgeschäfte in den USA. Bei diesen Attacken wurden Flash-Laufwerke verschickt, die Malware beinhalteten. Außerdem wurde Kontakt per E-Mail oder telefonisch

aufgenommen, um darauf zu drängen, die Laufwerke mit dem Rechner zu verbinden. /FBI22l01/, /HEI22w03/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.16 IT-Angriff auf Oiltanking

Übersicht

Laut /HEI22w07/ wurde am 29.01.2022 festgestellt, dass es zu einem IT-Angriff auf das Unternehmen Oiltanking gekommen ist. Oiltanking ist ein Tanklagerlogistikunternehmen und betreibt diverse Tanklager in Deutschland sowie anderen Ländern in Europa, Amerika, Afrika und Asien und ist damit ein Unternehmen einer kritischen Infrastruktur. Von den Angriffen waren allerdings nur deutsche Anlagen betroffen.

Beschreibung

Oiltanking wurde Opfer eines IT-Angriffs mit Ransomware, für den laut /COM22w01/ die Gruppierung BlackCat verantwortlich ist. Nach Entdeckung des Angriffs, wurden umgehend externe Spezialisten und Behörden zur Klärung hinzugezogen. Von den Angriffen waren alle Be- und Entladesysteme von Oiltanking in Deutschland betroffen, was dazu führte, dass Tankwagen nicht mehr beladen werden konnten. Dies wiederum führte dazu, dass viele Tankstellen in Norddeutschland, u. a. die des Unternehmens Shell, nicht mehr von Oiltanking beliefert werden konnten. Insgesamt waren 233 Tankstellen in Norddeutschland betroffen, in denen außerdem keine Kartenzahlung und keine automatische Anpassung der Preise mehr möglich war. Die Versorgungslage in Deutschland war durch den Angriff nicht gefährdet, da insgesamt 26 Unternehmen im Bereich der Tanklagerlogistik in Deutschland aktiv sind und diese die ausgefallenen Kapazitäten übernehmen konnten. /HEI22w07/

BlackCat ist eine bekannte Ransomware-Gruppierung, deren Angriffe erstmals im November des Jahres 2021 bekannt wurden und die seitdem bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. BlackCat ist dabei die erste Organisation, die ihre Ransomware in der Programmiersprache Rust geschrieben hat, wodurch die Ransomware relativ einfach auf mehrere Betriebssysteme und

Prozessarchitekturen anzupassen ist und damit speziell auf ein ausgewähltes Ziel zugeschnitten werden kann. Wie üblich erfolgt bei einem Angriff eine Verschlüsselung der Daten und eine Erpressung von Lösegeld für deren Entschlüsselung.

Für den Fall des Nichtbezahlens des Lösegeldes, wird mit der Veröffentlichung der Daten gedroht. Weitere Informationen zur BlackCat-Gruppierung finden sich in Abschnitt B.14.19.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.17 IT-Angriff auf Nordex

Übersicht

Am 31.03.2022 wurde festgestellt, dass es zu einem IT-Angriff auf Nordex, einem der weltweit größten Hersteller und Service Provider von Windenergieanlagen (kritische Infrastruktur) mit Niederlassungen in mehr als 30 Ländern und Hauptsitz in Deutschland, gekommen ist. Aufgrund des Angriffs wurden vorsorglich IT-Systeme an mehreren Standorten abgeschaltet, um eine weitere Ausbreitung zu verhindern. /BIS22r09/, /CYB22w01/, /NOR22w01/

Beschreibung

Nordex wurde Ziel eines IT-Angriffs mit Ransomware, zu dem sich die Ransomware-Gruppierung Conti bekannt hat. Der Angriff wurde frühzeitig bemerkt und es wurden umgehend Gegenmaßnahmen eingeleitet, wobei als Vorsichtsmaßnahme IT-Systeme an mehreren Standorten und in mehreren Geschäftsbereichen abgeschaltet wurden. Außerdem wurde der Fernzugriff auf von Nordex verwaltete Anlagen vorsorglich abgeschaltet. Der Angriff blieb auf interne Systeme bei Nordex beschränkt, ein Übergreifen auf Anlagen der Kunden von Nordex konnte nicht festgestellt werden. Die von Nordex betreuten Windenergieanlagen blieben ebenfalls ohne Beeinträchtigung weiter in Betrieb. /BLE22w04/, /NOR22w01/

Trotz der sofort eingeleiteten Maßnahmen zur Eingrenzung der Auswirkungen und zur Wiederherstellung der Systeme waren laut /SEC22w04/ auch mehr als eine Woche nach dem IT-Angriff noch nicht alle IT-Systeme wieder in Betrieb.

Conti ist eine bekannte Ransomware-Gruppierung, die von einer russischen Gruppe betrieben wird und bereits diverse erfolgreiche Angriffe auf Unternehmen weltweit durchgeführt hat. In der Regel verschafft sich Conti Zugang zu einem Unternehmensnetzwerk, nachdem ein Gerät durch einen Phishing-Angriff mit den Schadprogrammen Bazar-Loader oder TrickBot infiziert wurde. Darauffolgend breitet sich Conti lateral im Opfernetzwerk aus und stiehlt Daten, die auf Conti-Server geladen werden. Dann erfolgt die Verschlüsselung der Daten und die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie: Es wird ein Lösegeld für die Entschlüsselung der Daten verlangt. Wird dieses nicht gezahlt, werden die Daten nicht entschlüsselt und zusätzlich veröffentlicht. /BLE22w04/

Laut /BSI22r10/ wurden ca. 40 % (etwa 24 GB) der gestohlenen Daten von Conti auf deren Webseite veröffentlicht. Bei den Daten handelt es sich um insgesamt 18 Archive im tar- und rar-Format. Dies lässt darauf schließen, dass von Nordex kein Lösegeld bezahlt wurde und mit der Veröffentlichung der Daten begonnen wurde. Über eine Höhe des geforderten Lösegeldes oder weitere Einzelheiten sind keine Informationen verfügbar.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.18 IT-Angriff mit Black Basta Ransomware

Übersicht

Laut /BSI22r07/ ist seit April 2022 eine neue Ransomware-Gruppierung mit dem Namen Black Basta aktiv. Bis heute kam es bereits zu diversen erfolgreichen IT-Angriffen dieser Gruppierung, womit sie innerhalb eines kurzen Zeitraums zu einer bedeutenden Bedrohung geworden ist. Dabei wurden weltweit Unternehmen aus diversen Branchen, wie beispielsweise Fertigungsindustrie, Baugewerbe, Transportwesen, Telekommunikationsunternehmen, pharmazeutische Industrie, Kosmetikindustrie oder Autohändler

angegriffen. /HAC22w02/ Black Basta nutzt dabei die bei Ransomware-Gruppierungen übliche Vorgehensweise der doppelten Erpressungsstrategie. Vor dem Verschlüsseln der Daten werden diese extrahiert. Wird dann kein Lösegeld für das Entschlüsseln der Daten gezahlt, werden diese nicht entschlüsselt und außerdem veröffentlicht. /BSI22r07/

Beschreibung

Die ersten bekannt gewordenen Angriffe der Ransomware-Gruppierung Black Basta erfolgten in der zweiten Aprilwoche 2022. Die Angriffe erfolgten weltweit, wobei in Deutschland unter anderem die Deutsche Windtechnik aus Bremen ein Opfer der Angriffe wurde. /BSI22r07/ Innerhalb weniger Wochen wurden bereits diverse Unternehmen weltweit erfolgreich angegriffen, wobei die Lösegeldforderungen von Opfer zu Opfer variierten, aber im Bereich einiger Millionen US-Dollar lagen. /BLE22w02/ Der Angriff auf die Deutsche Windtechnik war dabei einer der ersten Angriffe der Gruppierung Black Basta. Er erfolgte am 11.04.2022. Infolge des Angriffs wurden die Datenüberwachungsverbindungen zu den Windenergieanlagen aus Sicherheitsgründen abgeschaltet. Diese konnten nach 1-2 Tagen wieder aktiviert werden. An den Windenergieanlagen ist kein Schaden entstanden. Als Folge der Angriffe hat die Deutsche Windtechnik eine neues IT-Sicherheitskonzept implementiert. /DEU22w01/

Laut /BSI22r07, BLE22w02/ handelt es sich bei der Gruppierung Black Basta vermutlich nicht um eine neue Gruppierung, sondern eher um eine Neuauflage einer früheren, hochrangigen Ransomware-Gruppierung. Hinweise darauf liefert die Tatsache, dass in kurzer Zeit viele erfolgreiche Angriffe durchgeführt wurden sowie die routinierte Verhandlungsweise mit den Opfern. Die Angriffe der Gruppierung Black Basta zeigen Ähnlichkeiten zur Gruppierung Conti (ähnlicher Verhandlungsstil, ähnliches Design der Webseite), wobei sich die von Black Basta genutzte Software zur Verschlüsselung der Dateien von der von Conti genutzten deutlich unterscheidet. Laut /HAC22w02/ bestreitet Conti, mit Black Basta in Verbindung zu stehen. Laut /SEC22w03/ gibt es Hinweise, die darauf hindeuten, dass es sich bei Black Basta um eine russische Gruppierung handelt.

Laut /SEC22w03/, /BLE22w02/ wird bei den Angriffen von Black Basta folgendermaßen vorgegangen: Nach dem Eindringen in das Opfernetzwerk wird gezielt nach dem Domain Controller gesucht und sich anschließend seitwärts im Netzwerk bewegt. Dabei werden auf kompromittierten Domain Controllern von Black Basta Gruppenrichtlinienobjekte erstellt, um Windows Defender zu deaktivieren. Gleichzeitig wird versucht, Antivirenprodukte auszuschalten. In der letzten Phase des Angriffs wird die Ransomware auf den

Zielgeräten installiert. Dies geschieht mittels eines verschlüsselten PowerShell-Befehls, der Windows Management Instrumentation (WMI) nutzt, um die Ransomware an ausgewählte IP-Adressen zu senden. Anschließend löscht die Ransomware die virtuellen Schattenkopien und andere Sicherungsdateien, bevor die Verschlüsselung durchgeführt wird.

Die Ransomware startet den Computer im abgesicherten Modus neu, darauffolgend wird ein gekaperter Windows-Dienst (z. B. Fax) gestartet, der wiederum die Verschlüsselung startet. Die Verschlüsselungssoftware selbst muss mit Administratorrechten ausgeführt werden, ansonsten ist eine Datenverschlüsselung nicht möglich. Des Weiteren wird durch die Ransomware der Bildschirmhintergrund geändert und eine Nachricht angezeigt, dass Daten verschlüsselt wurden. Die Verschlüsselungssoftware verwendet den ChaCha20-Algorithmus zur Verschlüsselung der Dateien, wobei der ChaCha20-Schlüssel mit einem öffentlichen RSA-4096-Schlüssel verschlüsselt wird. Laut /MAL22w01/ ist ChaCha20 ein kryptografischer Algorithmus, der für seine Geschwindigkeit bekannt ist. Er wird parallel mit Multithreading ausgeführt, um die Verschlüsselung zu beschleunigen, eine Entdeckung zu vermeiden und den Durchsatz der Ransomware zu erhöhen. Verschlüsselten Dateien wird die Endung .basta angefügt, außerdem wird ein benutzerdefiniertes Symbol angezeigt.

Laut /BSI22r08/, /UPT22w01/ wurde die Software von Black Basta weiterentwickelt und ist mittlerweile in der Lage, neben Windows-Systemen auch virtuelle Maschinen auf VMWare-ESXi-Servern unter Linux zu verschlüsseln. Dabei verschaffen sich die Angreifer Zugang zu ESXi-Servern und nach dem Start der Ransomware sucht diese nach dem Ordner /vmfs/volumes. Daran anschließend beginnt die Software mit der Verschlüsselung des Ordners, der standardmäßig alle virtuellen Maschinen des Linux-Servers enthält. Die Verschlüsselung erfolgt auch hier mit dem ChaCha20-Algorithmus.

Laut /BLE22w03/ hat sich die Black Basta-Gruppierung mit der Gruppierung QBot (QuakBot) zusammengeschlossen, um sich über gehackte Unternehmensumgebungen zu verbreiten. QBot ist eine Malware für Windows-Systeme, die ursprünglich zum Ausspähen von Bankdaten entwickelt und in Richtung des Ausspähens von Windows-Domänen-Zugangsdaten weiterentwickelt wurde. Außerdem ist QBot in der Lage, Malware-Programme auf infizierte Geräte zu übertragen. Die Opfer werden in der Regel durch Phishing-Angriffe mit maliziösen Anhängen mit QBot infiziert. QBot wird dabei für den Erstzugriff auf ein Ziel-Netzwerk verwendet, Black Basta hat es weiterhin genutzt, um sich seitlich im Netzwerk zu verbreiten. Eine Zusammenarbeit zwischen einer

Ransomware-Gruppierung und QBot ist nicht unüblich, QBot werden zahlreiche Kooperationen mit anderen Ransomware-Gruppierungen nachgesagt.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.19 IT-Angriff mit BlackCat Ransomware

Übersicht

Laut /FBI22l02/, /BSI22r05/ kommt es seit mindestens Mitte November des Jahres 2021 zu Angriffen einer neuen Ransomware-Gruppierung mit dem Namen BlackCat (auch bekannt als ALPHV oder Noberus). Hierbei handelt es sich um eine Ransomware-as-a-Service-Gruppierung, bei der es Hinweise darauf gibt, dass sie bereits über umfangreiche Erfahrungen und Netzwerke mit Ransomware-Operationen verfügt. Laut /FBI22l02/ sind weltweit bis Mitte April 2022 mindestens 60 Fälle bekannt geworden, bei denen es zu einem erfolgreichen Angriff von BlackCat gekommen ist. Dabei wurden laut /SEC22w01/ Firmen wie Moncler, Swissport oder Inetum Opfer der Angriffe. Laut /BSI22r05/ ist BlackCat die erste bekannte Ransomware, die in der Programmiersprache Rust entwickelt wurde.

Beschreibung

Die ersten bekannt gewordenen IT-Angriffe der Ransomware-Gruppierung BlackCat erfolgten laut /FBI22l02/ im November 2021. Es wurden diverse Firmen weltweit angegriffen, wobei in Deutschland laut /BSI22r06/, /SEC22w02/ zwei Unternehmen, die im Bereich der Lagerung und Lieferung von Öl und Mineralöl-Produkten tätig sind, betroffen waren. Dies waren die Oiltanking Deutschland GmbH, die Tanklager in Deutschland betreibt, sowie die Mabanaft-Gruppe, die Importeur, Großhändler und Lieferant von Heizöl, Benzin, Dieselkraftstoff, Düsentreibstoff und anderen Ölprodukten ist. /SEC22w02/ Weltweit wurden laut /ZDN22w03/ mehrere Unternehmen in Europa, Afrika, Asien und den USA angegriffen, wobei meist Firmen mit kritischer Infrastruktur das Ziel waren und mehr als 30 % der Angriffe auf US-Firmen abzielte. Laut /WAT22w02/ erfolgte Mitte Mai des Jahres 2022 ein Angriff von BlackCat auf staatliche IT-Systeme des österreichischen Bundeslandes Kärnten.

Von diesem Angriff waren die Regierung, Bezirksverwaltungen, der Rechnungshof und das Verwaltungsgericht betroffen. Eine Lösegeldforderung von 5 Millionen US-Dollar wurde nicht bezahlt. Außerdem erfolgte laut /WAT22w02/ durch BlackCat ein IT-Angriff auf die ecuadorianische Hauptstadt Quito, wobei mehrere staatliche Systeme lahmgelegt wurden.

Ein weiterer IT-Angriff der Ransomware-Gruppierung BlackCat auf Unternehmen der kritischen Infrastruktur erfolgte am 22. Juli 2022 auf den luxemburgischen Netzbetreiber Creos und den luxemburgischen Energieversorger Enovos, die beide zur Encevo-Gruppe gehören und eine Gaspipeline sowie die Stromversorgung in Luxemburg betreiben. Bei dem Angriff wurden Daten verschlüsselt und außerdem 150 GB Daten (180.000 Dateien) gestohlen, darunter vertrauliche Daten wie Verträge, Ausweiskopien, E-Mails und Daten zu Bankkonten. Unmittelbar nach Bekanntwerden des Angriffs wurde von den Geschädigten Anzeige erstattet, die zuständigen Behörden informiert und ein Krisenstab eingerichtet. Die Täter forderten ein Lösegeld in unbekannter Höhe, welches aber nicht gezahlt wurde. Daraufhin wurden die Daten zumindest in Teilen veröffentlicht. Der Angriff hatte Auswirkungen auf den Betrieb der Kundenportale, die Strom- und Gasversorgung wurden aber nicht beeinflusst. Die verschlüsselten Daten wurden aus gesicherten Servern wieder hergestellt, die Überwachung der Systeme wurde verstärkt und alle Passwörter geändert. /BOR22w01/, /SEC22w09/, /ENC22w01/, /SEC22w08/

Die Vorgehensweise war in allen bekannten Fällen ähnlich. Laut /FBI22l02/ werden von BlackCat zuvor kompromittierte Benutzeranmeldeinformationen genutzt, um einen ersten Zugang zum System des Opfers zu erhalten. Die anfängliche Bereitstellung der Ransomware erfolgt mittels Power-Shell-Skripten in Verbindung mit Cobalt Strike. Sobald ein Zugang hergestellt werden konnte, werden Active Directory-Benutzer und Administratorkonten kompromittiert. Außerdem wird der Windows Task Scheduler verwendet, um maliziöse Gruppenrichtlinienobjekte zu konfigurieren und die Ransomware so im System des Opfers weiter zu verteilen. Während der Kompromittierung werden auch legitime Windows-Tools wie das Windows-Verwaltungstool Microsoft Sysinternals genutzt, um Anti-Malware-Tools zu deaktivieren und Ransomware-Programme zu starten. Bevor die Ransomware zur Verschlüsselung der Daten auf dem Opfernetzwerk ausgeführt wird, werden die Daten des Opfers, darunter auch Informationen von Cloud-Anbietern, extrahiert.

Laut /KAS22w01/ umfasst das Arsenal von BlackCat diverse Elemente. Neben Kyrptor zur Verschlüsselung von Dateien wird auch das Programm Fendr zum Exfiltrieren von Daten aus dem Opfernetzwerk verwendet. Dieses Tool deutet darauf hin, das BlackCat enge Verbindungen zur Gruppierung BlackMatter (auch bekannt als Darkside, verantwortlich für Angriffe auf Colonial Pipeline (siehe Abschnitt B.13.5)) hat, da diese bislang als einzige bekannte Akteure dieses Tool eingesetzt haben.

Zudem verwendet BlackCat das PsExec-Tool für Seitwärtsbewegungen im Netzwerk des Opfers sowie die Software Mimikatz und Nirsoft zum Extrahieren von Netzwerkpasswörtern.

Laut /SEC22w01/ ist BlackCat die erste professionell genutzte Ransomware, die in der Programmiersprache Rust geschrieben wurde. Laut /BSI22r05/ ist Rust eine von Mozilla seit dem Jahr 2010 entwickelte Programmiersprache, die eine praxisnahe Alternative zu C++ darstellt. Dabei bietet Rust die Möglichkeit, relativ einfach auf mehrere Plattformen übersetzt zu werden, was es leichter macht, die Ransomware auf mehrere Betriebssysteme und Prozessarchitekturen anzupassen. BlackCat kann laut /SEC22w01/ auf Windows-, Linux- und VMWare ESXi-Systeme abzielen. Laut /REG22w01/ hat Rust im Gegensatz zu C++ Sicherheitsmaßnahmen eingebaut, was bedeutet, dass die Malware stabiler und zuverlässiger sein könnte. Laut /HAC22w01/ gilt Rust als speichersicher und leistungsfähig und bietet neben Entwicklungsvorteilen auch eine geringere Erkennungsrate von statischen Analysetools, die nicht an alle Programmiersprachen angepasst sind.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.20 IT-Angriffe mit Quietexit

Übersicht

Im Dezember 2019 wurde vom IT-Sicherheitsunternehmen Mandiant aufgedeckt, dass die APT-Gruppierung UNC3524 Unternehmen in einem Zeitraum von teilweise 18 Monaten ausspioniert und deren E-Mails mitgelesen hat. Um sich Zugriff auf die Firmennetzwerke zu verschaffen, hatten die Angreifer Backdoors auf IoT-Geräten (Internet of Things) und anderen Systemen installiert, die üblicherweise nicht überwacht und durch

Sicherheitssoftware geschützt werden können. Eine der Backdoors wird als Quietexit bezeichnet. Da die Angreifer systemeigene Programme und Prozesse geschickt nutzten, konnten ihre Aktivitäten so lange unerkannt bleiben.

Beschreibung

Die im Dezember 2019 vom IT-Sicherheitsunternehmen Mandiant aufgedeckte APT-Gruppierung UNC3524 hat Unternehmen in einem Zeitraum von teilweise 18 Monaten ausspioniert und deren E-Mails gelesen. Um nicht entdeckt zu werden, schleusten die Angreifer Backdoors auf IoT-Geräte (Internet of Things) ein, die üblicherweise nur wenig überwacht werden (keine Endpoint-Detektion oder Response-Werkzeuge), keine Sicherheitsupdates erhalten und für die keine spezielle Sicherheitssoftware existiert (keine Antivirenprogramme). Zu den mit den Backdoors infizierten Geräten gehören SAN-Arrays (Storage Area Networks), Load Balancer und Controller für das WLAN, auf denen oft ältere Versionen von Berkeley Software Distribution (BSD) oder Community Enterprise Operating System (CentoS) installiert sind. Von diesen Geräten aus wurde dann der Angriff auf weitere Teile des Firmennetzes ausgeweitet. Die Angreifer setzten dabei Router und sogar aus dem Internet erreichbare Kameras von Konferenzräumen als Command-and-Control-Server (C&C) ein. Die Suche nach der Schadsoftware gestaltet sich entsprechend schwierig. Mandiant empfiehlt deshalb den Einsatz des Programms grep, mit dem sich Dateien nach bestimmten Textfolgen (in diesem Fall Programmcode) durchsuchen lassen. /HEI22w16/, /ART22w01/, /MAN22w03/

Eine der von UNC3524 eingesetzten Backdoors wird als Quietexit bezeichnet. Sie nutzt das zur Verschlüsselung verwendete SSH-Protokoll und eine modifizierte Version der frei verfügbaren Software Dropbear (Ressourcen schonender SSH-Server und -Client /NET20w01/), um eine TCP-Verbindung vom infizierten Gerät im Firmennetzwerk zum externen C&C-Server der Angreifer aufzubauen. Die anschließend aufgebaute SSH-Verbindung ist dagegen vom C&C-Server auf das infizierte Gerät gerichtet. Ein alternativer Zugriffsweg der Backdoor Quietexit nutzt die Webshell[16] Regeorg zur Einrichtung eines SOCKS-Proxys[17]. Dabei achteten die Angreifer darauf die Namen der

[16] Eine Webshell ist ein schadhafter Programmcode, der einem Angreifer die Kompromittierung von Webservern ermöglicht /IMP22w01/.

[17] Ein SOCKS-Proxy ist ein Proxy-Server, der das Protokoll SOCKS (Abkürzung von SOCKetS) verwendet, welches die Kommunikation von Servern über eine Firewall erleichtert /FIN22w01/.

Webshell-Dateien auf den Webservern so zu wählen, dass sie zum infizierten System passten. Falls die Backdoor Quietexit entfernt wurde, konnte sie über die Webshell neu installiert werden. Um nicht aufzufallen, nutzten die Angreifer eine Vorgehensweise, die unter dem Namen Living off the Land (LotL) bekannt ist.

Dabei werden für den Angriff Standard-Programme und Standard-Prozesse des infizierten Systems eingesetzt /DIG22w01/. Zum Beispiel verwendeten sie Zeichenfolgen für Domänennamen, die für den Gerätehersteller plausibel erscheinen. Datenverkehr und Datenvolumen wurden nach Möglichkeit beschränkt. Aufgrund dieser Maßnahmen konnten die Angreifer ihre Aktivitäten über Monate verbergen. /HEI22w16/, /ART22w01/, /MAN22w03/

Auf welche Weise sich die Angreifer initialen Zugriff auf die Firmennetzwerke verschafften ist nicht bekannt. Sie nutzten die mit der Backdoor Quietexit infizierten Systeme für die laterale Ausweitung ihrer Aktivitäten auf weitere Teile des Firmennetzwerks. Die APT-Gruppierung UNC3524 zielte darauf ab Zugriff auf die Exchange-E-Mail-Postfächer von Führungskräften und Mitarbeitern zu erhalten, deren Tätigkeiten die Unternehmensentwicklung, Fusionen und Übernahmen oder die IT-Sicherheit betreffen und deren E-Mails mitzulesen. Dabei wurden integrierte Windows-Protokolle genutzt. Es wird vermutet, dass der Angriff auf das IT-Sicherheitsteam dazu diente, um zu testen, ob die installierte Schadsoftware unentdeckt bleibt. Das professionelle Vorgehen der APT-Gruppierung UNC3524 spricht dafür, dass diese staatlich gefördert wird. Die Angriffstechniken sind vergleichbar mit denen russischer APT-Gruppierungen wie APT28 und APT29. Das IT-Sicherheitsunternehmen Mandiant war jedoch nicht in der Lage UNC3524 einer dieser Gruppierungen oder einer staatlichen Organisation zuzuordnen. /HEI22wxx/, /ART22w01/, /MAN22w03/

Kerntechnischer Bezug

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

B.14.21 IT-Angriffe mit Hyperbro

Übersicht

Seit März 2022 greift die APT-Gruppierung APT27, auch bekannt unter dem Namen Emissary Panda, verstärkt deutsche Unternehmen mit der Schadsoftware Hyperbro an. Dabei sind hauptsächlich Pharma- und Technologieunternehmen betroffen. Das Ziel der Angriffe scheint der Diebstahl von Geschäftsgeheimnissen und geistigem Eigentum zu sein.

Beschreibung

Das Bundesamt für Verfassungsschutz (BfV) warnt in seinem Cyberbrief 01/2022, dass seit März 2021 die APT-Gruppierung APT27 Schwachstellen im Microsoft Exchange Server nutzt, um sich initialen Zugriff auf die IT-Netzwerke deutscher Unternehmen zu verschaffen. Weiterhin gibt das BfV an, dass die Zahl der Angriffe durch APT27 auf deutsche Unternehmen zunimmt. Dabei nutzen die Angreifer das Remote Access Tool (RAT) Hyperbro, um die Netzwerke auszuspionieren und Geschäftsgeheimnisse sowie geistiges Eigentum zu stehlen. Von den Angriffen sind hauptsächlich Unternehmen aus der Pharmaindustrie und Technologieunternehmen betroffen. Zudem kann das BfV nicht ausschließen, dass die Angreifer versuchen werden, die Netzwerke von Kunden und Dienstleistern zu kompromittieren, um Lieferkettenangriffe durchzuführen. Die APT-Gruppierung APT27, welche auch unter dem Namen Emissary Panda bekannt ist, ist seit 2010 aktiv und soll im Auftrag des chinesischen Staates handeln. /HEI22w17/, /ITS22w01/

Die RAT-Schadsoftware Hyperbro besteht aus vier Komponenten: Einem legitimen ausführbaren Loader msmpeng.exe oder vfhost.exe der Software CyberArk, der mit einem gültigen, aber abgelaufenen Zertifikat ausgestattet ist, der schadhaften DLL3-Datei vftrace.dll, die über den Loader per DLL-Hijacking geladen wird, der Payload thumb.dat, den ausführbaren Shellcode, eine schadhafte DLL-Datei sowie Informationen über den Command-and-Control-Server (C&C) der Angreifer beinhaltet und der Konfigurationsdatei config.ini der Schadsoftware. Bei der Installation von Hyperbro lädt der Loader zunächst die Dateie vtrac.dll, die wiederum die Payload thumb.dat lädt und entschlüsselt. Ohne Administratorrechte werden die Daten von Hyperbro im Ordner %Programm-Data%\windefenders\ abgelegt. Liegen Administratorrechte vor, werden die Daten dagegen im Ordner %ProgrammFiles%\Common Files\windefenders\ gespeichert. Die

Schadsoftware wird am neuen Speicherort neu gestartet und imitiert den Windows Defender. Ist Hyperbro bereits installiert und wird die Schadsoftware einfach nur ausgeführt, laufen zunächst die gleichen Schritte ab wie beim Installationsprozess. Nach dem Laden der Payload thumb.dat erfolgen jedoch andere Schritte. Ohne Administratorrechte wird ein Run Key in der Windows Registry erzeugt. Mit Administratorrechten wird dagegen ein Service erstellt. Auf beide Arten wird eine persistente Verbindung sichergestellt. Die Datei config.ini baut dann die Kommunikation mit dem C&C-Server der Angreifer über den TCP-Port 443 auf.

Über den C&C-Server erhält die Schadsoftware Hyperbro weitere Anweisungen von den Angreifern und es können weitere Schadsoftware-Werkzeuge wie z. B. Key-Logger geladen werden. /PRS22w01/

In seinem Cyberbrief veröffentlicht das BfV auch Angriffsindikatoren (Indicators of Compromise IOC). Dazu gehören die IP-Adressen (104.168.236.46, 103.79.77.200 und 87.98.190.184) der C&C-Server der Angreifer sowie die Namen von bestimmten Dateien, Pfaden und Prozessen. Um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu reduzieren, sollten daher nicht nur die entsprechenden Sicherheitsupdates für Microsoft Exchange und den Zoho AdSelf Service Plus 1 installiert werden, um deren Schwachstellen zu schließen, sondern die Systeme sollten auch auf die IOCs überprüft werden. /HEI22w17/, /PRS22w01/

Kerntechnischer Bezug

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

B.14.22 IT-Angriff auf WatchGuard Firewalls

Übersicht

Seit Juni 2019 wurden Firewalls von WatchGuard mit der Schadsoftware Cyclops Blink infiziert, über die von den Angreifern Daten aus dem Netzwerk gestohlen werden konnten. Zudem konnte die Schadsoftware das befallene Gerät zum Teil eines Botnetzes machen und für Angriffe auf andere Ziele nutzen.

Nach Angaben von WatchGuard waren etwa ein Prozent ihrer Geräte von der Schadsoftware betroffen. 2022 konnte das Botnet vom FBI zerschlagen werden.

Beschreibung

Nach einem gemeinsamen Bericht des britischen Cyberabwehrzentrums NCSC, des CISA, der NSA und des FBIs erfolgt seit Juni 2019 eine IT-Angriffswelle gegen die Firebox-Router des Herstellers WatchGuard /CIS22i02/. Dabei nistet sich die Schadsoftware Cyclops Blink in den Router ein. Sie kann Geräteinformationen an den Command-and-Control-Server (C&C) der Angreifer übermitteln. Danach kann die Schadsoftware je nach Einsatzbedarf weitere Schadsoftwarekomponenten nachladen.

Mit diesen können Daten aus dem Netzwerk gestohlen werden. Darüber hinaus kann Cyclops Blink den Router zum Teil eines Botnetzes machen und für Angriffe auf andere Ziele nutzen. Er kann dabei von den Angreifern als C&C-Server oder auch als Drohne eingesetzt werden /HEI22w10/. Zusätzlich kapert die Schadsoftware den Update-Prozess, indem sie sich als Firmware-Update installiert, wodurch sie einen Neustart übersteht. Nach den Angaben von WatchGuard war etwa ein Prozent ihrer in Umlauf befindlichen Geräte infiziert. Eine Infektionsgefahr bestand nur dann, wenn in den Geräten die externe Steuerung über das Internet eingeschaltet war, welche aber in den Standardeinstellungen deaktiviert ist. Wenn ein Gerät mit Cyclops Blink infiziert ist, müssen sämtliche Passwörter als kompromittiert betrachtet werden. Auch wenn kein Router von WatchGuard verwendet wird, ist Vorsicht geboten. Nach den Angaben des NCSC ist die Schadsoftware flexibel genug, um schnell auf andere Geräte übertragen werden zu können. /STE22w01/, /HEI22w10/, /KUD22w01/

Die IT-Angriffe mit Cyclops Blink sind die Fortsetzung einer weiter zurückliegenden Kampagne mit Namen VPNFilter, die 2018 von US-Behörden erfolgreich beendet wurde. Für beide Angriffe soll die APT-Gruppierung Sandworm verantwortlich sein, welche dem russischen Auslandsgeheimdienst GRU zugeordnet wird. /STE22w01/, /HEI22w10/, /KUD22w01/

WatchGuard hat eine entsprechende Anleitung mit Softwarewerkzeugen zusammengestellt, mit denen Administratoren eine Infektion erkennen und beheben können. Nach Angaben des Herstellers sind keine Fälle bekannt, in denen Daten von Kunden oder von WatchGuard selbst gestohlen wurden. Im April 2022 wurde das von Cyclops Blink gebildete Botnet vom FBI zerschlagen, bevor es für IT-Angriffe genutzt werden konnte. Das

FBI entfernte zudem die Schadsoftware Cyclops Blink von WatchGuard-Geräten, die es als C&C-Server identifiziert hatte und benachrichtigte zuvor die entsprechenden Nutzer in den USA und im Ausland. Diese sollten zusätzlich die Anleitungen von WatchGuard befolgen. /HEI22w10/, /BLE22w06/

Kerntechnischer Bezug

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

B.14.23 Physischer Angriff auf IT-Infrastruktur in Frankreich

Übersicht

In der Nacht des 27.04.2022 wurden in Frankreich von unbekannten Angreifern an verschiedenen Stellen Glasfaserkabel durchtrennt, die die Städte Paris, Lyon, Rouen und Straßburg miteinander verbinden. In der Folge kam es zu Netzwerkausfällen von Internet- und Telefonanschlüssen in mehreren Städten entlang der Strecken.

Beschreibung

Mehrere Medien berichteten am 27.04.2022 über eine vorsätzliche Zerstörung von Glasfaserkabeln in Frankreich. Die Kabel waren in der vorrausgegangenen Nacht zwischen 2:00 Uhr und 4:00 Uhr durchtrennt worden. Dabei wurde die Netzinfrastruktur von zwei Anbietern unterbrochen, darunter Free. Es wurden drei Backbone-Strecken an verschiedenen Stellen zerstört, welche von Paris nach Lyon, Rouen und Straßburg führen. Die Kabel sind Eigentum des Netzwerkbetreibers SFR und werden von Free gemietet. In der Folge kam es in mehreren Städten entlang der Strecken zur Verlangsamung von Netzwerkverbindungen und zu Netzwerkausfällen von Internet- und Telefonanschlüssen. Insgesamt waren zehn Internet- und Infrastrukturorganisationen betroffen. Bereits am Vormittag des 27.04.2022 konnten die teils massiven Störungen aber wieder abgefangen werden, indem der Datenverkehr vielfach manuell oder automatisch auf andere Kabel umgeleitet wurde /WIR22w02/. /BSI22i06/, /HEI22w18/, /WIR22w02/

Wer die Kabel zerstört hat ist nicht bekannt, die Angriffe sind jedoch koordiniert durchgeführt worden. Die Angreifer wussten offenbar an welchen Stellen sie an die Kabel gelangen können und auf welche Weise sie den größten Schaden erzielen.

Die Kabel wurden jeweils an zwei Stellen durchtrennt und die Zwischenstücke wurden entfernt, um die Reparatur zu erschweren. Bereits unmittelbar nach den Angriffen hat die Pariser Staatsanwaltschaft Untersuchungen eingeleitet. Der hier beschriebene Angriff ist kein Einzelfall. Bereits im Mai 2020 sind in Frankreich mehrere Netzwerkkabel unterbrochen worden. Die Zerstörung der Glasfaserkabel am 27.04.2022 wurde jedoch deutlich professioneller und koordinierter durchgeführt. /BSI22i06/, /CYB22w03/, /WIR22w02/

Kerntechnischer Bezug

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

B.14.24 IT-Angriff auf ein Unterseekabel

Übersicht

Anfang April 2022 versuchten international agierende Angreifer einen IT-Angriff auf ein Unterseekabel bei Hawaii durchzuführen. Der Angriff konnte rechtzeitig erkannt und gestoppt werden. Es kam zu keinen Schäden.

Beschreibung

Ein Unterseekabel bei Oahu, welches der Anbindung von Internet, Festnetz und dem Mobiltelefonnetz von Hawaii mit der pazifischen Region dient, wurde Anfang April 2022 zum Ziel eines IT-Angriffs /CYB22w04/, /STA22w01/. International agierende IT-Angreifer hatten zuvor Zugangsdaten von einem privaten Telekommunikationsunternehmen auf dem US-amerikanischen Festland gestohlen, das mit dem Unterseekabel in Verbindung steht und sich damit Zugriff auf die Server des Unternehmens verschafft /CYB22w04/, /THR22w01/. Durch einen Hinweis ihrer Kollegen vom Festland der USA, konnte der Angriff durch die Homeland Security Investigation (HSI) Hawaiis abgewehrt werden /HTE22w01/. Es kam zu keinen Schäden. Im Anschluss wurden Verhaftungen vorgenommen. Wer den Angriff durchgeführt hat und welches Telekommunikationsunternehmen betroffen war, wurde vom HSI allerdings nicht bekannt gegeben, um die Strafverfolgung nicht zu gefährden. /BSI22i07/, /HNN22w01/

Um welche Art von IT-Angriff es sich gehandelt hat ist ebenfalls unklar. Nach Meinung von Experten hätten Kommunikationsverbindungen abgeschaltet oder auch individuelle Ziele angegriffen werden können. Da Unterseekabel 95 % des internationalen Internet-Datenverkehrs führen, werden sie in wachsendem Maß zum Ziel autoritärer Regierungen. Diese versuchen den Internetzugriff zu kontrollieren oder den Datenverkehr zu überwachen, um sensible Informationen zu stehlen. Parallel setzen die Betreiber-Unternehmen zunehmend Remote-Management-Systeme für ihre Kabelnetzwerke ein, von denen viele über mangelhafte Sicherheitsfunktionen verfügen.

Dies versetzt IT-Angreifer in die Lage an beliebigen Orten auf der Welt über das Internet Zugriff auf diese Systeme zu erhalten und die Kabelsignale physisch zu manipulieren und zu kontrollieren. /CYB22w04/

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

B.14.25 Strahlenschutz Spanien

Übersicht

Zwischen März und Juni 2021 kam es zu einem IT-Angriff auf das Radioaktivitätsüberwachungs- und -warnsystem Spaniens (Red de Alerta a la Radiactividad (RAR)). Das RAR-System dient zur Überwachung der Gammastrahlungswerte in ganz Spanien und wird von der Generaldirektion für Katastrophenschutz und Notfälle (DGPCE) und dem Ministerium für innere Angelegenheiten verwaltet, betrieben und gewartet. Aufgrund des Angriffs konnten hunderte Detektoren des RAR-Systems, welches zur kritischen Infrastruktur gehört, zur Erkennung von Gammastrahlung temporär nicht genutzt werden/HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Beschreibung

Das RAR-System Spaniens, welches zur Überwachung der Gammastrahlungswerte in ganz Spanien dient, wurde zwischen März und Juni 2021 Opfer eines IT-Angriffs. Das RAR-System umfasst ca. 800 Detektoren für Gammastrahlung, die landesweit in Spanien verteilt sind, und dient als Warnsystem für den Fall, dass die Gammastrahlungswerte ansteigen. Jeder der Detektoren ist mit einem zentralen Knotenpunkt verbunden,

welcher sich im Kontrollzentrum der spanischen Zivilschutzbehörde Dirección General de Protección Civil y Emergencias (DGPCE) in Madrid befindet, welches sowohl Informationen sammeln als auch Befehle senden kann. Des Weiteren gibt es zehn regionale und sieben assoziierte Knotenpunkte, die einen alternativen Zugang zum RAR-System ermöglichen und über begrenzte Verwaltungsfunktionen verfügen. Durch den Angriff kam es zum Ausfall mehrerer hundert der über 800 Detektoren des RAR-Systems zur Erkennung erhöhter Gammastrahlungswerte. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Der Angriff erfolgte dabei in zwei Schritten. Zunächst verschafften sich die Angreifer unrechtmäßig Kontrolle über das Computersystem der DGPCE mit dem Ziel, eine Webanwendung aus dem Kontrollzentrum zu löschen, über welche das RAR-System verwaltet werden kann. In der zweiten Phase wurden im Laufe mehrerer Monate mehr als 300 der Gammastrahlungsdetektoren direkt angegriffen, um die Kommunikation zwischen diesen Detektoren und den Kontrollzentren zu unterbrechen. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Im Juli 2022 wurden zwei Verdächtige verhaftet, die angeblich für die Angriffe verantwortlich sind. Bei diesen handelt es sich um zwei ehemalige Mitarbeiter eines Drittanbieters, welcher im Auftrag der DGPCE mit der Wartung des RAR-Systems beauftragt war. Die beiden Verdächtigen waren dabei für die Wartung der Software zuständig, die sie bei dem Angriff löschen wollten. Es handelt sich also bei den Verdächtigen um Innentäter, durch deren fundierte Kenntnisse des Systems die Ausführung der Angriffe erleichtert wurde. Außerdem halfen die Kenntnisse dabei, die Urheberschaft der Angriffe zu verschleiern und damit die Ermittlungen zu erschweren. Das Motiv für den Angriff ist bisher unklar. Ausgangspunkt der Angriffe war ein öffentlich verfügbarer Internetzugang in einem Madrider Beherbergungsbetrieb. /HEI22w12/, /MAL22w03/, /REG22w03/, /REC22w02/

Kerntechnischer Bezug

Ziel des Angriffs war das Radioaktivitätsüberwachungs- und-warnsystem Spaniens, welches zur Überwachung der Gammastrahlungsaktivität in Spanien dient.

B.14.26 ZuoRAT

Übersicht

Im Mai 2022 wurde von den Sicherheitsforschern von Black Lotus Labs eine neue umfassende Kampagne zur Verbreitung eines auf Router zugeschnitten Remote Access Trojaners (RAT) publiziert. Der als ZuoRAT benannte Trojaner wurde spezifisch für Heimanwenderrouter und Router kleinerer Büros (Small Office/Homeoffice, SOHO) entwickelt und über einen Zeitraum von mindestens zwei Jahren gegen entsprechende Ziele eingesetzt.

Der ZuoRAT zeichnete sich dabei durch seine umfassenden Fähigkeiten aus, was den Angriff auf verschiedenste SOHO Router und seine Angriffswerkezuge betrifft. /MAL22r01/

Beschreibung

Mit der COVID-19 Pandemie kam es ab März 2020 zu einer deutlichen Verlagerung von Büroarbeitsplätzen in die als gesundheitlich sicherer eingeschätzten Heimarbeitsplätze. Infolgedessen wurden vermehrt Daten über Heimnetzwerke und damit SOHO Router geteilt, welche früher ausschließlich in Firmennetzwerken genutzt wurden. IT-Angreifer haben sich daher seit 2020 vermehrt auf IT-Angriffe auf Router, VPN-Verbindungen und andere für das Arbeiten im Homeoffice notwendige Infrastruktur konzentriert (siehe Abschnitt B.14.12 Pulse Connect Secure). Angriffe auf SOHO Router sind keine neue Erscheinung. So kam es 2016 zum gescheiterten IT-Angriff auf mehr als eine Million Telekom Router der Marke Speedport und 2016 wurde das Mirai Botnet bekannt, welches zum Teil auf übernommenen Realtek Routern basierte. Der ZuoRAT Trojaner zeichnete sich nicht nur dadurch aus, dass Teile der Mirai Schadsoftware massiv modifiziert in den Trojaner einflossen, sondern auch dass dieser Trojaner eine Vielzahl verschiedener Router angreifen kann und für anschließende Folgeangriffe im Netzwerk umfassend gerüstet ist. /BLL22r01/

Remote Access Trojaner dienen grundsätzlich IT-Angreifern zur Etablierung einer Backdoor, sodass sie einen temporären oder permanenten Einfallspunkt für die Angreifer etablieren. Der ZuoRAT Trojaner führt diesen ersten Angriffsschritt als erste Stufe einer IT-Angriffsserie aus, besitzt jedoch die Fähigkeit zur weiteren Verbreitung und für weitere Angriffe im betroffenen Netzwerk.

Obwohl verfügbare Daten zeigen, dass unter anderem Router von ASUS, Cisco, DrayTek und NETGEAR betroffen sind, wurde bisher ausschließlich das vollständige Angriffsscript für Router des Typs JCG-Q20 bei erkannten ZuoRAT Trojanern erkannt. Zur erstmaligen Infektion der ausschließlich in China eingesetzten Router wurde ein Proof of Concept für ältere Schwachstellen (CVE-2020-26878 und CVE-2020-26879) durch die Angreifer verpackt in einer Windows Portable Executable genutzt. Mittels dieses Angriffswerkzeugs erlangt ZuoRAT zuerst Zugang zu Passwörtern des betroffenen Routers, dann Zugang zum Router selbst und anschließend wird weiterer Schadcode nachgeladen. Dieser Schadcode ermöglicht das umfassende Ausspionieren des auf dem Router verarbeiteten Datenverkehrs und die Übernahme des Datenverkehrs. Im Rahmen der Ausspionierung können z. B. Accountdaten, verbundene IP-Adressen und Ziele der Datenströme ausgelesen werden.

Um zu erkennen, ob die Schadsoftware auf einem echten Router oder einer Testumgebung läuft, steuerte ZuoRAT per Kommando spezifische Webseiten mit IP-Erkennung an. Konnte keine IP ermittelt werden, löschte sich ZuoRAT selbst. /BLL22r01/

Die nächste Stufe der ZuoRAT Schadsoftware wird auf Kommando durch die Angreifer eingeleitet und dient dem Einwirken in verbundene Netzwerksysteme. Bis zu 2.500 verschiedene Funktionen wurden dafür in die Schadsoftware integriert. Hierzu zählt die vertiefte Auswertung des angeschlossenen LANs, das Auslesen von DNS-Verbindungen, die Speicherung von SSID Informationen und MAC-Adressen der angebundenen Geräte. Darauf aufbauend wurden DNS-Anfragen, also Domain Naming System Anfragen, welche IP-Adressen und ausgeschriebene Webadressen miteinander verbinden, von der Schadsoftware manipuliert. Hierdurch wurden legitime Webseitenaufrufe und Datenübertragungen auf von den Angreifern festgelegte IP-Adressen umgeleitet. Dies können Phishing-Webseiten sein oder Webseiten zur Verbreitung weiteren Schadcodes. Weitere Funktionen dienten dem Neuladen der Schadsoftware, dem Nachladen von Code oder der Abschaltung der Schadsoftware. /BLL22r01/

Der letzte Schritt der ZuoRAT Schadsoftware war der direkte Übergang vom Router auf angebundene Windows-Systeme. Hierzu wurde ein Loader für einen Windows-RAT an die angebundenen Systeme verteilt. Um die Infektionschancen zu erhöhen und die Entdeckungschancen zu minimieren, nutzte dieser Loader ein legitimes Zertifikat des chinesischen Technologiekonzerns Tencent. Über Shellcode wurde anschließend die Schadsoftware RAT CBeacon auf den Windows-Systemen installiert. Andere Systeme

wie Linux, Mac oder Android wurden mit der Schadsoftware GoBeacon RAT angegriffen. Zusätzlich wurde auf die Schadsoftware Cobalt Strike zurückgegriffen. /BLL22r01/

Die ZuoRAT Schadsoftware wurde insbesondere auf Routern in den USA und Europa aufgefunden, jedoch auch in Hongkong und Taiwan. Sie verschleiert sich effektiv durch die Nutzung von bereits infizierten Routern als Systeme zur Kommunikation und zum Nachladen von Schadsoftware und nutzt insbesondere chinesische Services für Datenspeicherung, um eine direkte Erkennung zu vermeiden. Aufgrund vieler chinesischer Bezüge im Quellcode, dem Umfang und der Detailarbeit der ZuoRAT Schadsoftware wurde die Angriffsserie chinesischen staatlichen Stellen attribuiert. „Zuo“ ist chinesisch für Links und leitet sich vom Dateinamen der Schadsoftware asdf, den linken vier Buchstaben der mittleren Tastaturreihe ab. /BLL22r01/

Um IT-Angriffe mit ZuoRAT oder ähnlicher Schadsoftware zu vermeiden, empfehlen die Forscher von Black Lotus Labs die folgenden Schritte: /BLL22r01/

- Nutzung der auf GitHub veröffentlichten Indicator of Compromise (IoC) für die genannten Loader und Schadsoftwares bei der Beobachtung und Sicherung von Netzwerken /GIT22w01/
- Sicherung von SOHO Routern durch regelmäßige Updates und dem Folgen der Best Practices bei der Einstellung der Sicherheitsmaßnahmen
- Einsatz von automatisierten Überwachungssystemen wie Secure Access Service Edge (SASE) im Geschäftsbereich.

Kerntechnischer Bezug

Bislang liegen keine Informationen zu einem konkreten kerntechnischen Bezug vor.

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-910548-09-1