Untersuchung von IT-Sicherheitsmaßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette

GRS - 776

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Untersuchung von IT-Sicherheitsmaßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette

Oliver Rest
Björn Becker
Henriette Gatz
Christian Korn
Claudia Quester
Alexander Schug

Dezember 2023

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4721R01630 durchgeführt.

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

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

GRS - 776
ISBN 978-3-910548-69-5

Deskriptoren

Cybersecurity, IT-Sicherheit, Lieferkette, Supply Chain, Supply-Chain-Attack

Kurzfassung

Der vorliegende Bericht umfasst Ergebnisse, die im Rahmen des vom Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz geförderten Forschungsvorhabens „Untersuchung von IT-Sicherheitsmaßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette“ (Förderkennzeichen 4721R01630) erarbeitet wurden. Die Zielsetzung dieses Vorhabens lag dabei in Analyse von bisher beobachteten IT-Angriffen im Zusammenhang mit der Lieferkette und der Untersuchung des entsprechenden Angriffspotentials auf kerntechnische Anlagen und Einrichtungen. Dazu wurden diverse IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette betrachtet und daraus Gemeinsamkeiten, unterschiedliche Arten von Angriffsmöglichkeiten und sich aus den betrachteten IT-Sicherheitsvorfällen ergebende generische Aspekte abgeleitet. Darüber hinaus wurden sowohl nationale wie auch internationale Regelwerke hinsichtlich der Vorgaben zur Sicherstellung der IT-Sicherheit in der Lieferkette untersucht und mit der deutschen Vorgehensweise verglichen. Zuletzt wurden generische Angriffsmuster im Zusammenhang mit der Lieferkette definiert, für die jeweils die Eignung und Wirksamkeit der im Vorhaben betrachteten Sicherungsmaßnahmen und die entsprechende Abdeckung im betrachteten Regelwerk untersucht wurde.

Abstract

This report contains results of a research project funded by the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (Promotion code 4719R01373). The goal of this project was to analyze so far observed cybersecurity incidents related to the supply chain and investigate the related potential for attacks on nuclear facilities. In this context, several cybersecurity incidents related to the supply chain were considered extracting commonalities, different attack possibilities and resulting generic aspects. Furthermore, national and international regulations were investigated regarding requirements to ensure cybersecurity of the supply chain and compared to the German approach. Finally, generic attack patterns related to the supply chain were defined. In the context of each of these generic attack patterns, the appropriateness and effectiveness of security measures considered in this research project were evaluated as well as the coverage of these measures in the analyzed regulations.

Inhaltsverzeichnis

Kurzfassung ..... **I**

1 Einleitung **1**

2 Kurzdarstellung des relevanten Standes von Wissenschaft und Technik **5**

3 Untersuchung des Potentials von IT-Angriffen im Zusammenhang mit der Lieferkette **11**

3.1 Bereits in der Voruntersuchung betrachtete IT-Sicherheitsvorfälle 12

3.1.1 IT-Sicherheitsvorfall in einem deutschen Kernkraftwerk 12

3.1.2 IT-Sicherheitsvorfall im Kernkraftwerk Monju 14

3.1.3 IT-Sicherheitsvorfall im Zusammenhang mit Ingérop 15

3.1.4 Cyberangriffe mit der Schadsoftware NotPetya 16

3.1.5 Cyberangriffe der APT-Gruppierung Dragonfly 18

3.1.6 Cyberangriff auf Target 22

3.1.7 IT-Sicherheitsvorfall im Zusammenhang mit MediaGet 23

3.1.8 ShadowHammer Cyberangriffe 25

3.1.9 Magecart Cyberangriffe 26

3.1.10 IT-Sicherheitsvorfall im Zusammenhang mit CCleaner 27

3.1.11 Operation Red Signature Cyberangriffe 29

3.1.12 Kingslayer Cyberangriff 30

3.2 Bisher nicht betrachtete IT-Sicherheitsvorfälle 31

3.2.1 Cyberangriffe mit der Schadsoftware Stuxnet 33

3.2.2 Cyberangriffe im Zusammenhang mit schadsoftwarebehafteten SolarWinds Produkten 38

3.2.3 Schwachstellen in Microsoft Exchange 43

3.2.4 Schwachstelle in Log4J 47

3.2.5 IT-Sicherheitsvorfall im Zusammenhang mit Kaseya 50

3.2.6 Cyberangriff auf CodeCov 53

3.2.7 IT-Sicherheitsvorfall in Zusammenhang mit NPM-Paketen 55
3.2.8 Cyberangriff auf Adesso 57
3.2.9 IT-Sicherheitsvorfall im Zusammenhang mit 3CX VoIP-Desktop App 59
3.2.10 Cyberangriffe auf Bitmarck 61

4 Analyse nationaler und internationaler Vorgehensweisen zur Sicherstellung der IT-Sicherheit in der Lieferkette 65
4.1 Nationales Regelwerk 66
4.1.1 Deutschland 66
4.1.2 Vereinigte Staaten 78
4.1.3 Großbritannien 90
4.1.4 Finnland 96
4.2 Internationales Regelwerk 98
4.2.1 IAEA 98
4.2.2 Normen 107
4.3 Vergleich des deutschen Regelwerks mit internationalen Vorgehensweisen 119

5 Generische Angriffsmuster und Untersuchung der Eignung und Wirksamkeit von Sicherungsmaßnahmen in Bezug auf die IT-Sicherheit in der Lieferkette 125
5.1 Betrachtung von Angriffsmöglichkeiten im Zusammenhang mit der Cybersicherheit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems 125
5.2 Gemeinsamkeiten und generische Aspekte der betrachteten IT-Sicherheitsvorfälle und abgeleitete Sicherungsmaßnahmen 129
5.3 Generische Angriffsmuster 134
5.3.1 Upstream-Angriffe 135
5.3.2 Midstream-Angriffe 138
5.3.3 Downstream-Angriffe 141
5.3.4 Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten 144

5.4 Eignung und Wirksamkeit von Sicherungsmaßnahmen zur Verhinderung, Detektion und Mitigation von IT-Angriffen im Zusammenhang mit der Lieferkette 146
5.4.1 Grundlegende Sicherungsmaßnahmen 147
5.4.2 Reaktive Sicherungsmaßnahmen und Forensik 148
5.4.3 Update- und Patchmanagement 149
5.4.4 Überprüfung von Code auf Schadsoftware 151
5.4.5 Maßnahmen zur Echtzeitüberwachung und Detektion 152
5.5 Abdeckung der Angriffsmuster und Sicherungsmaßnahmen durch betrachtetes Regelwerk 153

6 Zusammenfassung 159

Literaturverzeichnis 163

Abbildungsverzeichnis 181

1 Einleitung

Die Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH (GRS) befasst sich als Deutschlands zentrale Fachorganisation auf dem Gebiet der nuklearen Sicherheit mit Fragen zur Sicherheit und Sicherung kerntechnischer Anlagen und Einrichtungen. Einen wesentlichen Aspekt stellt in diesem Zusammenhang in der heutigen Zeit angesichts der fortgeschrittenen und weiter voranschreitenden Digitalisierung und einer damit einhergehenden immer größer werdenden Angriffsfläche einerseits und einer stetig wachsenden IT-Bedrohungslage andererseits die Sicherstellung der Informationssicherheit solcher Einrichtungen dar. Angesichts dessen zählt die Gewinnung wissenschaftlicher und technischer Erkenntnisse in den Bereichen der Sicherung und Informationssicherheit kerntechnischer Anlagen und Einrichtungen zu den zentralen Aufgabenstellungen der GRS. Neben der fortwährenden Beobachtung des Standes und der Entwicklung von Wissenschaft und Technik beteiligt sich die GRS durch Forschungsarbeiten im Rahmen diverser Eigen- und Auftragsforschungsprojekte an der Fortschreibung und Entwicklung des Standes von Wissenschaft und Technik in diesen Gebieten, um die Sicherheit und Sicherung kerntechnischer Anlagen in Deutschland zu verbessern.

In deutschen kerntechnischen Anlagen und Einrichtungen werden allgemein und in unterschiedlichem Ausmaß verschiedene Systeme zur digitalen Informationsverarbeitung sowie zur Steuerung von Systemen und Prozessen eingesetzt. Dies gilt sowohl für seit längerer Zeit bestehende Anlagen wie beispielsweise Kernkraftwerke, die im Laufe ihrer Betriebszeit mit entsprechenden Komponenten nachgerüstet wurden und werden, als auch für neuere Anlagen wie beispielsweise Brennelemente-Zwischenlager, die sich teilweise aktuell noch im Aufbau befinden. Es handelt sich dabei neben informationsverarbeitenden Systemen der Informationstechnik (IT) wie beispielsweise Büro-IT vermehrt auch industrielle Steuerungssysteme (industrial control systems, ICS) zur Überwachung und Steuerung verfahrenstechnischer Prozesse. Auch international sind solche Systeme insbesondere bei neu errichteten oder geplanten Kernkraftwerken im europäischen sowie globalen Ausland relevant. Im Folgenden werden Systeme der Informationstechnik wie beispielsweise Büro-IT und jegliche Art von programmgesteuerten Komponenten oder Systemen, insbesondere auch industrielle Steuerungssysteme, zusammengefasst als „IT-Systeme“ bezeichnet. Hierzu zählen auch rechnerbasierte oder programmierbare Komponenten oder Systeme, die durch externe Geräte konfiguriert oder parametriert werden können.

In den vergangenen Jahren sind in diesem Zusammenhang vermehrt Cyberangriffe auf IT-Systeme und sicherheitskritische Einrichtungen beobachtet worden, die mit der Lieferkette zusammenhängen. Zunehmend treten IT-Sicherheitsvorfälle[1] auf, bei denen bereits mit Schadsoftware infizierte IT-Systeme geliefert und eingebaut werden oder denen eine Verletzung der Informationssicherheit bei einem Zulieferer oder externen Dienstleister zugrunde liegt. Cyberangriffe im Zusammenhang mit der Lieferkette haben insgesamt für das Sicherheitsverständnis der Betroffen und die Angriffsmöglichkeiten der Angreifer in den letzten Jahren erheblich an Bedeutung gewonnen. Dabei gibt es neben der Manipulation von Hardware vor der Lieferung unterschiedliche Angriffsformen über die Lieferkette, wie beispielsweise das Einschleusen von Schadsoftware behaftetem Code in legitime Software, die Manipulation von Software-Updates oder die Kompromittierung von (IT-)Dienstleistungen von Drittherstellern. Betroffen sind nicht nur die Büro-IT, sondern auch industrielle Steuerungssysteme einschließlich betrieblicher Leittechnik und Sicherheitsleittechnik sowie/oder IoT (Internet of Things-) Geräte, die über das Internet verknüpft sind und Daten und Informationen austauschen.

Ein wirksamer Schutz von schutzbedürftigen IT-Systemen gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD) setzt die Auswahl und Definition von Sicherungsmaßnahmen voraus, welche mögliche Angriffspfade und Schwachstellen umfassend betrachten und deren potenzielle Ausnutzung verhindern, mitigieren oder detektierbar machen. Eine vollständige Betrachtung der Informationssicherheit eines IT-Systems ist daher nur möglich, wenn potenzielle Cyberangriffe im Zusammenhang mit der Lieferkette für jedes schutzbedürftige System mit betrachtet und entsprechende Sicherungsmaßnahmen ergriffen werden. In diesem Vorhaben werden dazu bisherige Cyberangriffe im Zusammenhang mit der Lieferkette analysiert und ihr Angriffspotential auf kerntechnische Anlagen und Einrichtungen untersucht, insbesondere hinsichtlich Sicherungsmaßnahmen, die in diesem Zusammenhang besonders relevant sind. Weiterhin werden einschlägige nationale und internationale Regelwerke bzgl. des Aspekts der Cybersicherheit im Zusammenhang mit der Lieferkette ausgewertet. Das Ziel ist dabei Identifikation von Vorgehensweisen und Sicherungsmaßnahmen, die Cyberangriffe im Zusammenhang mit der Lieferkette verhindern/mitigieren können sowie die Identifikation bisher nicht im Regelwerk adressierter Aspekte. Als Grundlage der Untersuchungen wird der aktuelle Stand von Wissenschaft und Technik herangezogen.

---

[1] Als IT-Sicherheitsvorfall gilt im Folgenden ein Vorfall, der die IT-Sicherheit in einer Weise beeinträchtigt, dass die Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) gefährdet sind und Rückwirkungen auf die Sicherheit oder Sicherung nicht ausgeschlossen werden können.

Mit den gewonnenen Erkenntnissen wird die Fachkompetenz der GRS auf dem Gebiet der Cybersicherheit langfristig erhalten und weiter ausgebaut. Außerdem bieten die gewonnen Erkenntnisse eine Grundlage für zukünftige sachgerechte Bewertungen zur Cybersicherheit von IT-Systemen in kerntechnischen Anlagen und Einrichtungen sowie für die fachliche Mitarbeit in nationalen und internationalen Gremien.

2 Kurzdarstellung des relevanten Standes von Wissenschaft und Technik

Digitale Komponenten und Systeme sind seit mehreren Jahrzenten essenzielle Bestandteile technologischen Fortschritts und dynamischer Entwicklungen. Die Einsatzgebiete sind vielfältig und erstrecken sich auf nahezu alle Lebensbereiche. Neben dem Einsatz von IT-Systemen und Komponenten, die in vielen Bereichen wie beispielsweise Kommunikation, Verwaltung, Unterhaltung, Handel und Industrie eingesetzt werden, ist für verfahrenstechnische Anlagen und kritische Infrastrukturen zunehmend der Einsatz von IT-Systemen in Form von speicherprogrammierbaren Steuerungen, Prozessleitsystemen und allgemein Systemen zur Prozessautomatisierung relevant. Auch in deutschen kerntechnischen Anlagen und Einrichtungen finden derartige Systeme vermehrt Anwendung, wobei vormals rein analoge Komponenten schrittweise oder vollständig ersetzt werden. International ist diese Entwicklung ebenfalls und ggf. in weitaus größerem Ausmaß und Umfang zu beobachten. Mit der Zunahme an digitalen Komponenten in diesem Bereich steigt auch kontinuierlich die entsprechende Angriffsoberfläche für eine Störmaßnahme oder sonstige Einwirkung Dritter auf diese Systeme. In den Fokus rückten derartige Cyberangriffe auf industrielle Steuerungssysteme vor allem im Rahmen des Stuxnet-Angriffs auf eine kerntechnische Anlage im Iran, der 2010 öffentlich bekannt wurde (siehe Abschnitt 3.2.1). Dabei hebt im Wesentlichen der Aspekt, dass durch eine Einwirkung auf programmierbare bzw. rechnerbasierte Systeme und Komponenten physische Schäden in der betroffenen Anlage hervorgerufen werden konnten die besondere Problematik derartiger Cyberangriffe hervor. Insbesondere seit dieser Zeit steht das Thema Cybersicherheit in kritischen Infrastrukturen vermehrt im Blickfeld aktueller Forschungen und ist ein zentraler Ansatzpunkt von Wissenschaft und Technik in diesem Bereich.

Die GRS hat das Thema Cybersicherheit von kerntechnischen Anlagen unter anderem Bereits mit den Weiterleitungsnachrichten 2010/07 *„Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7“* /GRS10r01/, 2016/08 *„Schadsoftwarefunde im Kernkraftwerk Gundremmingen, Block B“* /GRS16r01/ und 2021/01 *„IT-Angriffe auf kritische Infrastrukturen im Zusammenhang mit der Schadsoftware Triton/TriSIS“* /GRS21r14/ adressiert. Zudem wurde insbesondere angesichts des Stuxnet-Angriffs und der sich weiter verschärfenden IT-Bedrohungslage im Jahr 2013 vom damaligen Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU) 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-Richtline IT)“ /BMU13n03/ bekannt gemacht, in der die Cybersicherheit kerntechnischer Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter explizit adressiert wird. Im Jahr 2020 folgte mit Bekanntmachung zur „*Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III)“* /BMU20n02/ durch das BMU die entsprechende Richtlinie für kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III. Ein wesentlicher Bestandteil der Sicherungsmaßnahmen kerntechnischer Anlagen und Einrichtungen sowie generell kritischer Infrastrukturen in Deutschland im Zusammenhang mit der Cybersicherheit ist dabei zudem das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI), indem das Thema Informationssicherheit ausführlich adressiert ist.

Der Stand von Wissenschaft und Technik im Bereich der Informationssicherheit unterliegt dynamischen Entwicklungen und hat sich insbesondere in den letzten Jahren stark entwickelt. Die IT-Bedrohungslage für kerntechnische Anlagen und Einrichtungen in diesem Zusammenhang ist ebenso starken und dynamischen Entwicklungen unterworfen und wird von der GRS intensiv analysiert. Diesbezüglich veröffentlichte die GRS unter anderem in den Jahren 2021, 2022 und 2023 die GRS-Berichte /GRS21r16, GRS23r02, GRS24r01/ zur Entwicklung der IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen. Ein wesentlicher Aspekt der IT-Bedrohungslage stellt dabei das Thema Informationssicherheit im Zusammenhang mit der Lieferkette von Hardware und Software dar.

IT-Angriffe bzw. Cyberangriffe im Zusammenhang mit Lieferketten (Supply-Chains, weiterhin auch bezeichnet als Supply-Chain-Angriffe) haben mit der Digitalisierung und Internationalisierung der Lieferketten in den letzten Jahren stark zugenommen und sind für den Bereich Cybersicherheit hochgradig relevant. Aufgrund der zunehmenden Verwendung komplexer, digitaler Systeme sind Unternehmen, Anlagen und Organisationen in der Regel auf die Bereitstellung von Produkten, Daten und Programmen wie zum Beispiel hochspezialisierte Softwaresysteme durch externe Zulieferer angewiesen, die typischerweise nicht selbst vollständig verifiziert und auf ihre Integrität geprüft werden können. Die Möglichkeiten für IT-Angriffe im Zusammenhang mit der Lieferkette sind dabei vielfältig, beispielsweise durch die Manipulation von Hard- oder Software vor der Auslieferung an den Kunden oder die Manipulation von Software über Updates. Die steigende Komplexität von Software, Hardware und IT-Dienstleistungen in diesem Zusammenhang

bietet Angreifern insgesamt vielfältige Möglichkeiten, insbesondere innerhalb der Lieferkette von Komponenten oder Diensten. IT-Sicherheitsvorfälle der jüngeren Vergangenheit und insbesondere verschiedene Supply-Chain-Angriffe auf international aufgestellte Unternehmen bzw. Produkte, die weltweit große Aufmerksamkeit erfuhren, verdeutlichen die potenziell verheerenden Folgen derartiger Angriffe.

Grundsätzlich betrifft die Frage der IT-Sicherheit in der Lieferkette alle IT-Systeme, die in kritischen Infrastrukturen und kerntechnischen Anlagen und Einrichtungen eingesetzt werden. Dies beinhaltet sowohl Software- als auch Hardwarebestandteile. In der heutigen Zeit werden die Bestandteile der Software und Hardware in der Regel nicht vollständig von einzelnen Herstellern oder Unternehmen alleinig erzeugt bzw. hergestellt, sondern durch verschiedene und häufig mehrere Zulieferer bereitgestellt. Zudem sind nicht zwangsläufig alle Softwarebestandteile, die für ein IT-System erforderlich sind, lokal auf dem betreffenden IT-System vorhanden, sodass externe Softwarebestandteile erforderlich sind, die über entsprechende Abhängigkeiten eingebunden werden. Bei der Lieferkette eines IT-Systems kann es sich prinzipiell um eine einzelne, unverzweigte Verbindung zwischen einem Betreiber und einem beauftragten Unternehmen handeln. Sehr viel wahrscheinlicher ist in der heutigen Zeit jedoch, dass die Lieferkette eines IT-Systems von einer ganzen Reihe von Lieferketten und darin enthaltenen Hard- und Softwarebestandteilen abhängt, von denen jedes einzelne für sich allein genommen als Zwischenziel eines potenziellen IT-Angriffs dienen kann. Zudem sind Angriffe auf die Lieferkette eines IT-Systems nicht auf die „erste Lieferung“ eines IT-Systems bzw. seiner Komponenten beschränkt, sondern umfassen den gesamten Lebenszyklus. Dies beinhaltet u. a. neben der Konzeptions-, Entwurfs- und Entwicklungsphase auch 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 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 Sicherungsmaßnahmen vor Ort, sondern auch darüberhinausgehende Sicherungsmaßnahmen relevant, die den gesamten Lebenszyklus von Hard- und Softwarekomponenten eingesetzter IT-Systeme einschließen und permanent aktualisiert und an neue Erkenntnisse angepasst werden müssen.

Wie bereits diskutiert kommt IT-Dienstleistern im Zusammenhang mit Supply-Chain-Angriffen eine besondere Bedeutung zu. Dies ist im Wesentlichen darin begründet, dass IT-Angriffe auf derartige Unternehmen Angreifern potenziell eine Vielzahl möglicher Opfer bieten und somit die Auswirkungen eines einzelnen erfolgreichen Angriffs sich möglicherweise auf eine große Zahl mit dem IT-Dienstleister in Verbindung stehender Unternehmen erstrecken. Außerdem werden in der heutigen Zeit immer mehr Dienste und Dienstleistungen durch externe Unternehmen und Dienstleister bereitgestellt, wodurch sich die potenzielle Angriffsoberfläche fortwährend vergrößert. Sowohl für finanziell motivierte Angreifer wie auch auf Angreifer, deren Ziel die Einschränkung der Verfügbarkeit von Diensten und Dienstleistungen ist, bieten derartige Angriffe somit ein erstrebenswertes Kosten-Nutzen-Verhältnis. Zudem stellt für Angreifer, deren Motive Informationsdiebstahl und Spionage sind, ein IT-Angriff auf zentrale Dienstleister, die ggf. für mehrere Behörden oder Unternehmen tätig sind, ein lohnendes Ziel dar. Dies gilt sowohl für gezielte IT-Angriffe wie auch für ungerichtete IT-Angriffe, bei denen Angreifer kein spezifisches Angriffsziel im Auge haben (den IT-Dienstleister selbst oder ein damit in Verbindung stehendes Unternehmen). Zudem sind bei derartigen IT-Angriffen auf IT-Dienstleister nicht nur deren direkte Kunden betroffen, sondern potenziell auch Unternehmen und Einrichtungen, die selbst keine Beziehung zum angegriffenen Dienstleister haben,

deren Zulieferer und IT-Dienstleister jedoch eine entsprechende Verbindung zum Angriffsziel haben (siehe beispielsweise Abschnitt 3.2.5). Ansonsten gelten für Supply-Chain-Angriffe über bzw. auf IT-Dienstleister die gleichen oben genannten Aspekte, insbesondere hinsichtlich der potenziellen Umgehung von Sicherheits- und Sicherungsmaßnahmen sowie der Komplexität und Vielschichtigkeit der Lieferketten im Allgemeinen.

Generell gab es in den vergangenen Jahren wiederholt 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. 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 Sicherungsmaßnahmen 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.

Aufgrund der zunehmenden Relevanz der Thematik für die Cybersicherheit und der sich stetig wandelnden IT-Bedrohungslage in diesem Zusammenhang steht die IT-Sicherheit im Zusammenhang mit der Lieferkette national und international zunehmend im Fokus von Behörden und Sicherheitseinrichtungen. In den vergangenen Jahren wurden zahlreiche Regelwerke, Richtlinien und einschlägige Dokumente diese Thematik betreffend veröffentlicht. Der Aspekt wird auch in bereits bestehendem Regelwerk bzw. entsprechenden Normen zunehmend ausführlicher adressiert. Für Deutschland in diesem Zusammenhang relevante Dokumente werden in Abschnitt 4.1 diskutiert. Zudem werden in Abschnitt 4.2 internationale Dokumente beispielsweise von der Internationalen Atomenergie-Organisation (IAEA) bzw. entsprechende Normen hinsichtlich der für das Thema IT-Sicherheit in der Lieferkette relevanten Aspekte betrachtet. Darüber hinaus gibt es

diverse weitere relevante Veröffentlichungen zu diesem Thema von unterschiedlichen Institutionen wie der European Union Agency for Cybersecurity (ENISA) (GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY /ENI23r01/) oder IAEA (Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain /IAE22r01/). Die GRS hat in diesem Zusammenhang und als Voruntersuchung dieses Vorhabens bereits den GRS-Bericht 638 /GRS21r15/ veröffentlicht. Darin geht es um die initiale Untersuchung des aktuellen Standes der Wissenschaft und Technik im Zusammenhang mit der IT-Sicherheit in der Lieferkette. Neben einer Übersicht über IT-Angriffe im Zusammenhang mit der Lieferkette des letzten Jahrzehnts, die in Abschnitt 3.1 aufgegriffen und weitergehend analysiert wurde, befasst sich der Bericht zudem mit dem Bedeutungszuwachs der IT-Sicherheit in der Lieferkette und stellt die Bedeutung dieser Thematik für die Cybersicherheit von Unternehmen heraus.

3 Untersuchung des Potentials von IT-Angriffen im Zusammenhang mit der Lieferkette

Aufbauend auf der Voruntersuchung /GRS21r15/ wurden in einem ersten Schritt IT-Sicherheitsvorfälle analysiert, die im Zusammenhang mit der Lieferkette von IT-Systemen stehen. Neben IT-Sicherheitsvorfällen mit direktem Bezug zu kerntechnischen Anlagen wurden auch IT-Sicherheitsvorfälle ohne direkten kerntechnischen Bezug betrachtet, die entsprechende Rückschlüsse ermöglichen und für das Vorhaben mögliche relevante Erkenntnisse hervorbringen. Neben den zwölf bereits in der Voruntersuchung betrachteten IT-Sicherheitsvorfällen wurden insgesamt zehn bisher nicht untersuche IT-Sicherheitsvorfälle analysiert. Dabei wurde neben den eingesetzten IT-Angriffswerkzeugen, Schadsoftwarekomponenten und deren Wirkungsweise insbesondere Aspekte betrachtet, die wesentlich für den Lieferkettenaspekt des IT-Sicherheitsvorfalls sind. Dazu zählen mit Einzelheiten über die Entdeckung des IT-Sicherheitsvorfalls oder Cyberangriffs und zu Angriffshandlungen bzw. spezifischen Aspekten im Zusammenhang mit der Lieferkette insbesondere Informationen, die wesentliche Erkenntnisse für die Untersuchung präventiver und reaktiver Sicherungsmaßnahmen sowie Maßnahmen zur Detektion für die weiteren Arbeiten des Vorhabens liefern. Abschließend wurden direkte bzw. indirekte und potenzielle Auswirkungen analysiert und sowohl spezifische, bei den jeweiligen Vorfällen ergriffene, wie auch generische, aus den Vorfällen abzuleitende, Sicherungsmaßnahmen betrachtet. Naturgemäß sind die Etablierung und dauerhafte Einhaltung von einer breiten Auswahl an Sicherungsmaßnahmen in jedem Fall und für alle Arten von Cyberangriffen relevant. In diesem Kapitel werden dabei jedoch im Zusammenhang mit dem Sachverhalt besonders relevante Maßnahmen für die jeweiligen IT-Sicherheitsvorfälle genannt, die sich im Rahmen der jeweiligen Bearbeitung aufgrund von Besonderheiten der entsprechenden IT-Sicherheitsvorfälle ergeben, beispielsweise anhand von durch forensische Untersuchungen gewonnenen Erkenntnissen oder sich daraus ergebende Erfahrungen und Lehren. Diese Sicherungsmaßnahmen werden entsprechend jeweils für die IT-Sicherheitsvorfälle in Abschnitt 5.2 gesammelt aufgelistet, anhand von Gemeinsamkeiten gruppiert und in den darauffolgenden Abschnitten in Kapitel 5 aufgegriffen und weitergehend diskutiert. Je nach Umfang der verfügbaren Informationen zu den einzelnen IT-Sicherheitsvorfällen unterscheidet sich die Detailtiefe der nachfolgenden Abschnitte entsprechend. Für die Auswahl der im Rahmen des Vorhabens untersuchten IT-Sicherheitsvorfälle ist allgemein ein Zusammenhang mit der IT-Sicherheit in der Lieferkette von Software oder Hardware entscheidend. Dieser Zusammenhang kann sich auf verschiedene Umstände beziehen und ist beispielsweise nicht beschränkt auf

die Erlangung des initialen Zugriffs auf die Zielsysteme durch potenzielle Angreifer, der typischerweise ein wesentliches Ziel für Angreifer darstellt.

3.1 Bereits in der Voruntersuchung betrachtete IT-Sicherheitsvorfälle

In der Voruntersuchung /GRS21r15/ wurden bereits zwölf IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette betrachtet, die im Rahmen des Vorhabens weitergehend analysiert wurden. Insgesamt fünf IT-Sicherheitsvorfälle weisen dabei einen direkten Bezug zu kerntechnischen Anlagen und Einrichtungen auf, wobei es sich bei einem IT-Sicherheitsvorfall um ein Ereignis aus einer deutschen kerntechnischen Anlage handelt.

Im Folgenden werden die IT-Sicherheitsvorfälle kurz vorgestellt und insbesondere die Lieferkettenaspekte diskutiert. Für bereits in der Voruntersuchung betrachtete Aspekte der entsprechenden IT-Sicherheitsvorfälle und allgemeine Informationen wird auf /GRS21r15/ verwiesen. Die nachfolgenden Abschnitte zu den einzelnen IT-Sicherheitsvorfällen werden dabei zur Veranschaulichung der allgemeinen IT-Bedrohungslage hinsichtlich von Cyberangriffen im Zusammenhang mit der Lieferkette vorgestellt und zur Illustration des Vorgehens der Angreifer, der allgemeinen Auswirkungen und der für den Sachverhalt besonders relevanten Aspekte diskutiert. In Kapitel 5 werden die analysierten IT-Sicherheitsvorfälle und die daraus erlangten Erkenntnisse aufgegriffen und entsprechend der für das Vorhaben vorgesehenen Untersuchung der bekannten Vorgehensweisen, inwieweit potenzielle IT-Angriffe abgewehrt werden können, weitergehend analysiert.

3.1.1 IT-Sicherheitsvorfall in einem deutschen Kernkraftwerk

Verwendete Quelle(n): /VER16r01/

Kurzüberblick

Im Frühjahr 2016 meldete ein deutsches Kernkraftwerk im Rahmen der Meldepflicht gemäß Atomrechtlicher Sicherheitsbeauftragten- und Meldeverordnung (AtSMV), dass auf mehreren IT-Systemen der Anlagensicherung Schadsoftware gefunden wurde. Bei den betroffenen IT-Systemen handelt es sich um IT-Systeme, welche im äußeren und im inneren Sicherungsbereich eingesetzt wurden. Nach bisherigen Erkenntnissen wurde die Schadsoftware bereits bei der Installation eines IT-Systems im Jahr 2010 in das

Kernkraftwerk eingebracht und verteilte sich anschließend über Netzwerkverbindungen und mittels Wechseldatenträgern, sodass auch Systeme und Komponenten betroffen waren, die keine direkten Datentechnischen Verbindungen zueinander haben. Welche Unternehmen bzw. einzelnen Personen für die initiale Schadsoftwareinfektion verantwortlich ist, ließ sich im Rahmen der forensischen Analyse nicht mehr feststellen. Bei diesem Fall wurde handelt es sich mutmaßlich nicht um einen gezielten Angriff, sondern eine zufällige Infektion, die zu keiner Beeinträchtigung im Anlagenbetrieb führte. Es kam zudem generell zu keiner bekannten, direkten Auswirkung auf die IT-Systeme der Anlage.

Entdeckung des IT-Sicherheitsvorfalls

Aufgrund des Schadsoftwarefunds in einem anderen deutschen Kernkraftwerk wurde aufgrund einer Empfehlung der WLN 2016/08 ein Schadsoftwarescan für alle IT-Systeme der IT-Schutzbedarfsklassen „Hoch“ und „Sehr hoch“ im betroffenen Kernkraftwerk durchgeführt, woraufhin die Schadsoftwareinfektion der betroffenen Systeme entdeckt wurde.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Nach Angaben des Betreibers gelangte die Schadsoftware bereits während der Einrichtungsphase des IT-Systems der Anlagensicherung in das Kernkraftwerk und verteilte sich anschließend autonom über Wechseldatenträger und Netzwerkverbindungen auf weitere Systeme und Komponenten, was durch entsprechende Zeitstempel der Schadsoftwaredateien erkannt wurde. Die genauen Umstände der Schadsoftwareinfektion, wie das verantwortliche Unternehmen/ggf. verantwortliche Personen konnten nicht mehr identifiziert werden. Da die Infektion mutmaßlich nicht gezielt erfolgte, liegt vermutlich eine zufällige Infektion vor, bei der die betroffenen Komponenten entweder bereits beim Zulieferer vor Ort durch eine Verbindung ins Internet oder damit in Verbindung stehenden Systemen infiziert wurden oder auf dem Anlagengelände im Zuge der Einrichtung durch Fremdpersonal. Der Fall stellt dahingehend eine Besonderheit dar, dass er zeigt, dass bei Fragen zur IT-Sicherheit in der Lieferkette auch Aspekte nicht gezielter Angriffe bzw. zufälliger Infektionen, herbeigeführt durch bzw. bei Betroffenheit von Hersteller oder Dienstleister, relevant sind.

3.1.2 IT-Sicherheitsvorfall im Kernkraftwerk Monju

Verwendete Quelle(n): /CSI14r01, ENS20w01, HUM14w01, JAE14r01, JAT14r01, SOP14r01/

Kurzüberblick

Am 2. Januar 2014 wurde Schadsoftware auf einem Computer in der Warte des japanischen Kernkraftwerks Monju entdeckt. Der inzwischen stillgelegte Brutreaktor befand sich zu dieser Zeit bereits im Langzeitstillstand. Die Schadsoftware gelangte wahrscheinlich über den Update-Mechanismus eines Video-Wiedergabeprogramms auf einen Computer, der von den Mitarbeitern hauptsächlich für Büroarbeiten und zu Dokumentationszwecken genutzt wurde. Nach Angaben der japanischen Atomenergiebehörde handelt es sich bei den auf dem betroffenen Computer gespeicherten Daten um Ausbildungsberichte und Schulungsunterlagen für das Dienstpersonal und ähnliche administrative Dokumente, sowie um etwa 42.000 gespeicherte E-Mails. Eine Verbindung zur Steuerung oder Überwachung des Anlagenbetriebs bestand laut der vorliegenden Informationen nicht. Nach ersten Untersuchungen wurde festgestellt, dass die gefundene Schadsoftware vermutlich unwissentlich von einem Mitarbeiter der Anlage heruntergeladen wurde, der ohne Berechtigung ein Softwareupdate eines Video-Wiedergabeprogramms durchgeführt hatte.

Entdeckung des IT-Sicherheitsvorfalls

Der Angriff wurde durch einen Systemadministrator des Kernkraftwerks Monju entdeckt, der verdächtige Kommunikationsverbindungen eines Computers im Kontrollraum mit einem südkoreanischen Server bemerkte. Nachdem der betroffene Computer vom Netzwerk getrennt und untersucht wurde, stellte man am 3. Januar 2014 fest, dass eine externe Verbindung über 30-mal innerhalb von fünf Tagen hergestellt wurde.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Schadsoftware gelangte vermutlich über die Durchführung eines Softwareupdates des Video-Wiedergabeprogramms „GOM-Player“ auf den Computer des Kernkraftwerks. Dieses Programm ist insbesondere in Südkorea und Japan weit verbreitet. Nach Angaben des Herstellers der Software wurde der Update-Server des GOM-Players dahingehend manipuliert, dass vom ursprünglichen Update-Server eine Weiterleitung auf eine externe Seite erfolgt, woraufhin die reguläre Software des GOM-Players und zusätzlich

die Schadsoftware heruntergeladen wird. Nach bisherigen Informationen verschafften sich die Angreifer über eine PHP-basierte Webshell, versteckt in einer Bild-Datei, die sich mutmaßlich seit Oktober 2011 auf dem Host befand, Zugriff zum Netzwerk des Herstellers des GOM-Players.

Nach Ansicht von Experten war die kerntechnische Anlage nicht gezielt für einen Angriff ausgewählt worden, sondern wurde wahrscheinlich Opfer eines zufälligen Angriffs, der durch das unbedachte Vorgehen eines Mitarbeiters erst ermöglicht wurde.

3.1.3 IT-Sicherheitsvorfall im Zusammenhang mit Ingérop

Verwendete Quelle(n): /IBI21w01, ING19r01, HEI18r01, ZFK18r01/

Kurzüberblick

Im November 2018 wurde bekannt, dass Daten des französischen Baudienstleisters Ingérop zuerst teilweise im Internet aufzufinden waren und anschließend ein entsprechendes Datenpaket im Darknet[2] zum Kauf angeboten wurde. Ingérop arbeitet als Baudienstleister für den französischen Staat unter anderem an diversen nuklearen Bauprojekten wie dem französischen Endlagerprojekt Cigéo und bemüht sich fortwährend um weitere Bauprojekte aus dem Bereich der kritischen Infrastrukturen. Nach bisherigen Erkenntnissen wurde Ingérop im ersten Halbjahr 2018 Opfer eines entsprechenden IT-Angriffs, in dessen Folge insgesamt etwa 11.000 Dateien mit einer Gesamtgröße von 65 Gigabyte von den Angreifern gestohlen wurden. Zu den entwendeten Daten gehören Informationen zu verschiedenen Bauprojekten im Bereich der kritischen Infrastruktur, an welchen Ingérop beteiligt ist, sowie Mitarbeiterinformationen und E-Mail-Korrespondenzen. Nach bisherigen Kenntnissen sind auch Daten aus zwei nuklearen Anlagen in den veröffentlichten Dateien enthalten, welche Informationen zum geplanten Endlager für hochradioaktive Abfälle Cigéo im Department Meuse sowie zum Kernkraftwerk Fessenheim enthalten.

[2] Als Darknet werden Bereiche des Internets genannt, welche nicht im freien Netz öffentlich sind und somit nicht direkt gesucht werden können.

Entdeckung des IT-Sicherheitsvorfalls

Der NDR, die Süddeutsche Zeitung und Le Monde hatten im Darknet einen Datensatz von über 65 Gigabyte ausgewertet, der aus Dokumenten des Baudienstleiters Ingérop bestand. Ingérop bestätigte nach entsprechenden Medienanfragen den Datenverlust als Folge eines IT-Angriffs. Derzeit gibt es keine weitergehenden Informationen, ob bzw. wann und ggf. wie Ingérop vor der Berichterstattung durch die Medien von dem IT-Angriff Kenntnis erlangt hat.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Daten von Ingérop wurden nach bisherigen Erkenntnissen infolge eines Phishing-Angriffes auf Mitarbeiter entwendet, indem ein oder mehrere Mitarbeiter des Konzerns mittels fingierter E-Mails zur Installation der bisher nicht bekannten Schadsoftware verleitet wurde(n). Inwiefern Ingérop gezielt als Baudienstleister insbesondere für kerntechnische Anlagen in Frankreich bzw. generell für kritische Infrastrukturen als Angriffsziel ausgewählt wurde, lässt sich anhand der vorliegenden Informationen nicht abschließend beurteilen. Der Fall zeigt jedoch, dass Dienstleister für bestimmte Bereiche oftmals ein lohnenswertes Angriffsziel darstellen, insbesondere wenn die Angreifer auch finanzielle Interessen haben. Auch wenn wie in diesem Zusammenhang keine direkte informationstechnische (Daten)Verbindung besteht, können Angreifer aus erbeuteten Informationen Kapital schlagen oder diese zur Vorbereitung weiterer Angriffsschritte verwenden.

3.1.4 Cyberangriffe mit der Schadsoftware NotPetya

Verwendete Quelle(n): /BUS17w01, CNE18w01, CNN17w01, FAY18r01, GUA17w01, IJR19r01, KAS16r01, LAN19r01, LRL17t01, MIT21w02, NYT17w03, PRV17r01, WIR17r01/

Kurzüberblick

Am 27. Juni 2017 waren weltweit Unternehmen und Organisationen von einem massiven Ausfall ihrer IT-Infrastruktur betroffen. Die von Angreifern über ein maliziöses Softwareupdate der Steuerabrechnungssoftware M.E.Doc verbreitete Schadsoftware „NotPetya“ breitete sich global aus und zerstörte alle gespeicherten Daten der betroffenen Systeme. Innerhalb weniger Tage entstand ein geschätzter wirtschaftlicher Schaden von ca. 10 Milliarden Dollar weltweit für betroffene Unternehmen. Ursprünglich galt der Angriff mutmaßlich Firmen und Regierungsbehörden in der Ukraine, darunter die Post,

das Metrosystem in Kiew, ukrainische Banken und das ukrainische Stromnetzunternehmen Kievenergo. Durch die Aktivitäten internationaler Unternehmen in der Ukraine und durch die teilweise unkontrollierte Vervielfältigung, konnte sich die Schadsoftware jedoch jenseits der ursprünglichen Ziele weiterverbreiten. Im Kernkraftwerk Tschernobyl fiel beispielsweise unter anderem das System zur automatisierten Strahlungsmessung aus, sodass manuelle Messungen der Strahlenbelastung als Ersatzmaßnahme notwendig wurden. Nach bisherigen Informationen kam es zu keinen weiteren Einflüssen auf die Systeme der Anlage und mittels Backups wurde die Verfügbarkeit der betroffenen Computersysteme wiederhergestellt.

Dadurch, dass sich die Schadsoftware automatisiert in den betroffenen Netzwerken verbreite, wurden teilweise Firmennetzwerke vollständig zerstört bzw. mussten, um die Verbreitung zu stoppen, vollständig abgeschaltet werden. Betroffene Systeme und Backups wurden durch die Schadsoftware verschlüsselt ohne die Möglichkeit zur Entschlüsselung und waren somit unbrauchbar. Ein umfassendes Beispiel der Schadenswirkung von NotPetya ist in diesem Zusammenhang die Zerstörung des Firmennetzwerkes bei dem global agierenden Logistikunternehmen Maersk. Eine einzelne Niederlassung von Maersk in der Ukraine nutzte die Software M.E.Doc, über die das schadsoftwarebehaftete Softwareupdate verbreitet wurde. Von hier aus infizierte NotPetya das aus über 80.000 IT-Systemen bestehenden Netzwerk des Unternehmens, welches zu dieser Zeit aus über 100 das Netzwerk steuernden Hauptsystemen bestand. Durch NotPetya wurden bis auf ein einziges Hauptsystem, welches sich zum Zeitpunkt des Vorfalls in einem Flugzeug ohne Netzwerkverbindung befand, die Daten sämtlicher Hauptsysteme des Netzwerks zerstört. Ausgehend von diesem einen nicht betroffenem System und analogen Kopien von Informationen konnte Maersk sein Netzwerk innerhalb einiger Wochen wieder in Betrieb nehmen.

Entdeckung des IT-Sicherheitsvorfalls

Der IT-Angriff wurde zuerst von den Mitarbeitern der betroffenen Unternehmen bemerkt, als betroffene Systeme und Geräte spontan neu starteten und nach dem Neustart einen Sperrbildschirm anzeigten, der von einer weiteren Schadsoftware mit Namen Petya (Ransomware) bekannt ist. Auf diesem gaben die Angreifer bekannt, dass die Systemdaten verschlüsselt seien und forderten eine Zahlung von 300 Dollar in Bitcoins für die Entschlüsselung der Daten. Dies war jedoch nicht möglich. Zu den ersten von dem IT-Angriff betroffenen Unternehmen gehörte eine Niederlassung des Logistikunternehmens Maersk in der Ukraine und die (Staatliche Sparbank der Ukraine) Oschadbank, welche

die zweit größte Bank der Ukraine ist. Die Oschadbank informierte zunächst das IT-Sicherheitsunternehmen Information Systems Security Partners ISSP über den Angriff.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Im Frühling 2017 erlangten unbekannte Angreifer Zugriff auf die Server des Unternehmens Linkos Group und übernahmen unbemerkt die Kontrolle über die Updateserver des Unternehmens. Von hier aus verteilten die Angreifer eine Backdoor über die Updateroutinen des Programms M.E.Doc der Linkos Group auf IT-Systeme, welche das entsprechende Programm installiert hatten. M.E.Doc ist in der Ukraine weit verbreitet und wird auch von vielen in der Ukraine tätigen ausländischen Unternehmen und Konzerntöchtern verwendet. Die Angreifer luden auf allen betroffenen Systemen die Schadsoftware NotPetya mittels der installierten Backdoors hoch und aktivierten diese zeitgleich am 27. Juni 2017. Von diesen Initialsystemen aus verbreitete sich NotPetya weltweit.

3.1.5 Cyberangriffe der APT-Gruppierung Dragonfly

Die APT-Gruppierung Dragonfly führt seit einigen Jahren breit angelegte, langfristige IT-Angriffe auf kritische Infrastrukturen durch. Für den Erstzugriff auf die eigentlich anvisierten Ziele wählen die Angreifer häufig Angriffsvektoren über die Lieferkette. Es sind mehrere teilweise andauernde Angriffswellen durch Dragonfly auszumachen, wobei die erste bereits im Jahr 2011 startete und 2014 vom IT-Sicherheitsunternehmen Symantec aufgedeckt wurde. Angriffsziele der Gruppe Dragonfly sind hauptsächlich im Energiesektor angesiedelt. Unter den Opfern befinden sich Netzbetreiber, Kraftwerke, Hersteller, Zulieferer und Betreiber, darunter beispielsweise das US-amerikanische Kernkraftwerk Wolf Creek. Ein Großteil der angegriffenen Unternehmen und Institutionen, die diese Angriffe öffentlich gemacht haben, haben ihren Sitz in westlichen Industrieländern. Im Folgenden werden zwei IT-Sicherheitsvorfälle im Zusammenhang Dragonfly, die die Lieferkette betreffen, vorgestellt.

3.1.5.1 Dragonfly: Havex

Verwendete Quelle(n): /ARS14w01, BSI20i01, CIS14r01, DRA17r02, EWO20w01 FSE15w01, INS18r01, NET14w01, SEC14r01, SYM14r02, SYM17r02/

Kurzüberblick

Die erste Angriffswelle durch Dragonfly war hauptsächlich auf das Ausspähen technischer Informationen ausgerichtet, während es in der zweiten Angriffswelle verstärk auch um das Ausspähen betrieblicher Aspekte bis hin zu Abläufen und Personalhandlungen bei der Bedienung industrieller Steuerungssysteme geht.

Für die einzelnen Angriffsschritte ihrer komplexen und hochentwickelten IT-Angriffe setzt Dragonfly ein breites Spektrum an IT-Angriffswerkzeugen, Schadsoftwarekomponenten und Angriffstechniken ein. Vor allem während der ersten Angriffswelle setzte Dragonfly stark auf Supply Chain Angriffe unter Einsatz der Schadsoftwarekomponente Havex. Unabhängig von der letztlich installierten Schadsoftware nutzten die Angreifer hierbei drei Angriffsvektoren für die Kompromittierung der Zielsysteme, von denen einer direkt mit der Lieferkette im Zusammenhang steht. Dabei führte Dragonfly gezielte Supply Chain Angriffe durch, indem sie die Update-Seiten von Herstellern industrieller Steuerungssysteme kompromittierten und Schadsoftware in legitime, auf diesen Seiten zum Download bereitstehende Software-Updates für die Software industrieller Steuerungssysteme injizierten.

Entdeckung des IT-Sicherheitsvorfalls

Nach bisherigen Erkenntnissen wurden die IT-Angriffe nicht durchgeführt, um direkte Schäden zu verursachen. Es wird vermutet, dass sie als Vorbereitung weiterer Angriffe dienten. Mit der Entdeckung durch das IT-Sicherheitsunternehmen Symantec im Jahr 2014 und vor allem mit Bekanntwerden der dabei eingesetzten IT-Angriffswerkzeuge und Schadsoftwarekomponenten wurde die erste Angriffswelle weitgehend beendet. Über Einzelheiten bezüglich der Entdeckung durch Symantec liegen derzeit keine Informationen vor.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Der Einschätzung des IT-Sicherheitsunternehmens F-Secure zufolge nutzte Dragonfly bei der Kompromittierung der Herstellerwebseiten Schwachstellen in der Software, mit denen die Webseiten betrieben werden, aus. Anschließend ersetzten sie die legitimen, zum Download bereitstehenden Softwarepakete durch kompromittierte, mit ihrer Schadsoftware infizierten Versionen. Diese Art von Supply Chain Angriffen wird auch als Strategic Web Compromise bezeichnet. In dem hier beschriebenen Zusammenhang ist von mindestens drei IT-Sicherheitsvorfällen bei Zwischenzielen auszugehen. In allen drei

Fällen injizierten die Angreifer ihre Schadsoftwarekomponenten in Software-Updates, welche auf den zuvor kompromittierten Webseiten zum Download bereitgestellt waren. Die so manipulierten Software-Updates waren für die Firmen, die auf diese zum Download bereitgestellten Softwarepakete zugriffen, nicht von legitimen Softwarepaketen zu unterscheiden. Die jeweils zunächst unbemerkte Bereitstellung dieser manipulierten Softwarepakete führte zu einer erheblichen Zahl an Infektionen mit der darin enthaltenen Schadsoftware.

3.1.5.2 Dragonfly: Kompromittierte VPN-Zugänge

Verwendete Quelle(n): /BSI19i01, BSI20i01, CIS18r01, CIS20r02, CYC18w01, NCS18i01, NYT17w01, NYT18w02, NYT20w01, SYM14r02, SYM17r02/

Kurzüberblick

Nach Bekanntwerden der ersten Angriffswelle durch Dragonfly im Jahr 2014 wurden etwa ein Jahr lang nur wenige Aktivitäten der Angreifergruppierung beobachtet. Anfang 2015 begann eine zweite Welle an IT-Angriffen, ab 2017 wurden verstärkt Angriffe beobachtet. Ein Ende der zweiten Angriffswelle ist bislang noch nicht abzusehen. Das Bundesamt für Sicherheit in der Informationstechnik stufte im Mai 2020 die Bedrohung durch Dragonfly weiterhin als hoch ein /BSI20i01/. Das BSI hebt explizit hervor, dass Dragonfly *„auch dann in der Lage ist, aktuelle Schwachpunkte in der Umgebung zu identifizieren bzw. auszunutzen, wenn die Firmen selbst ein hohes Schutzniveau im Bereich der IT-Sicherheit umgesetzt haben“.* Dies schließt Supply Chain Angriffe mit der Kompromittierung schwächer geschützte Hersteller, Zulieferer und Dienstleister ein. Während der zweiten Angriffswelle nutzt Dragonfly verstärk Angriffstechniken, die auf Credential Harvesting, d. h. das Erbeuten von legitimen Zugangsdaten setzten. Diese Zugangsdaten nutzen die Angreifer beispielsweise bei Zwischenzielen in der Lieferkette, um sich Zugriff auf deren Netzwerke zu verschaffen. Darauf aufbauend legen die Angreifer beispielsweise lokale Accounts an, über die sie in der Folge Informationen ausspähen, autorisiert erscheinende Zugriffe auf die eigentlich anvisierten Ziele durchführen und Spuren verwischen. Ausgehend von der Kompromittierung eines Zwischenziels in der Lieferkette setzt Dragonfly häufig auch gängige IT-Angriffswerkzeuge im Bereich der VPN-Zugänge ein, um vom Zwischenziel aus das eigentlich anvisierte Ziel zu kompromittieren und beispielsweise Schadsoftware zur Etablierung von Backdoors einzuschleusen.

Das britische National Cyber Security Centre (NSCS) veröffentlichte im April 2018 eine gemeinsame Warnmeldung mit FBI und DHS, welche von einer breit angelegten Angriffswelle und der Kompromittierung von Firmen ausgeht, die in Zusammenhang mit industriellen Steuerungssystemen stehen. Es wird weiter davon ausgegangen, dass die angegriffenen Firmen einen Teil der Lieferkette für kritische Infrastrukturen bilden und wahrscheinlich Remote-Zugriff auf dort vorhandene, kritische Systeme besitzen. Die zweite Angriffswelle fokussiert sich insbesondere auf das Ausspähen von Informationen zum Betrieb und zur Bedienung von industriellen Steuerungssystemen, beispielsweise über das systematische Erfassen von Screenshots. Eine Manipulation der industriellen Steuerungssysteme wurde nach bisherigen Erkenntnissen bislang unterlassen. Dabei ist es den Angreifern gelungen, auf Dateien mit Bezug zu industriellen Steuerungssystemen oder deren Herstellern zuzugreifen. Kompromittiert wurden hierbei nicht nur allgemeine Informationen, sondern auch spezifische Informationen wie Zugriffs- und Konfigurationsdaten. Im Jahr 2017 wurde bekannt, dass auch mindestens ein Kernkraftwerk in den USA von den Dragonfly Angriffen betroffen war. Aus einem Bericht der New York Times, welcher sich vornehmlich auf Informationen des FBI und des DHS stützt, geht hervor, dass das US-amerikanische Kernkraftwerk Wolf Creek im Rahmen der Angriffswelle kompromittiert wurde. Ein Sprecher des DHS wird in diesem Zusammenhang mit der Aussage zitiert, es habe den Anschein, als seien die möglichen Auswirkungen der Kompromittierung auf administrative und geschäftliche Teile des Anlagennetzwerks beschränkt.

Entdeckung des IT-Sicherheitsvorfalls

Die zweite Angriffswelle wurde nicht aufgrund eines einzelnen IT-Sicherheitsvorfalls sondern von verschiedenen Stellen aufgrund einer Reihe von Kompromittierungen durch Dragonfly festgestellt.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Das BSI und auch die US-amerikanische CISA berichten, dass die Angreifer Dienste für Remote- Zugriffe wie VPN für ihre Zwecke instrumentalisieren und über die entsprechende Infrastruktur eines Zwischenziels gleich mehrere eigentlich anvisierte Ziele angreifen. Durch Verwendung erbeuteter Credentials sind diese Zugriffe zunächst nicht von legitimen Zugriffen zu unterscheiden. Erlangen die Angreifer so Zugriff auf das Netz eines eigentlich anvisierten Ziels, beginnen sie mit systematischem Ausforschen dieses Netzwerks. Laut BSI wurde die beschriebene Vorgehensweise des nicht autorisierten

Zugriffs mittels erbeuteter, legitimer VPN-Zugangsdaten bereits bei kompromittierten Unternehmen in Deutschland nachgewiesen. Bereits im Juni 2019 berichtete das BSI von einem IT-Sicherheitsvorfall im Rahmen dieser zweiten Angriffswelle, bei dem ein nicht näher genanntes Unternehmen über VPN-Zugänge von Zulieferern kompromittiert wurde. Hierzu beschafften sich die Angreifer Zugangsdaten von mindestens zwei verschiedenen Zulieferern. Mit diesen Zugangsdaten griffen die Angreifer nacheinander erfolgreich über VPN-Verbindungen auf das Netzwerk des eigentlich anvisierten Ziels zu und erweiterten ihre Rechte. Anschließend griffen sie auf im Netzwerk verfügbare Daten zu und exfiltrierten diese.

3.1.6 Cyberangriff auf Target

Verwendete Quelle(n): /CYA19w01, DSW14r01, WAP18r01, ZDN15r01/

Kurzüberblick

Für einige Wochen im November und Dezember 2013 wurde das amerikanische Einzelhandelsunternehmen Target Opfer eines IT-Angriffes, welcher über ein Unternehmen in der Lieferkette von Target initiiert wurde. Zu einem unbekannten Zeitpunkt vor dem 27. November 2013 erlangten die Angreifer dabei über einen Dienstleister von Target Zugriff auf das IT-Netzwerk des Unternehmens und konnten dort eine auf Kassensysteme spezialisierte Schadsoftware installieren. Am 27. November 2013 aktivierten die Angreifer ihre Schadsoftware und begannen Kredit- und Debitkarteninformationen der Kunden von Target abzugreifen. Am 13. Dezember 2013 informierte Target die Justizbehörden der USA über den IT-Angriff und am 15. Dezember 2013 wurde der Datendiebstahl nach Angaben des Unternehmens vollständig unterbunden. Bis dahin wurden über 100 Millionen Datensätze mit entsprechenden Zahlungsinformationen der Kunden gestohlen.

Die Angreifer nutzten im Rahmen des IT-Angriffes auf Target über die Lieferkette mehrere, zum Teil unbekannte IT-Angriffswerkzeuge und Schadsoftwarekomponenten und waren dabei in der Lage, sich Zugriff auf die Server von Target zu verschaffen. Den Veröffentlichten Informationen zufolge gab es frühzeitig, registriert durch netzwerktechnische Sicherheitssysteme, erste Anzeichen für einen Angriff, denen das Unternehmen jedoch zunächst nicht konsequent nachging.

Entdeckung des IT-Sicherheitsvorfalls

Der IT-Angriff wurde am 27. November 2013 gestartet und wurde drei Wochen später von Target entdeckt. Einzelheiten hierzu liegen derzeit nicht vor. Der Konzern informierte daraufhin am 13. Dezember 2013 das U.S. Justizministerium. Am 18. Dezember 2013 berichtete der Blogger Brian Krebs in einem Blog über den IT-Angriff, der von Target am Tag darauf bestätigt wurde und somit einer breiteren Öffentlichkeit bekannt wurde.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Zu einem unbekannten Zeitpunkt vor dem IT-Angriff führten die Angreifer eine gezielte Aufklärungskampagne zur Entdeckung möglicher Eintrittspunkte in das IT-Netzwerk von Target durch. Dabei oder darauf folgend führten die Angreifer in einem ersten Schritt eine auf Dienstleister, Zulieferer und Vertragspartner von Target abzielende Phishing-Mail-Kampagne durch, um Zugriff auf deren Systeme zu erhalten. Mit einer solchen E-Mail waren die Angreifer erfolgreich, sodass die Systeme eines lokalen Kühlsystemlieferanten mit einem Trojaner infiziert wurden. Damit waren die Angreifer in der Lage, die Login-Details für verschiedene Portale und Netzwerke mit Verbindung zu Target zu ermitteln. Obwohl der verwendete Trojaner zum Tatzeitpunkt von sämtlichen großen Antivirenprogrammen erkannt wurde, blieb er bei dem Vertragspartner unerkannt, da kein Antivirenprogramm mit Echtzeiterkennung eingesetzt wurde.

3.1.7 IT-Sicherheitsvorfall im Zusammenhang mit MediaGet

Verwendete Quelle(n): /BLE18w01, MSS17r01, MSS18r02, TOR18w01/

Kurzüberblick

Im März 2018 berichtete Microsoft von einem Schadsoftwarebefall bei rund 400.000 Nutzern innerhalb weniger Stunden überwiegend in Russland, der Türkei und der Ukraine. Ein laut Microsoft hochentwickelter Trojaner gelangte mutmaßlich über den Filesharing-Client „MediaGet“ des BitTorrent Filesharing-Protokolls auf die Rechner der Nutzer und installierte einen Krypto-Miner[3]. Die Software MediaGet wird von Microsoft als potenziell

[3] Beim illegalen Krypto-Mining installieren Angreifer unbemerkt eine spezielle Software auf dem Rechner des Opfers, die dann Krypto-Währung für sie generiert, indem sie die Rechenleistung des Rechners zur Transaktionsverarbeitung, Absicherung und Synchronisierung der Nutzer im Netzwerk ausnutzt. Die Opfer merken oftmals nichts von dem Angriff und den auf ihren Rechnern ausgeführten Prozessen.

unerwünschte Anwendung[4] eingestuft. Die Schadsoftware wurde mutmaßlich über den kompromittierten Update-Server der russischen Entwickler von MediaGet verteilt. Nach Angaben von Microsoft begannen die Täter mit den Vorbereitungen des Angriffs bereits Mitte Februar 2018 durch die Kompromittierung des Update-Servers von MediaGet. Der Befehl zur Aktivierung der Schadsoftware wurde ab dem 1. März 2018 gegeben und am 6. März 2018 wurde die massenhafte Vermehrung und Aktivierung von Microsoft bemerkt, wobei nach Angaben von Microsoft die Windows Defender Antivirus-Software über 80.000 Instanzen des Trojaners an diesem Tag registrierte und blockierte. Innerhalb der nächsten 12 Stunden wurden bereits über 400.000 Instanzen registriert. Innerhalb einiger Sekunden wurde der Angriff durch den Windows Defenders geblockt und nach wenigen Minuten wurden Mitarbeiter von Microsoft alarmiert. Am 7. März 2018 wurde eine entsprechende Sicherheitswarnung veröffentlicht und am 13. März 2018 folgte eine ausführliche Meldung nach eingehender Analyse des IT-Sicherheitsvorfalls und der Schadsoftware durch Microsoft.

Entdeckung des IT-Sicherheitsvorfalls

Der IT-Angriff wurde durch Microsoft, insbesondere durch automatisierte Tools des Windows Defender Systems, entdeckt. Es handelt sich dabei um einen Cloud-Dienst zur möglichst frühen Erkennung von IT-Angriffen, der ggf. teilweise erste Schritte zur Blockierungen von Verbindungen durchführen kann. Neben dem Schwachstellen- und Bedrohungsmanagement bietet der Dienst weitere Schutzmechanismen wie kontinuierliche Scans, um Bedrohungen zu erkennen und zu blockieren, sowie einen verhaltensbasierten, heuristischen und Echtzeit-Virenschutz. Bei entsprechender Erkennung von Bedrohungen werden neben automatischen Maßnahmen auch Alarmierungen abgesetzt. Somit wurde der MediaGet-Angriff zunächst automatisiert durch Microsofts Defender ATP entdeckt, woraufhin Mitarbeiter von Microsoft automatisch informiert wurden weitergehende Untersuchungen anstellten.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Einschleusung des schadsoftwarebehafteten Updates über die Lieferkette erfolgte nach Angaben des Herstellers von MediaGet über den Updateserver, auf den die

[4] Potenziell unerwünschte Anwendungen können laut Microsoft dazu führen, dass die Leistungsfähigkeit des Systems beeinträchtigt wird, unerwartete Werbung angezeigt wird oder ggf. fremde Software installiert wird, bei der es sich möglicherweise um Schadsoftware handelt.

unbekannten Angreifer Zugriff über eine Sicherheitslücke im Dienstleistungsprogramm „Zabbix“ erhielten. Bei der Software „Zabbix“ handelt es sich um ein Open-Source-Netzwerk-Monitoringsystem, welches der Überwachung von IT-Infrastrukturen dient. Welche Schwachstelle der Software die Angreifer genau ausnutzten, geht aus den verfügbaren Informationen nicht hervor. Die von den Angreifern modifizierte Datei „mediaget.exe“ beinhaltete die gleiche Funktionalität wie die originale, legitime Datei, jedoch erweitert um eine Backdoor. Der Angriff wurde insgesamt über mehrere Wochen vorbereitet, wobei die Manipulationen des Updates bereits im Februar begannen, bevor die Verbreitung der Malware im März initiiert und der breit angelegte Angriff am 6. März gestartet wurde. Microsoft vermutet zudem, dass eine Programmdatei von MediaGet im Rahmen des Angriffs mit einem gestohlenen Zertifikat eines Dritt-Softwareherstellers signiert wurde.

3.1.8 ShadowHammer Cyberangriffe

Verwendete Quelle(n): /KAS19r01, SEN19r01, TVE19w01, VIC19w01/

Kurzüberblick

Im März 2019 veröffentlichte das IT-Sicherheitsunternehmen Kaspersky Labs Informationen über einen bis zu diesem Zeitpunkt unbekannten Supply-Chain-Angriff im Zusammenhang mit dem Computerhersteller ASUSTeK Computer Inc. (ASUS), welcher im Folgenden ShadowHammer genannt wurde. Im Rahmen dieses Supply-Chain-Angriffs wurde eine schadhafte Version einer ursprünglich offiziellen Software auf der Webseite des Herstellers zur Nutzung für Kunden bereitgestellt, wodurch Schadsoftware auf die Endgeräte der Anwender verteilt wurde.

Nach bisherigen Erkenntnissen wurde ab Mitte bis Ende Juni 2018 die mit dem Schadcode versehene Software auf der Webseite des Herstellers verbreitet. Der Supply-Chain-Angriff wurde nach bisherigen Kenntnissen im November 2018 beendet oder unterbrochen, ohne dass Informationen von dem Angriff bekannt wurden. Als Ziel des Angriffs wurden von den Angreifern etwa 600 ausgewählte MAC-Adressen in der Schadsoftware angegeben. Erst bei Übereinstimmung der MAC-Adresse eines infizierten Systems mit den vorher festgelegten Zielen wurden in einem zweiten Schritt weitere Schadsoftwarekomponenten heruntergeladen. Zu den Opfern gehören insbesondere IT-Unternehmen aus der Volksrepublik China und den USA, sowie ein südkoreanisches Pharmaunternehmen. Von dem manipulierten Softwareupdate von ASUS waren möglicherweise weltweit über eine Millionen Nutzer betroffen.

Entdeckung des IT-Sicherheitsvorfalls

Am 29. Januar 2019 entdeckte Kaspersky Lab den Supply-Chain-Angriff. Zuvor hatte Kaspersky ein neues Software-Werkzeug zur Entdeckung von Supply-Chain-Angriffen entwickelt und es zu seinem Antivirenscanner hinzugefügt. Dieses Werkzeug untersucht Dateien auf anormale Programmcode-Fragmente und ist in der Lage Programmcode zu entdecken, der normale Rechenoperationen illegitim übernimmt. In der Folge entdeckte Kaspersky die Schadsoftware in ASUS-Updates. Am 30. Januar 2019 wurde ASUS von Kaspersky informiert. Einen Tag später konnte bestätigt werden, dass die aktuelle Version der ASUS-Software nicht manipuliert war. Ende März 2019 wurden die Erkenntnisse veröffentlicht.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Der erste Teil des Angriffs findet über die Lieferkette statt. Hierzu wurde auf der Webseite des Herstellers ASUS eine von den Angreifern modifizierte Version des ASUS Live Updaters Kunden des Unternehmens angeboten, welche eine Backdoor auf dem Zielrechner etabliert. Über diese wird die Schadsoftware weiter entpackt und gestartet. Die manipulierte Datei wurde zudem mit einem legitimen Zertifikat des Herstellers signiert, welches die Angreifer mutmaßlich gestohlen hatten. Es ist somit davon auszugehen, dass die Angreifer (beschränkten) Zugriff auf die Infrastruktur von ASUS hatten. Wie es den Angreifern gelang diesen Zugriff zu erlangen, kann mit den vorliegenden Informationen zu dem IT-Sicherheitsvorfall nicht abschließend geklärt werden.

3.1.9 Magecart Cyberangriffe

Verwendete Quelle(n): /ENI22w01, ITW19w01, RIS18r01, STR18r01/

Kurzüberblick

Der Begriff „Magecart“ bezeichnet eine bestimmte Art von Cyberangriffen bzw. in diesem Zusammenhang agierende Gruppierungen. Dabei handelt es sich um sogenannte Web-Skimming-Angriffe, die auf Online-Unternehmen bzw. Unternehmen mit Online-Diensten abzielen, um vertrauliche Informationen wie Zahlungs- bzw. Kreditkartendaten zu stehlen. Neben Magecart existieren auch andere Formen des Web-Skimmings. Bei Magecart wird typischerweise ein maliziöses JavaSkript auf einer Online-Shopping-Website platziert bzw. in die bestehende Softwarearchitektur integriert. Die Kunden- und Kreditkartendaten werden dann abgegriffen und an einen Server des Angreifers geschickt,

woraufhin die Angreifer die erbeuteten Informationen für illegitime Aktivitäten weiter einsetzen bzw. weiterverkaufen können. Insgesamt waren im Verlauf über mehrere Jahre mutmaßlich tausende Online-Shops von Magecart-Angriffen zwischenzeitlich betroffen. Zu den bekannteren gehören die Seiten des National Republican Senate Committee (USA) und die amerikanische Ticketagentur Ticketmaster. Größere Bekanntheit erlangte Magecart vor allem durch einen IT-Angriff auf die Fluggesellschaft British Airways im August/September 2018. Bei diesem Angreifer wurden die Namen, Rechnungsadressen, E-Mail-Adressen und Kreditkarteninformationen (teilweise inklusive der auf der Kreditkarten-Rückseite vermerkten CVV-Nummern) von mindestens 380.000 Kunden, welche die Website oder App der Fluggesellschaft genutzt haben, ausgespäht. Den Zugang zum Netzwerk von British Airways erlangten die Angreifer nach derzeitigen Informationen über einen legitimen kompromittierten Zugangsaccount eines mit dem Unternehmen verbundenem Frachtabfertigungsunternehmens.

Entdeckung des IT-Sicherheitsvorfalls

Oftmals werden derartige Cyberangriffe gar nicht oder sehr spät bevor die Opfer entsprechende Abbuchungen auf ihren Konten bemerken entdeckt. Der Angriff auf British Airways verlief zunächst unbemerkt und es dauerte zwei Monate, bevor das Unternehmen von einem Sicherheitsforscher auf das Problem aufmerksam gemacht wurde. British Airways ergriff daraufhin Abhilfemaßnahmen und informierte die britische Datenschutzaufsichtsbehörde, das Information Commissioner's Office (ICO).

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Generell wird bei Magecart üblicherweise ein maliziöses JavaSkript, in der Regel ohne Wissen des jeweiligen Online-Händlers, auf dessen Website eingeschleust. Die vom Käufer auf der Website eingegebenen Kundendaten werden kopiert und an einen Server des Angreifers weitergeleitet. Im Fall von British Airways kompromittierten die Angreifer ein British Airways-Netzwerkkonto, das auf einen Mitarbeiter des Frachtabfertigungsunternehmens Swissport ausgestellt war, bevor sie auf der Zahlungsseite der Fluggesellschaft eine Schadsoftware zum Abgreifen von Karten einschleusten.

3.1.10 IT-Sicherheitsvorfall im Zusammenhang mit CCleaner

Verwendete Quelle(n): /CIT17w01, INS18r01, IIT17w01, WIR18r01/

Kurzüberblick

Am 13. September 2017 veröffentlichten Analysten des IT-Sicherheitsunternehmens Cisco Talos die Warnung, dass die populäre Software CCleaner, ein kostenloses Programm zur Optimierung von Betriebssystemen, mit Schadsoftware versehen und seit mehr als einem Monat in dieser Form auf der offiziellen Webseite des Anbieters herunterladbar ist. Insgesamt 2,27 Millionen Nutzer haben die manipulierte Version von CCleaner heruntergeladen, ungefähr 1,65 Millionen IT-Systeme waren insoweit betroffen, dass dort die Schadsoftware an die Command and Control (C&C) Server der Angreifer Daten sendete. Lediglich bei insgesamt 40 Systemen von elf verschiedenen Unternehmen wurden zusätzlich die in der Schadsoftware enthaltenen Funktionalitäten genutzt, um eine weitere Payload, die zweite Stufe der Schadsoftware, zu installieren. Dies führte anschließend zum Download und zur Installation der dritten Payload, der Schadsoftware Shadowpad, einem umfassenden Kontroll- und Überwachungsprogramm. Insgesamt handelte es sich daher um einen sehr zielgerichteten IT-Angriff mit einer ausgewählten Zielgruppe. Der Fokus des Angriffs lag bei Technik- und Telekommunikationsunternehmen in Japan, den USA, Taiwan, Deutschland und Großbritannien.

Entdeckung des IT-Sicherheitsvorfalls

Am 13. September 2017 führten die Analysten von Cisco Talos einen Test ihrer neuen Erkennungstechnologie von Schadsoftware durch. Dabei wurde das Malware-Protection-System des Unternehmens durch die ausführbare Installationsdatei des CCleaner ausgelöst. Untersuchungen zeigten, dass der Programmcode der Installationsdatei zwar ein gültiges digitales Zertifikat des Herstellers aufwies, aber dennoch eine Payload beinhaltete. Am gleichen Tag informierte Cisco Talos den Anbieter des Ccleaner Avast, der die Version sofort aus dem Netz nahm.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Der IT-Angriff über die Lieferkette mittels der Software CCleaner begann am 11. März 2017. An diesem Tag erlangten die Angreifer erstmalig Zugriff auf die IT-Systeme des Herstellers von CCleaner, Piriform. Hierfür nutzten die Angreifer einen ihnen vorliegenden administrativen Zugriff über die bei Piriform eingesetzte Software TeamViewer, eine Software zur Steuerung und (Fern)Wartung externer PCs. Die Entwickler von CCleaner vermuten, dass diese Daten bei einem früheren Angriff auf Piriform in Erfahrung gebracht wurden. In den nachfolgenden Tagen erweiterten die Angreifer ihren Zugriff auf verschiedene IT-Systeme im Netzwerk von Piriform und installierten ihre

Schadsoftware Shadowpad auf diesen IT-Systemen, zu denen auch ein Build Server für die Software CCleaner gehörte. Zwischen April und Juli 2017 arbeiteten die Angreifer anschließend an einer eigenen Version des CCleaners, welche mit Schadsoftware manipuliert wurde. Am 18. Juli 2017 wurde Piriform von dem IT-Sicherheitsunternehmen Avast gekauft, insbesondere aufgrund von CCleaner, welcher in seiner Geschichte über 2 Milliarden Mal heruntergeladen wurde. Am 2. August 2017 ersetzten die Angreifer dann die auf den Servern von Avast vorliegende CCleaner-Version mit der mit Schadsoftware manipulierten Version des CCleaners.

3.1.11 Operation Red Signature Cyberangriffe

Verwendete Quelle(n): /CYA18w01, SEC18w01, TRM18w01/

Kurzüberblick

Vom 18. Juli 2018 bis 31. Juli 2018 wurden IT-Angriffe mit Namen Operation Red Signature gegen Unternehmen in Südkorea durchgeführt. Dazu kompromittierten die Angreifer einen Update-Server eines Anbieters für Remote-Support-Lösungen. Sobald eine Update-Anfrage an den Server von einer bestimmten IP-Adresse erfolgte, die in einer von den Angreifern vorgegebenen Liste von IP-Adressen enthalten war, lud der Update-Server einen Remote Access Trojaner vom Server der Angreifer auf das Zielgerät. Der Trojaner stellte eine persistente Verbindung zum Server der Angreifer her und lud weitere Schadsoftwarekomponenten von diesem herunter. Das Ziel der Angriffe war der Diebstahl von sensiblen Daten der betroffenen Unternehmen. Offenbar gingen die Angreifer dabei sehr zielgerichtet vor, da sie Operation Red Signature bereits am 31. Juli 2018, genau zwei Wochen nach Beginn der Angriffe, selbstständig beendeten. Der Zeitpunkt für die Deaktivierung der Schadsoftware war im Programmcode der Schadsoftware bereits vorgegeben. Bei den Angriffszielen handelt es sich nach aktuellem Kenntnisstand ausschließlich um Unternehmen in Südkorea. Welche Unternehmen genau von den Angriffen betroffene waren und welche Auswirkungen diese hatten ist zurzeit nicht bekannt.

Entdeckung des IT-Sicherheitsvorfalls

Mitarbeiter der IT-Sicherheitsorganisation Trend Micro und von IssueMakersLab haben die Angriffe Ende Juli 2018 entdeckt. Die Medien berichteten am 6. August über die

Entdeckung. Es liegen derzeit keine detaillierten Informationen vor, wie genau die IT-Angriffe entdeckt wurden.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Angreifer versahen die von ihnen eingesetzte Schadsoftware mit einem gültigen, digitalen Zertifikat, dass sie zuvor gestohlen hatten. Danach luden sie die Schadsoftware auf einen Command-and-Control-Server (C&C) mit IP-Adresse 207.148.94.157 hoch und kompromittierten einen Update-Server eines Anbieters von Remote-Support-Lösungen. Anschließend wurde die Konfiguration des Update-Servers von den Angreifern so verändert, dass die Schadsoftware nur an Unternehmen mit spezifischen IP-Adressen übermittelt wurde. Stellte ein Nutzer mit passender IP-Adresse eine Update-Anfrage an den Update-Server, lud dieser die Schadsoftware vom C&C-Server der Angreifer und sendete sie an den Nutzer weiter.

3.1.12 Kingslayer Cyberangriff

Verwendete Quelle(n): /ITW17w01, KRE17w01/

Kurzüberblick

Bei Kingslayer handelt es sich um einen 2016 bekannt gewordenen Supply-Chain-Angriff, der die Software „EvLog 3.0“ betraf. Die betroffene Software ist ein Windows Eventlog Analyzer der Firma „Altair Technologies“ zur Analyse von Windows Event Logs, die unter anderem von Systemadministratoren überwiegend größerer Organisationen genutzt wird. Im April 2015 war die über einen Softwareanbieter bereitgestellte Version von „EvLog 3.0“ mit Schadsoftware kompromittiert, sodass jeder, der zu dieser Zeit die Software heruntergeladen hat, betroffen war. Da zudem der Updateserver betroffen war erhielten alle Anwender, die Updates für bereits installierte Software vom Hersteller heruntergeladen haben, die kompromittierte Software, die abseits der Kompromittierung vollständig funktionsfähig war. Es ist nach derzeitigen Informationen nicht bekannt, welche Unternehmen bzw. Nutzer konkret von der Kompromittierung von EvLog betroffen waren. Zu den möglichen Nutzern der infizierten Software gehören unter anderem Telefonanbieter, westliche militärische Organisationen, Rüstungsunternehmen, westliche Regierungsorganisationen, Banken und Finanzinstitute sowie Hersteller von IT-Produkten oder Anbieter von IT-Dienstleistungen. Nach erfolgreicher Installation wurde ein zweites Schadprogram heruntergeladen, das als Command-and-Control-Server

fungierte. Zudem wurden weitere Schadsoftwarekomponenten ausgeführt, beispielsweise zum Stehlen gespeicherter Passwörter gängiger Browser wie Google Chrome und Mozilla Firefox.

Entdeckung des IT-Sicherheitsvorfalls

Während einer nicht mit diesem IT-Sicherheitsvorfall in Verbindung stehenden anderen Untersuchung entdeckte das auf IT-Sicherheit spezialisierte Unternehmen „RSA Research“ nicht identifizierbare periodische digitale Signale im Zusammenhang mit zum damaligen Zeitpunkt als maliziös bekannten Domains. Nach diesen Entdeckungen wurden ein gezieltes Monitoring und forensische bzw. weiterführende Analysen diesbezüglich, sowie Reverse Engineering Versuche durchgeführt. Es stellte sich heraus, dass die Software EvLog 3.0 im April 2015 mit Hilfe von Schadsoftware manipuliert und scheinbar legitim signiert vom Hersteller verteilt wurde. Dabei waren sowohl Updates wie auch die Vollversion des Programms betroffen.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Der nicht genannte Softwareanbieter unterhält mehrere Websites für den Download von Software und zum automatischen Update der Anwendungen. Während der Zeit, in der diese Websites kompromittiert waren, erhielt jeder Nutzer bei Neuinstallation oder einem (automatischen) Update von EvLog die maliziöse Version der Software. Hierzu wurde unter anderem eine Weiterleitung auf eine Website des Angreifers genutzt. Zudem wurden Teile der Schadsoftware mit gestohlenen legitimen Zertifikaten signiert, wobei derzeit keine Informationen vorliegen, wie die Angreifer in den Besitz dieser Zertifikate gekommen sind. Es stellte sich nach den Untersuchungen des Vorfalls heraus, dass die Paketverwaltung des Softwareanbieters kompromittiert worden war und vom 09. April 2015 bis zum 25. April 2015 kompromittierte Dateien ausgeliefert hatte. Die eigentliche Verteilung der kompromittierten Software erfolgte somit über einen Zeitraum von etwa zwei Wochen, wobei davon auszugehen ist, dass der Angriff schon früher begann und sich die Angreifer über einen unbekannten Zeitraum unbemerkt im Netzwerk ihres Opfers aufhielten.

3.2 Bisher nicht betrachtete IT-Sicherheitsvorfälle

Zusätzlich zu den bereits in der Voruntersuchung /GRS21r15/ betrachteten IT-Sicherheitsvorfällen wurden im Rahmen des Vorhabens insgesamt zehn weitere IT-

Sicherheitsvorfälle analysiert, die im Zusammenhang mit der Lieferkette stehen. Dabei handelt es sich einerseits um neuere Vorfälle aus den letzten Monaten und Jahren, sowie um Vorfälle die bereits längere Zeit zurück liegen, zu denen in letzter Zeit jedoch weitergehende Informationen veröffentlicht wurden, die im Rahmen des Vorhabens relevante Aspekte betreffen. Von diesen analysierten IT-Sicherheitsvorfällen weisen zwei einen direkten kerntechnischen Bezug auf. Die restlichen acht betrachteten IT-Sicherheitsvorfälle weisen keinen direkten Bezug zu kerntechnischen Anlagen und Einrichtungen auf, jedoch ergeben sich insbesondere durch das Ausmaß der jeweiligen Auswirkungen bzw. die Verbindung zu kritischen Infrastrukturen relevante Erkenntnisse bzgl. derartiger IT-Sicherheitsvorfälle, die auch in Bezug auf kerntechnische Anlagen und Einrichtungen interessant sich und entsprechend übertragbare Aspekte beinhalten. Die Auswahl der im Rahmen des Vorhabens betrachteten IT-Sicherheitsvorfälle erfolgte dabei anhand verschiedener Kriterien. Einerseits wurden IT-Sicherheitsvorfälle betrachtet, die durch ihr Ausmaß, ihre Komplexität und die globalen Auswirkungen eine besondere Bedeutung für Fragen zur IT-Sicherheit im Zusammenhang mit der Lieferkette haben. Das relevanteste Beispiel ist in diesem Zusammenhang der IT-Angriff auf Solar Winds (siehe Abschnitt 3.2.2). Andererseits wurden insbesondere IT-Sicherheitsvorfälle im Zusammenhang mit externen Komponenten, Diensten, Dienstleistern und Abhängigkeiten ausgewählt, da IT-Angriffe auf diese Bereiche der Lieferkette in den letzten Jahren stark zugenommen haben und vermehrt im Fokus der Angreifer stehen. Zudem wurden insgesamt kürzlich aufgetretene IT-Sicherheitsvorfälle betrachtet, sowie IT-Angriffe auf Ziele der Lieferkette, bei denen jeweils bereits die eigene Lieferkette kompromittiert war.

Im Folgenden werden die IT-Sicherheitsvorfälle kurz vorgestellt und insbesondere die Lieferkettenaspekte diskutiert. Im Vergleich zu den in Abschnitt 3.1 betrachteten IT-Sicherheitsvorfällen liegen zu den nachfolgend vorgestellten IT-Sicherheitsvorfällen keine Vorarbeiten mit Relevanz für dieses Vorhaben vor, sodass zusätzlich zu den in Abschnitt 3.1 diskutierten Aspekten im Zusammenhang mit der Lieferkette, dem allgemeinen Kurzüberblick und den im Zusammenhang mit dem Sachverhalt besonders relevante Aspekten außerdem weitergehende Informationen genannt werden, die zur Einordung des IT-Sicherheitsvorfalls und der Relevanz für das Vorhaben insgesamt hilfreich sind. Dazu zählen insbesondere Einzelheiten zu den eingesetzten Schadsoftwarekomponenten, Angriffswerkzeugen und ggf. ausgenutzten Schwachstellen. Dabei ist zu beachten, dass sich die verfügbaren Informationen zu den einzelnen IT-Sicherheitsvorfällen von Fall zu Fall unterscheiden und insbesondere für die im letzten Jahr vorliegenden Fälle, bei denen die Untersuchungen jeweils teilweise noch andauern bzw. nicht vollständig

abgeschlossen sind, die Informationslage ggf. eingeschränkt ist oder bisher nur wenige Informationen veröffentlicht wurden.

Die nachfolgenden Abschnitte zu den einzelnen IT-Sicherheitsvorfällen werden dabei wie in Abschnitt 3.1 zur Veranschaulichung der allgemeinen IT-Bedrohungslage hinsichtlich von Cyberangriffen über die Lieferkette vorgestellt und zur Illustration des Vorgehens der Angreifer, der allgemeinen Auswirkungen und der im Zusammenhang mit dem Sachverhalt besonders relevanten Aspekte diskutiert. In Kapitel 5 werden die analysierten IT-Sicherheitsvorfälle und die daraus erlangten Erkenntnisse aufgegriffen und entsprechend der für das Vorhaben vorgesehenen Untersuchung der bekannten Vorgehensweisen, inwieweit potenzielle IT-Angriffe abgewehrt werden können, weitergehend analysiert.

3.2.1 Cyberangriffe mit der Schadsoftware Stuxnet

Verwendete Quelle(n): /IRW15w01, SEC14w02/

Kurzüberblick

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 die nicht so stark verbreiteten 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. Die nachfolgenden Beschreibungen beziehen sich ausschließlich auf diese Varianten von Stuxnet. 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 wird hier nicht näher beschrieben. Auf weitere Varianten der Schadsoftware Stuxnet wird ebenfalls nicht eingegangen.

Bei Stuxnet handelt es sich insgesamt um hochentwickelte, ausgefeilte Schadsoftware, die auf die gezielte Manipulation von industriellen Steuerungssystemen ausgerichtet ist. Dabei handelt es sich nicht nur um die erste entdeckte Schadsoftware dieser Komplexität, Stuxnet ist in vielen Aspekten bis heute anderen Angriffswerkzeugen und Schadsoftwares voraus. So erreichte Stuxnet über einen langen Zeitraum das mutmaßliche Ziel der Angreifer – die Manipulation der Urananreicherung in der iranischen Anlage Natanz – ohne dabei entdeckt zu werden. Vielmehr kam es langfristig zu erheblichen physischen Schäden in der Anlage, wobei die eigentlichen Manipulationen so ausgeführt waren, dass ihre unmittelbaren Auswirkungen nicht zum Ansprechen von Schutzfunktionen führten. Es gelang den Angreifern, mehrere Varianten ihrer Schadsoftware, in die isolierten IT-Systeme von Natanz einzuschleusen. Hierbei wird – mit Ausnahme von Stuxnet 0.5 – nicht von der Mithilfe eines wissentlich agierenden Innentäters, sondern vielmehr von einem Überspringen von Air Gaps durch Kompromittierung der Lieferkette ausgegangen. Im Gegensatz zu vielen seither bekannten komplexen Schadsoftwarekomponenten ist Stuxnet zwar prinzipiell in der Lage, einen Kommunikationsweg zu den IT-Angreifern aufzubauen und Befehle entgegenzunehmen, kann aber auch vollständig autonom agieren und ist nicht auf das Nachladen weiterer Payloads angewiesen. Die IT-Systeme in der iranischen Atomanreicherungsanlage in Natanz besitzen beispielsweise keinerlei Verbindung zum Internet und sind vollständig isoliert.

Die Manipulation von Motoren war nicht die einzige Aufgabe von Stuxnet. Zusätzlich beinhaltete die Schadsoftware auch eine Funktionalität zum Ausspionieren von Informationen. Die Varianten A, B und C von Stuxnet besitzen darüber hinaus die Funktionalität, eine Kommunikationsverbindung aufzubauen und die ausspionierten Informationen weiterzugeben. Es ist davon auszugehen, dass diese Funktionalität zum Ausspionieren und Ausschleusen von Informationen vor allem für die frühen Angriffsschritte innerhalb der Lieferkette relevant war.

Entdeckung des IT-Sicherheitsvorfalls

Im Juni 2020 entdeckten Analysten der weißrussischen Firma VirusBlokAda eine Instanz der Stuxnet Variante B auf einem iranischen Rechner. Dieser Rechner wies keinerlei Verbindungen zur Urananreicherungsanlage in Natanz auf, es handelte sich vielmehr um eine durch unerwünschte Ausbreitung erfolgte Infektion. Von diesem Zeitpunkt an dauerte es noch Monate, bis es schließlich gelang, die Funktionsweise von Stuxnet vollständig zu entschlüsseln und dadurch Rückschlüsse auf die Zielsetzung der Schadsoftware zu ziehen.

Die Varianten A, B und C von Stuxnet besaßen alle Funktionalitäten zur Ausbreitungsbegrenzung. So enthält die Schadsoftware beispielsweise ein Datum, ab dem keine weitere Ausbreitung erfolgen darf. Zusätzlich ist festgelegt, dass jede Stuxnet-Instanz höchstens drei Kopien von sich selbst anfertigen darf. Für hochspezialisierte, verdeckt agierende Schadsoftware besteht der ideale Fall darin, ausschließlich die Zielrechner in der Zielanlage zu infizieren, da mit jedem infizierten Rechner auch die Chance auf eine Entdeckung der Schadsoftware größer wird. Dies ist zwar bei Einschleusung der Schadsoftware über einen entsprechenden Innentäter denkbar, aber weder bei einem IT-Angriff von außen noch – wie im Fall der Stuxnet Varianten A, B und C – bei einer Einbringung über die Lieferkette möglich. Stuxnet verbreitete sich letztlich über die Lieferkette sowohl in die anvisierte Anlage hinein als auch weltweit.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Stuxnet beinhaltet zahlreiche Komponenten und Funktionalitäten. Darunter befinden sich Exploits für mehrere Zero-Day-Schwachstellen, bereits bekannte Schwachstellen und übliche Fehlkonfigurationen, Funktionalitäten für Verbreitung, Evasion, Kommunikation und Logging sowie zwei Rootkits zum Verschleiern der Infektion bzw. der vorgenommenen Manipulationen. Darüber hinaus finden sich Schadsoftwarekomponenten zum Ausspähen von Informationen. Das eigentliche Herzstück ist eine Schadsoftwarekomponente zur Infektion und Modifikation von speicherprogrammierbaren Steuerungen (SPS).

Stuxnet sucht auf infizierten Systemen gezielt nach SCADA-Systemen, die SIMATIC WinCC/SIMATIC PCS7 von Siemens zur Konfiguration von SPS einsetzen. Sind diese vorhanden, greift Stuxnet in den Datentransfer zwischen der Programmiersoftware Step 7 und der SPS ein. Dabei ist Stuxnet in der Lage, den Schreib- und Lesezugriff auf die SPS zu überwachen, selbst unbemerkt Code auf die SPS zu scheiben und diesen maliziösen Code wiederum vor Veränderung zu schützen. Die Infektion und Modifikation der SPS erfolgt hierbei durch Austausch bzw. Hinzufügen von Codeblöcken, was die Implementierung neuer Funktionen ermöglicht. Für den Benutzer ist dabei selbst bei Auslesen des Programmcodes nicht erkennbar, ob eine SPS modifiziert wurde, da die .dll zum Austausch von Codeblöcken so wirkt, dass die SPS den maliziösen Code „sieht“, wohingegen der Workstation noch den ursprünglichen Code „liest“.

Eine SIMATIC S7-Steuerung besteht typischerweise aus Organisationsbausteinen (zyklische Abarbeitung), Systemdatenbausteinen (Daten zum Aufbau der Steuerung), DB:

Datenbausteinen (Datenstruktur der Programme) und Funktionsbausteinen mit Programmcode. Der Organisationsbaustein OB1 ist der Einstieg für jedes Programm, die anderen Bausteine werden in der Reihenfolge ihres Aufrufs abgearbeitet. Stuxnet platziert Schadcode direkt am Anfang von OB1, so dass der Schadcode immer zuerst gelesen wird. Stuxnet gleicht die Konfiguration der infizierten SPS mit der Konfiguration der anvisierten SPS ab. Hierbei sucht Stuxnet unter anderem nach einem speziellen Funktionsbaustein und spezifischen Modulen bei den Systemdatenbausteinen, welche über Ansteuerung von Frequenzumformern die Drehgeschwindigkeiten von Motoren regeln können.

Es ist sinnvoll, die Wirkungsweise dieser Manipulation aus drei verschiedenen Richtungen zu betrachten:

- **Wirkungsweise in Bezug auf die Leittechnik**: Die Manipulationen an den verfahrenstechnischen Komponenten der Stuxnet Varianten A, B und C veränderten in erratischen Abständen kurzzeitig die Drehgeschwindigkeiten der Motoren für die Zentrifugen. Konkret wird nach einem einleitenden Beobachtungszeitraum die Frequenz von 807 bis 1210 Hz (dieser Bereich ist notwendig für den Betrieb von Zentrifugen) kurz auf 1410 Hz erhöht und anschließend auf 2 Hz abgebremst. Dieser Vorgang wird dann in unregelmäßigen Abständen von 13 Tagen bis 3 Monaten wiederholt. Die Herauf- bzw. Herabsetzung der Drehgeschwindigkeit der Motoren erfolgte dabei jeweils nur so kurz, dass die resultierenden Abweichungen der im verfahrenstechnischen Prozess notwendigen Drehgeschwindigkeiten der Zentrifugen unterhalb der Ansprechwerte der Sicherheitsleittechnik lagen.

- **Wirkungsweise in Bezug auf die verfahrenstechnischen Komponenten:** Häufiges, abruptes und kurzzeitiges Abbremsen bzw. Beschleunigen bedeutet für die beteiligten verfahrenstechnischen Komponenten u. a. mechanischer Stress, der zu Schäden führt. Es wird angenommen, dass aufgrund der Stuxnet Varianten A, B und C bis zu 2000 Zentrifugen in Natanz ausgetauscht werden mussten.

- **Wirkungsweise in Bezug auf das hergestellte Produkt:** Das Abbremsen der Zentrifugen während des Anreicherungsproduktes führt in gewissem Umfang wieder zu einer Vermischung der bereits entmischten Bestandteile. Als Resultat ist das Uran am Ende des Vorgangs weniger hoch angereichert. Die von den Stuxnet Varianten A, B und C etablierten Manipulationen beeinträchtigen daher auch die Qualität des hergestellten Produkts.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Schadsoftware Stuxnet besitzt eine besondere Eigenschaft, die es ermöglicht, Infektionspfade und Angriffsvektoren leichter nachzuvollziehen: In einem internen Log speichert Stuxnet chronologisch Namen, Windows Domains und IP-Adressen der auf dem bisherigen Infektionspfad infizierten IT-Systeme. Bei jeder auf einem IT-System aufgefundenen Stuxnet Instanz lässt sich aus diesem internen Log also ablesen, welchen Weg die Schadsoftwarekomponente bis zu diesem IT-System genommen hat. Auch lässt sich nachvollziehen, welche IT-Systeme initial infiziert waren, d. h. von welchen IT-Systemen die Infektion die Ausbreitung begann. Die IT-Sicherheitsfirmen Symantec und Kaspersky werteten beide diese internen Logs aus. Allein Kaspersky zog dazu mehr als 2000 aufgefundene Instanzen von Stuxnet heran und konnte sehr zuverlässig die von den in den Jahren 2009 bzw. 2010 verbreiteten Stuxnet Varianten (Variante A im Jahr 2009 und Varianten B bzw. C im Jahr 2010) initial infizierten Firmen identifizieren.

Bei einer der von Variante A initial infizierten Firma handelt es sich um das iranische Unternehmen Foolad Technic Engineering Co., das industrielle Steuerungssysteme herstellt, die beispielsweise in der iranischen Stahlindustrie und bei Energieerzeugern eingesetzt werden. Sie stellt beispielsweise Datenaustausch zwischen SPS und Remotesystemen her und implementiert unterschiedliche Netzwerkstrukturen einschließlich Profibus, DP, Ethernet etc. Dieselbe Firma zählte auch zu den initialen Angriffsopfern bei mindestens einer späteren Stuxnet Variante. Zu den initialen Angriffsopfern zählte auch das iranische Unternehmen Behpajooh Co. Elec & Comp. Engineering, ein weiterer Hersteller industrieller Steuerungssysteme. Behpajooh wurde nicht nur mit Stuxnet Variante A im Jahr 2009, sondern auch zwei Mal von späteren Stuxnet-Varianten angegriffen. Zum dritten initialen Angriffsopfer, der Neda Industrial Group mit Sitz in Iran, gehört ein Unternehmenszweig, der sich mit industrieller Steuerungstechnik für Kraftwerke sowie die Öl- und Gasindustrie beschäftigt. Auch das vierte der initialen Angriffsopfer, die Control-Gostar Jahed Company, arbeitet im Bereich der industriellen Steuerungssysteme. Sowohl die Neda Industrial Group als auch die Control-Gostar Jahed Company wurden nur im Jahr 2009 angegriffen. Alle vier initialen Angriffsopfer arbeiten demnach im Bereich der industriellen Steuerungssysteme, besitzen aber keine offensichtlichen, direkten Verbindungen zur Urananreicherungsanlage in Natanz, die weithin als eigentlich anvisiertes Angriffsziel gilt. Es erscheint daher plausibel anzunehmen, dass es den Angreifern bei diesen initialen Opfern neben der Weiterverbreitung über die Lieferkette vornehmlich um das Ausspähen relevanter Informationen ging.

Im Jahr 2010 gab es mit der Kalaye Electric Company, einem iranischen Unternehmen in Staatsbesitz ein weiteres initiales Angriffsopfer. Die Kalaye Electric Company ist der iranischen Atomenergiebehörde untergeordnet und gilt zum einen als primärer Standort für Forschungen in Bezug auf Urananreicherung. Zum anderen entwickelt und testet das Unternehmen Zentrifugen zur Urananreicherung und gilt als Zulieferer für die Zentrifugen der iranischen Urananreicherungsanlage Natanz. Es ist davon auszugehen, dass die Kalaye Electric Company von den Angreifern als erstes Glied in der Infektionskette ausgewählt wurde, über die Stuxnet in Natanz eingeschleust wurde.

Signifikante Auswirkungen

Insbesondere die Stuxnet Variante B verbreitete sich 2010 und infizierte Computer weltweit. Die Ausbreitung von Stuxnet ist noch immer nicht vollständig zum Erliegen gekommen, bis heute kommt es immer wieder zu IT-Sicherheitsvorfällen in Zusammenhang mit Stuxnet. Die meisten betroffenen Anlagen und Unternehmen haben keinen kerntechnischen Bezug. Stuxnet wurde gezielt für einen Angriff auf eine kerntechnische Anlage, die Urananreicherungsanlage im iranischen Natanz, entwickelt. Dort rief Stuxnet über Monate hinweg physische Schäden hervor.

3.2.2 Cyberangriffe im Zusammenhang mit schadsoftwarebehafteten SolarWinds Produkten

Verwendete Quelle(n): /BSI21i01, BUN21r01, BUS20w01, CBS21w01, CIS20i01, CIS21r02, DAR21w01, DAR21w02, FIR20r01, MIC20w04, NYT20w02, POL20w01, SAN20w01, SEC20w03, SOL21i01, TWP20w01, WSJ20w01/

Kurzüberblick

Anfang Dezember 2020 wurde eine breit angelegte Welle von IT-Angriffen über manipulierte, schadsoftwarebehaftete SolarWinds Produkte bekannt. Angriffsziele waren hauptsächlich Regierungseinrichtungen, Forschungseinrichtungen, kritische Infrastrukturen und auf IT spezialisierte Unternehmen. Das texanische Unternehmen SolarWinds stellt unter anderem Monitoring- und Managementsysteme her. Produkte von SolarWinds werden weltweit von mehr als 300 000 Organisationen bzw. Unternehmen eingesetzt. Hierzu zählen zahlreiche Regierungsorganisationen in den USA und Europa sowie staatliche bzw. internationale Organisationen und Einrichtungen wie beispielsweise NSA, NASA und NATO. Darüber hinaus nutzen auch IT-Sicherheitsfirmen sowie die Mehrheit aller großen US-Konzerne, aber auch viele große Unternehmen in Europa SolarWinds

Produkte. Von den Manipulationen betroffen ist die SolarWinds Orion Platform, wobei SolarWinds angibt, dass etwa 18 000 Kunden die kompromittierten Updates heruntergeladen hätten.

Aus diesen 18 000 Kunden, die sich das kompromittierte Update heruntergeladen haben, wählten die Angreifer interessante Angriffsziele für weiterführende, individuell auf das jeweilige Angriffsziel abgestimmte Angriffsschritte aus. Es wird von mehr als 250 Angriffszielen ausgegangen, bei denen über die Kompromittierung mit dem manipulierten Update hinausgehende Angriffsschritte durchgeführt wurden. Allerdings 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 /FIR20r01/. 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.

Der Hersteller SolarWinds hat inzwischen Updates für alle Orion Versionen, welche manipuliert sind und die Schadsoftwarekomponente Sunburst enthalten, veröffentlicht. Zusätzlich wurde das digitale Zertifikat zu Code-Signierung, mit dem auch die manipulierten SolarWinds Orion Versionen signiert worden waren zurückgezogen und die mit diesem Zertifikat signierte Software neu kompiliert. Spezialisten gehen insgesamt davon aus, dass es eine sehr komplexe Herausforderung darstellt, die Angreifer von kompromittierten Systemen zu entfernen und dass die einzige Möglichkeit dies sicherzustellen darin besteht, alle betroffenen Systeme komplett neu aufzusetzen.

Entdeckung des IT-Sicherheitsvorfalls

Entdeckt wurde die Angriffswelle durch die IT-Sicherheitsfirma FireEye, die selbst zu den Opfern zählt. Im November 2020 entdeckte ein Mitarbeiter von FireEye eine Unregelmäßigkeit bei der Zwei-Faktor-Authentifizierung, welche die Firma bei der Arbeit aus dem Homeoffice nutzt. Hierbei registrieren die Mitarbeiter ihre Mobiltelefone und bekommen bei einem Login-Versuch einen Code auf das Mobiltelefon gesendet, welcher beim Login zusätzlich zu den Credentials (Kombination aus Nutzernamen und Passwort) abgefragt wird. Einem Angehörigen des IT-Sicherheitspersonals von FireEye fiel auf, dass sich ein Mitarbeiter einloggte, der ein zusätzliches Mobiltelefon auf seinen Namen registriert hatte. Auf Anfrage gab dieser Mitarbeiter an, nur ein Mobiltelefon registriert zu haben.

Diese Unregelmäßigkeit veranlasste FireEye zu einer detaillierten Suche nach weiteren Unregelmäßigkeiten. Hierbei entdeckten die Analysten in ihrem Netzwerk Eindringlinge, die als Mitarbeiter getarnt agierten und Informationen stahlen. Insbesondere wurde auch der Diebstahl von speziell entwickelten Red Team Tools[5] entdeckt.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Die mit der Schadsoftwarekomponente Sunburst infizierten Versionen von SolarWinds Orion wurden von Tausenden Kunden des Unternehmens heruntergeladen. Das Herunterladen des Updates führt zur Einschleusung der Schadsoftware auf die IT-Systeme der betroffenen Kunden. Die Schadsoftware Sunburst etabliert eine Backdoor, welche nach einer bis zu zweiwöchigen Ruhephase aktiviert wird. Anschließend führt die Schadsoftware eine ganze Reihe von Prüfungen durch, um sicherzustellen, dass sie sich in einem tatsächlichen, geeigneten Netzwerk befindet. Anschließend kontaktiert sie einen Command-and-Control-Server (C2) und kann dann Befehle bzw. weitere Schadsoftwarekomponenten nachladen und ausführen sowie bei Anforderung auch einen weiteren Command-and-Control-Server kontaktieren. Damit eröffnet sie den Angreifern einen komfortablen Handlungsspielraum für sekundäre Angriffsschritte. Zur Kommunikation nutzt die Schadsoftware ein Protokoll, dass zunächst nicht vom legitimen SolarWinds Kommunikationsprotokoll zu unterscheiden ist.

Die betroffenen SolarWinds Orion Versionen enthalten eine kompromittierte Bibliothek, die neben legitimen Klassen und Methoden auch eine manipulierte Klasse enthält, welche die Sunburst Backdoor im Rahmen des legitimen Update-Vorgangs implementiert. Die Manipulation ist so angelegt, dass die Schadsoftwarekomponente Sunburst von einer legitimen SolarWinds Anwendung ausgeführt wird, deren primäre Aufgabe darin besteht, SolarWinds Plugins zu laden und auszuführen. Diese wird regelmäßig aufgerufen, wodurch die Angreifer sowohl die Ausführung als auch die Persistenz der enthaltenen Schadsoftwarekomponente Sunburst sicherstellen. Alle legitimen Funktionalitäten der von der Kompromittierung betroffenen SolarWinds Orion Updates laufen völlig ungestört.

Die Schadsoftwarekomponente Sunburst wird erst nach Ablauf einer variablen Wartezeit ausgeführt. Auch werden zahlreiche Checks durchgeführt, die sicherstellen sollen, dass sich Sunburst in einer geeigneten Installationsumgebung befindet und das Risiko einer

[5] IT-Werkzeuge zur Durchführung von Penetration Tests, d. h. Werkzeuge, die für das effektive, unbemerkte und ungehinderte Eindringen in zu untersuchende Netzwerke entwickelt wurden.

möglichen Detektion gering ist. Um einer möglichen Entdeckung vorzubeugen, sucht Sunburst auf dem Zielsystem gezielt nach ausgewählten Security-Anwendungen, versucht diese bei deren Vorhandensein zu deaktivieren und führt sofern dies misslingt keine weiteren Aktivitäten aus. Sind alle Checks erfolgreich abgeschlossen, beginnt die Schadsoftware mit der Ausführung ihrer eigentlichen Funktionalitäten.

Der Schwerpunkt liegt hierbei zunächst auf der Herstellung und Aufrechterhaltung der Kommunikation mit von den Angreifern kontrollierten Command-and-Control Servern. Nach dem ersten Kontakt mit dem Command-and-Control Server senden die Angreifer häufig alternative Domains bzw. IP-Adressen an die Schadsoftware, um die weitere Kommunikation auf einen zweiten Command-and-Control Server zu verlagern. Damit steht den Angreifern auch dann noch eine Kommunikationsmöglichkeit zur Verfügung, wenn der erste Kommunikationskanal entdeckt bzw. blockiert wird. Bei der Kommunikation mit einem Command-and-Control Server imitiert Sunburst das Orion Improvement Program (OIP) protocol, um diese wie normale Kommunikation von SolarWinds Orion erscheinen zu lassen.

Neben dem Aufbau der Kommunikation mit einem Command-and-Control Server beinhaltet Sunburst Funktionalitäten, um einschlägige Systeminformationen zusammenzustellen und anschließend zu exfiltrieren. Darüber hinaus enthält Sunburst weitreichende Funktionalitäten, die einem Hands-on-Keyboards Angreifer weitreichenden Handlungsspielraum einräumen, indem sie beispielsweise erlauben, ausgewählte Tasks auszuführen, terminierte Tasks oder auch Prozesse zu beenden, Rechte von Prozessen zu beeinflussen, Dateien zu löschen oder hinzuzufügen, Registry-Einträge zu verändern, weitere Details über das kompromittierte System auszuspähen, Hash-Werte zu berechnen, angegriffene Rechner herunterzufahren oder weitere Payloads auszuführen. Mit den Hands-on-Keyboard Aktivitäten und dem Einsatz der sekundären Angriffswerkzeuge und Schadsoftwarekomponenten führen die Angreifer typische Angriffsschritte wie die Eskalation von Rechten, Credential Harvesting, laterale Bewegungen und Ausspähung relevanter Informationen aus. Darüber hinaus etablieren sie zusätzliche Backdoors und bringen sie weitere Payloads ein.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Bei den Angriffen in Zusammenhang mit schadsoftwarebehafteten SolarWinds Produkten handelt es sich um einen klassischen Supply-Chain-Angriff, allerdings in bislang nicht dagewesener Komplexität und Tragweite. Zunächst attackierten die Angreifer das IT-Unternehmen SolarWinds. Den IT-Angreifern gelang es hierbei, unbemerkt eine Reihe

von SolarWinds Orion Versionen mit der Schadsoftwarekomponente Sunburst zu infizieren. Diese manipulierten Updates wurden dann digital signiert und über den offiziellen Update-Server von SolarWinds verteilt. Die Schadsoftwarekomponente Sunburst etabliert auf den durch das Update kompromittierten Systemen eine Backdoor, welche von den Angreifern bei ausgewählten Angriffszielen für weitergehende Angriffsschritte ausgenutzt wurde. Analysten sind sich einig, dass es sich um die am höchsten entwickelte und am breitesten angelegte IT-Angriffskampagne handelt, die bislang bekannt geworden ist - und dass von ihr ein erhebliches Gefährdungspotenzial ausgeht.

Nach der Kompromittierung der Infrastruktur des IT-Unternehmens SolarWinds gelang es den Angreifern, Schadsoftware in den Software-Lebenszyklus von SolarWinds Orion einzubringen und so über einen langen Zeitraum eine Reihe von SolarWinds Orion Versionen mit Schadsoftware zu infizieren. Inzwischen ist klar, dass die IT-Angreifer Zugriff auf den Build-Server (dient zur Kompilierung des Source Codes) von SolarWinds hatten und den Build-Prozess der SolarWinds Software Orion manipulierten. Im Rahmen der forensischen Analysen eines Build-Servers von SolarWinds wurde von IT-Spezialisten der Firma CrowdStrike eine weitere Schadsoftwarekomponente aufgefunden, die dazu diente, die Schadsoftwarekomponente Sunburst in den Kompilierungsprozess der SolarWinds Orion Produkte einzubringen. Diese Schadsoftwarekomponente wird mit dem Namen Sunspot bezeichnet. Die schadsoftwarebehafteten SolarWinds Orion Versionen wurden dann mit dem legitimen SolarWinds Zertifikat digital signiert und über den offiziellen Update-Server von SolarWinds verteilt.

Signifikante Auswirkungen

Von der Angriffswelle betroffen sind unter anderem eine Reihe von Ministerien, Behörden, anderen Regierungseinrichtungen und regierungsnahen Forschungseinrichtungen in den USA, Deutschland und Europa, darunter beispielsweise das U.S. Department of Homeland Security, das U.S. Department of Defense (Verteidigungsministerium der Vereinigten Staaten), das U.S. Department of State, das U.S. Department of the Treasury (Finanzministerium der Vereinigten Staaten), das U.S. Department of Commerce (Handelsministerium der Vereinigten Staaten) sowie das U.S. Department of Justice /BUS20w01, CBS21w01/. Darüber hinaus zählen zu den anvisierten Zielen namhafte IT-Unternehmen sowie auf IT-Sicherheit spezialisierte Unternehmen wie beispielsweise: Microsoft, Cisco Systems, Intel, Nvidia, VMware, Belkin International, Mimecast, FireEye oder CrowdStrike. Weitere Angriffsziele waren aber auch Unternehmen und

Einrichtungen aus vielfältigen Branchen und Lebensbereichen, darunter zahlreiche Universitäten, Forschungseinrichtungen, Krankenhäuser und Unternehmen des Finanzsektors.

Im Rahmen der IT-Angriffe mit manipulierten SolarWinds Orion Produkten ist es auch zur Kompromittierung kerntechnischer Anlagen und Einrichtungen gekommen. Hierzu zählen beispielsweise das Los Alamos National Laboratory und die Sandia National Laboratories. Bei ersterem handelt es sich um eine US-amerikanische Forschungseinrichtung, die der NNSA untersteht und in der unter anderem zu Nuklearwaffen und Kernfusion geforscht und deren Entwicklung vorangetrieben wird. Bei zweiterem handelt es sich um eine US-amerikanische Forschungseinrichtungen, die ebenfalls der NNSA unterstehen und in denen hauptsächlich die nicht-nuklearen Komponenten von Nuklearwaffen entwickelt und hergestellt werden. Darüber hinaus zählen auch einige Institutionen und Einrichtungen zu den Angriffsopfern, die mit diesen in engem Zusammenhang stehen, wie beispielsweise die National Nuclear Security Administration, die Federal Energy Regulatory Commission (FERC) und das U. S. Department of Energy. Bei der NNSA handelt es sich um eine Bundesbehörde, die dem Department of Energy untersteht und der unter anderem die Sicherheit und Sicherung des Atomwaffenarsenals der USA sowie der Sicherstellung der Leistungsfähigkeit dieser Waffen obliegt.

3.2.3 Schwachstellen in Microsoft Exchange

Verwendete Quelle(n): /BAR21w01, BOR21w01, BSI21i03, BSI21i04, BSI21i05, CIS21w05, CVE21w01, ESE21w01, MAL21w02, MIC21w09, MIC21w10, MIC21w11, MIC21w12, MIC21w13, MIC21w14, MIC21w15, MIC21w16, VOL21w01, ZDN21w04/

Kurzüberblick

Im ersten Quartal 2021 wurden Informationen über schwerwiegende Sicherheitslücken bekannt, welche von Angreifern für IT-Angriffe auf Microsoft Exchange Server, welche unter anderem für das weltweit verbreitete E-Mail- und Organisationsprogramm Outlook genutzt werden, ausgenutzt werden können. Zum Zeitpunkt des Bekanntwerdens wurden die Schwachstellen aktiv von Angreifern ausgenutzt, wodurch potenziell eine hohe Anzahl von Unternehmen, Behörden und Betreibern kritischer Infrastruktur betroffen waren. Die Schwachstellen in Microsoft Exchange ermöglichen unter anderem den Datendiebstahl und die Installation weiterer Schadsoftware, sowie die Übernahme des gesamten Systems aus der Ferne durch Angreifer. Nach den Angaben von Microsoft wurden

über die Schwachstellen bereits IT-Angriffe gegen amerikanische Einrichtungen durchgeführt. Zu den Angriffszielen gehören Forschungseinrichtungen mit dem Schwerpunkt Pandemie, Hochschulen, Anwaltsfirmen, der Rüstungssektor, Think Tanks und nichtstaatliche Organisationen. Die Schwachstellen wurden mutmaßlich bereits im November 2020 für gezielte IT-Angriffe genutzt. Die Angreifer verschafften sich dabei Zugang über die E-Mail-Accounts und installierten danach weitere Schadsoftware zur Herstellung einer persistenten Verbindung. Von den Schwachstellen waren im März 2021 in Deutschland etwa 57000 Server potenziell betroffen.

Entdeckung des IT-Sicherheitsvorfalls

Am 2. März 2021 veröffentlichte Microsoft Updates bzgl. der Schwachstellen für Microsoft Exchange Server. Einzelne Schwachstellen und IT-Angriffe wurden bereits Monate vorher bzw. weitere Schwachstellen später im Jahr 2021 bekannt. Die IT-Sicherheitsfirma Volexity entdeckte beispielsweise am 6. Januar 2021 auffällige Aktivitäten auf zwei Microsoft Exchange Servern ihrer Kunden, die den Netzwerksicherheitsüberwachungsdienst von Volexity für ihre Server verwendeten. Analysen des Datenverkehrs zeigten, dass es sich um einen IT-Angriff handelte, bei dem die vier als ProxyLogon bezeichneten Schwachstellen des Microsoft Exchange Servers zum Datendiebstahl und zur lateralen Ausbreitung im Netzwerk eingesetzt wurden. Nach Angaben von Microsoft handelte es sich bei den Angreifern um die APT-Gruppierung Hafnium, die im Auftrag des chinesischen Staates handelt. Am 12. Oktober 2021 entdeckte die IT-Sicherheitsfirma Cisco Talos mit Hilfe ihrer Produkttelemetrie von Cisco Secure Angriffe auf Microsoft Exchange Server, die die drei unter dem Namen ProxyShell bekannten Schwachstellen ausnutzten. Sie wurden von der russischen APT-Gruppierung Tortilla eingesetzt, um die Ransomware Babuk zu verbreiten. Da es sich um eine Vielzahl von IT-Sicherheitsvorfällen in Bezug auf Schwachstellen von Microsoft Exchange handelt, gibt es insgesamt keine einzelne eindeutige Entdeckung, sondern einen mehrstufigen Prozess unterschiedlicher Vorgänge wie beispielsweise die Entdeckung von einzelnen Schwachstellen (öffentlich und nicht-öffentlich) - Sicherheitsforscher von DEVCORE meldeten beispielsweise die vier als ProxyLogon bezeichneten Schwachstellen am 5. Januar 2021 an Microsoft – sowie einzelner IT-Angriffe.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Insgesamt handelt es sich bei den bekannt gewordenen Sicherheitslücken um mehrere unterschiedliche Schwachstellen, von denen im Folgenden einige wesentliche kurz vorgestellt werden. Vier Schwachstellen sind seit dem 02.03.2021 unter dem Namen ProxyLogon bekannt. Sie ermöglichen den Datendiebstahl und die Installation weiterer Schadsoftware. Relevante IT-Angriffe, bei denen diese 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:

- **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. CVSS-Score: CVSS:3.0 9.1 / 8.4.

- **CVE-2021-26857**: Ermöglicht die Ausführung beliebigen 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.

- **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. CVSS-Score CVSS:3.0 7.8 / 7.2.

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

- **CVE-2021-31207**: Diese Schwachstelle ermöglicht es einem Angreifer per Fernzugriff den Authentifizierungsprozess zu umgehen. CVSS-Score: CVSS:3.0 6.6 / 5.8.

- **CVE-2021-34523**: Ermöglicht einem Angreifer die Erhöhung von Zugriffsrechten/Rechteeskalation. CVSS-Score: CVSS:3.0 9.0 / 7.8.
- **CVE-2021-34473**: Die Schwachstelle erlaubt einem Angreifer die Ausführung beliebigen Programmcodes. Der Angreifer benötigt dazu eine Authentifizierung. CVSS-Score: CVSS:3.0 9.1 / 7.9.

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

- **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.

Darüber hinaus gibt es eine Vielzahl weiterer Schwachstellen. Zurzeit sind 31 Schwachstellen bekannt.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Generell ermöglichten die Schwachstellen im Zusammenhang mit Microsoft Exchange Angreifern IT-Angriffe auf unzählige Ziele, die diese Software nutzen und stellen damit eine typische Angriffsmöglichkeit über die Lieferkette dar. In diesem Zusammenhang stellt sich durch die genauen Umstände und Abfolgen der Ereignisse zudem ein weiterer für die Lieferkette relevanter Aspekt dar. Am 5. Januar 2021 meldeten Sicherheitsforscher von DEVCORE die vier als ProxyLogon bezeichneten Schwachstellen an Microsoft. Bereits einen Tag später am 6.Januar 2021 wurde von der IT-Sicherheitsfirma Volexity die Ausnutzung der Schwachstellen durch die APT-Gruppierung Hafnium entdeckt. Am 2. März 2021 veröffentlichte Microsoft die entsprechenden Updates für den Microsoft Exchange Server. Dass die Ausnutzung der Schwachstellen bereits vor der Veröffentlichung von Informationen erfolgte, lässt die Möglichkeit offen, dass diese durch ein Datenleck bei Microsoft bekannt gemacht wurden. Nach Angabe des Wallstreet Journals wurde für die Angriffe auf die Microsoft Exchange Server nahezu der gleiche Programmcode verwendet wie der Proof-of-Concept-Code (PoC), den die Sicherheitsforscher von DEVCORE mit ihrer Meldung an Microsoft schickten. Möglicherweise gab es in diesem Zusammenhang somit ein Abfließen der Informationen von Microsoft an die Angreifer, wobei unklar ist, ob dies durch aktive Angriffshandlungen gezielt auf Microsoft als Zwischenziel der Lieferkette erfolgten.

Signifikante Auswirkungen

Zu den Angriffszielen der APT-Gruppierung Hafnium, die die als ProxyLogon bekannten Schwachstellen einsetzte, gehören Einrichtungen in den USA wie Think Tanks, gemeinnützige Organisationen, der Rüstungssektor und Forschungseinrichtungen. Darüber hinaus wurden die ProxyLogon-Schwachstellen nicht nur von Hafnium, sondern auch von anderen APT-Gruppierungen wie LuckyMouse, Tick, Winnti Group und Calypso ab dem 28. Februar 2021 gegen US-Einrichtungen eingesetzt. Die Angriffe richteten sich gegen lokale Regierungsstellen, Universitäten, Ingenieurunternehmen und den Einzelhandel, vermutlich mit dem Ziel des Datendiebstahls. Angriffsziele in Deutschland und Großbritannien umfassen Regierungs- und Militäreinrichtungen, die Fertigungsindustrie, Finanzdienstleister, die Europäische Bankenaufsichtsbehörde (EBA) und Softwareanbieter. Die IT-Angriffe der APT-Gruppierung Tortilla, die die drei als ProxyShell bekannten Schwachstellen ausnutzte, um die Schadsoftware Babuk zu verbreiten, richteten sich im Wesentlichen gegen Einrichtungen in den USA. Darüber hinaus erfolgten Angriffe auf Organisationen in Deutschland, Großbritannien, der Ukraine, Finnland, Brasilien, Honduras und Thailand.

3.2.4 Schwachstelle in Log4J

Verwendete Quelle(n): /CIS21i10, BLO21w03, FAZ21w04, HEI22w24, SOP22w01, SPI21w02, SPI21w03/

Kurzüberblick

Im Dezember 2021 wurden Informationen über eine Schwachstelle der Programmierbibliothek Log4j des amerikanischen Herstellers Apache bekannt, welche dem Loggen von Meldungen in der Programmiersprache Java dient. Bei Java handelt es sich um eine weit verbreitete Programmiersprache. Entsprechende Programme sind potenziell auf Milliarden IT-Systemen weltweit installiert, was neben Büro-IT auch industrielle PCs, Internet-of-Things-Geräte und andere Anwendungen und leittechnische Systeme umfassen kann. Log4j selbst wurde gegen Ende der 1990er Jahre entwickelt und als Open-Source-Software veröffentlicht und in Verbindung mit auf Java basierender Software seitdem verwendet, da Java selbst keine eigenen Logging-Funktionen besitzt. Log4j ist über die Jahre Teil diverser Open-Source- und kommerzieller Softwareprodukte geworden und hat sich zu einem De-Fakto-Standard entwickelt, der entsprechend weit verbreitet ist. Die Schwachstelle (CVE-2021-44228), genannt Log4Shell, ermöglicht einem

Angreifer in einen Angriff durch die Übermittlung eines bestimmten Zeichencodes beliebigen Code auf dem angegriffenen System auszuführen und beispielsweise die vollständige Systemkontrolle zu übernehmen. Betroffen sind die Log4j-Versionen 2.0 bis 2.16. Diverse IT-Sicherheitsbehörden weltweit wie beispielsweise die CISA oder das BSI veröffentlichten nach Bekanntwerden der Schwachstelle entsprechende Warnmeldungen. Erste Angriffe über die Schwachstelle begannen Anfang Dezember 2021, wobei die Anzahl der Angriffe mit der Veröffentlichung der Informationen am 9. Dezember 2021 stark zugenommen hat. Die Schwachstelle kann unter Umständen vollautomatisch über das Internet angegriffen werden, wenn betroffene Systeme entsprechende Verbindungen aufweisen. Daher ist ein großer Teil der Angriffslast wahrscheinlich auf automatisierte Angriffe zurückzuführen. Innerhalb von Netzwerken kann die Schwachstelle zudem zu lateralen Bewegungen und weiteren Verbreitungen bzw. Zugriffsmöglichkeiten ausgenutzt werden.

Entdeckung des IT-Sicherheitsvorfalls

Die Schwachstelle Log4Shell wurde am 24. November 2021 von Chen Zhaojun, einem Mitarbeiter von Alibaba Cloud Services, entdeckt und den Entwicklern von Apache gemeldet. Während Apache an einem Patch zur Behebung der Schwachstelle arbeitete, wurden Informationen zu Log4Shell in chinesischen Blogs diskutiert (8. Dezember 2021). Am 9. Dezember 2021 veröffentlichte Log4j daraufhin einen ersten Patch und es erschienen Informationen dazu bzw. ein Proof-of-Concept in diversen Blogs. Am 12. Dezember 2021 erfolgte die Veröffentlichung von Informationen der Schwachstelle vom NIST. Nachdem die Schwachstelle einer breiten Öffentlichkeit bekannt wurde, folgten Zahlreiche Angriffe unter Ausnutzung deren im Dezember 2021 bis zum heutigen Tag.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Log4Shell ermöglicht unter gewissen Umständen die Ausführung beliebigen Shell-Codes, indem spezifische Befehle übermittelt werden, sodass externe Java-Bibliotheken auf dem betroffenen System aufgerufen werden können. Bei entsprechender Vorbereitung lässt sich dadurch beliebiger Code ausführen und prinzipiell die komplette Systemkontrolle erlangen. Die Wirkungsweise von Log4shell basiert darauf, dass Log4j externe Daten nicht einfach in eine Log-Datei schreibt, sondern die Strings deserialisiert (Umwandlung eines Bytestroms, der durch Serialisierung eines Objekts gewonnen wurde, zurück in ein Objekt) und den Inhalt wie Java-Objekte behandelt und somit wie

auszuführende Befehle. Dies führt in Kombination mit dem Java Naming and Directory Interface (JNDI), einer Programmierschnittstelle für Verzeichnisdienste innerhalb von Java, dazu, dass Java Konfigurationsdateien innerhalb der Laufzeit eines Programms aus dem Internet heruntergeladen werden bzw. externe Java-Bibliotheken eingebunden werden können. Die Kombination von Log4j und JNDI ist insoweit problematisch, dass potenzielle Angreifer einen Pfad zu einem (ggf. vorher präpariertem) schadsoftwarebehafteten-Code in eine Webanfrage einbringen könnten, was dazu führt, dass Log4j diesen Pfad nicht einfach als Text speichert, sondern (durch die Funktionen von JNDI) als Befehl interpretiert, wodurch der besagte Code auf das System gelangt und ausgeführt wird. Das bedeutet, dass in externen Bibliotheken, die eingebunden werden, sogenannter Shell-Code (Instruktionen für die Ausführung von Befehlen durch einen Exploit eines Programms, wodurch im Prinzip ein Code entsteht, welcher in andere Programme integriert werden kann; die Zielsetzung ist beispielsweise die Ausführung der Kommandozeile und darin dann die Ausführung von weiterem schadhaftem Code) integriert sein kann, welcher zur Ausführung beliebigen Codes auf dem betroffenen System eingesetzt werden kann. Logging-Programme werden auf den Systemen in der Regel mit Administrator-Rechten durchgeführt, sodass sich potenzielle Angreifer ohne Authentifizierung und ohne Rechte durch einfache Anfragen prinzipiell einen vollständigen Systemzugriff beschaffen können und die Kontrolle über das gesamte System erlangen.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Der Lieferkettenaspekt von Log4j/Log4shell besteht insbesondere darin, dass es sich um eine Schwachstelle in einer Programmbibliothek von Java handelt, welche als De-Fakto-Standard in diversen Open-Source- oder kommerziellen Produkten weltweit eingesetzt wird. Die betroffenen Programme binden diese externe Bibliothek ein, ohne dass deren Inhalt unter eigener Kontrolle steht. Somit sind die betroffenen Programme im Fall eines Zero-Day-Exploits oder anderer Schwachstellen direkt angreifbar, ohne dass potenzielle Angreifer zuvor spezifische Angriffsschritte für ein spezielles Opfer durchführen müssten. Außerdem würden auf Schadsoftwareerkennung ausgelegte Programme zunächst bei der Ausnutzung der Schwachstelle keine Alarmmeldungen produzieren, da die Ausnutzung zunächst wie eine legitime Programmfunktion erscheint. Angreifer haben somit in diesem Fall Zugriff auf unzählige verwundbare Systeme weltweit verteilt.

Signifikante Auswirkungen

Die Auswirkungen der Schwachstelle in Log4Shell sind weitreichend und betreffen Firmen, Organisationen und Institutionen weltweit, was durch die immense Verbreitung von Log4j begründet ist. Zu den einsetzenden Organisationen und Unternehmen zählen beispielsweise Apple, Google, Tesla und Amazon, sowie mehrere deutsche Bundesbehörden. Es gab weltweit diverse Angriffe, die Log4j ausnutzten, darunter auch kritische Infrastrukturen und Regierungsbehörden. Beispielsweise wurden mit dem Internet verbundene Systeme des belgischen Militärs angegriffen. In Deutschland waren unter anderem der Bundesfinanzhof und der Landtag von Schleswig-Holstein Ziele von Angriffen, die Log4Shell ausnutzten. In beiden Fällen führte dies dazu, dass entsprechende Internetseiten nicht mehr erreichbar waren, wobei mutmaßlich jedoch keine sensiblen Daten gestohlen wurden bzw. die Angreifer keinen Zugang zu internen Netzwerken erhielten. Insgesamt wurden nach Angaben des britischen IT-Unternehmens Sophos nicht so viele IT-Angriffe über Log4Shell beobachtet, wie anfänglich hinsichtlich der Schwere und Verbreitung befürchtet wurde, was unter anderem auf die große (mediale) Aufmerksamkeit und damit einhergehenden Maßnahmen zurückgeführt wurde. Dennoch stellt die weite Verbreitung von Java in Kombination mit der umfassenden Nutzung von Log4j eine ernstzunehmende Bedrohung dar, da neben regulären Büro-IT-Systemen auch Java nutzende Systeme mit eingeschränkter Programmierfähigkeit wie industrielle Steuerungen, SCADA oder DCS Systeme Internet of Things (IoT und IIoT), Netzwerksysteme wie Router und weitere Systeme wie Kameras, Scanner, RFID-gesteuerte Systeme usw. betroffen sein können. Zu betroffenen Herstellern gehören unter anderem ABB, Cisco, Schneider Electric und Siemens, die in diversen Unternehmen, Organisationen und auch kritischen Infrastrukturen weite Verbreitung haben.

3.2.5 IT-Sicherheitsvorfall im Zusammenhang mit Kaseya

Verwendete Quelle(n): /BSI21i12, DIV21w02, DIV21w03, HEI21w15, HEI21w16, KAS21w04, SOP21w01, SUE21w01/

Kurzüberblick

Am 2. Juli 2021 ereignete sich ein IT-Angriff auf VSA-Server verschiedener weltweit verteilter Unternehmen, wobei über 1000 Firmen betroffen waren. Im weitesten Sinn handelt es sich bei VSA um eine Plattform zum Management von Software, ein Remote-Monitoring und -Management-Tool, mit dem Dienstleistungen wie beispielsweise Fernwartung

o. Ä. durchgeführt werden können, gehört. Management Service Provider (MSP), die VSA nutzen, setzen derartige Software u. a. zur Administration und Fernwartung Ihrer Kunden ein. Unter anderem wird VSA häufig zum Ausführen von Softwareupdates verwendet. Dabei gibt es die Option einer eigenen VSA-Installation (On Premise) oder ein von Kaseya selbst gehostetes Cloud-Angebot als Software-as-a-Service (SaaS).

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 folgte eine Lösegeldforderung im Darknet über 70 Millionen US-Dollar in Form von Kryptowährung für die Entschlüsselung der Daten. Betroffen war neben überwiegend Unternehmen in den USA, Deutschland und Großbritannien auch die schwedische Supermarktkette Coop, deren Zahlungsdienstleister die Software von Kaseya nutzt. Coop musste in der Folge am 3. Juli alle 800 Filialen schließen, da die Kassensysteme blockiert waren. Neben den über 1000 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. 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.

Entdeckung des IT-Sicherheitsvorfalls

Die Entdeckung des IT-Angriffs erfolgte mit der Verschlüsselung der Daten der Kaseya-Kunden am 2. Juli 2021. Die ausgenutzten Schwachstellen und Zero-Day-Exploits waren zwar dem Softwarehersteller Kaseya durch Mitarbeiter des Dutch Institute for Vulnerability Disclosure (DIVD) bekannt gemacht worden und es wurde entsprechend an einer Lösung in Form von Patches gearbeitet, jedoch kam der IT-Angriff der Veröffentlichung der Sicherheitsupdates zuvor. Kaseya selbst informierte bereits am 2. Juli die Öffentlichkeit, dass sie einen potenziellen Angriff auf VSA untersuchen und empfahlen allen ihren Kunden, die On Premise Software herunterzufahren.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

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. Dabei werden neben dem ursprünglich betroffenen System auch damit verbundene (Wechsel)Datenträger und Netzwerklaufwerke verschlüsselt. Außerdem werden Einstellungen der Firewall geändert, sodass der betroffene Computer im Netzwerk sichtbar für andere Computer ist. Betroffen war neben den On-Premise-Installationen der Kaseya-Kunden auch die SaaS-Cloud-Infrastruktur, wobei Kaseya nach eigenen Angaben jedoch dazu in der Lage war, diese Cloud-Infrastruktur rechtzeitig herunterzufahren, sodass darüber keine Client-Systeme infiziert wurden. Insgesamt berichtet Kaseya von 60 betroffenen Kunden der On Premise Version von VSA. Der ursprüngliche Zugriff auf die Infrastruktur von Kaseya gelang den Angreifern durch die Ausnutzung von Schwachstellen und Zero-Day-Exploits. Forscher des DIVD informierten Kaseya im April 2021 über insgesamt 7 Schwachstellen (CVE-2021-30116, CVE-2021-30117, CVE-2021-30118, CVE-2021-30119, CVE-2021-30120, CVE-2021-30121 und CVE-2021-30201) Einige dieser Schwachstellen konnte Kaseya durch Patches bereits vor dem Angriff am 2. Juli beheben, jedoch konnten die Angreifer an diesem Tag mehrere Schwachstellen Ausnutzen, um Zugriff auf VSA Server zu erlangen.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Einschleusung der Schadsoftware bzw. das Einfallstor für diesen Lieferkettenabgriff waren mehrere Zero-Day-Exploits in Kaseyas Software VSA. Die Existenz dieser Sicherheitslücken war bereits teilweise vor dem Angriff bekannt. Standardmäßig bietet Kaseya VSA On premise eine Download-Seite, auf der die Clients für die Installation heruntergeladen werden können. Im Wesentlichen handelt es sich bei den eingesetzten Angriffstechniken um einen Authentication-Bypass, bei dem Angreifer ohne Authentifizierung über das Internet mit den betroffenen VSA-Servern kommunizieren konnten. Dabei ist es den Angreifern möglich, weitreichende Informationen (sessionID, Zugriff auf programminterne Initialisierungs-Dateien) zur Intensivierung des Angriffes zu erlangen. Letztlich war es den Angreifern möglich, eigene Befehle auf dem VSA-System auszuführen und somit die Systeme zu kontrollieren, die dafür zuständig sind, die Clients mit neuer Software und Patches zu versorgen. Die kompromittierten VSA-Server wurden so

manipuliert, dass ein angeblich legitimes Update („Kaseya VSA Agent Hot-fix“) auf alle von diesem Server gemanagten Client-Systeme ausgerollt wurde, welche das unbemerkt manipulierte Update ordnungsgemäß einspielten. Der Umstand, dass Kaseya für seine Management-Software großzügige Ausnahmeregeln für Antivirus- und Firewall-Software empfiehlt, kam den Angreifern in diesem Fall zusätzlich zugute. Die Angreifer nutzten außerdem während ihres Angriffs ein legitimes Zertifikat („PB03 TRANSPORT LTD“), wobei davon auszugehen ist, dass dieses im Rahmen der Vorbereitung des Angriffs gestohlen wurde. Ansonsten setzte REvil gezielt vorbereitete IT-Angriffswerkzeuge ein.

Signifikante Auswirkungen

Die Auswirkungen des IT-Angriffs wurden in den Tagen nach dem 2. Juli 2021 nach und nach bekannt, wobei bis heute viele betroffene Firmen nicht bekannt sein dürften. Betroffen waren neben den USA vor allem auch Deutschland, Großbritannien und weitere europäische Länder. Neben den direkten Kunden von Kaseya waren auch viele Firmen betroffen, die indirekt mit Kaseya VSA Servern in Verbindung stehen über Managed Service Provider (MSP) bzw. IT-Dienstleister, die wiederum Kunden von Kaseya sind. Kaseya selbst spricht von etwa 40 betroffenen Unternehmen, die jedoch teilweise IT-Dienstleister sind, sodass die Zahl von hunderten betroffenen Firmen angenommen werden kann. Zu den öffentlichkeitswirksamsten Auswirkungen zählt die Schließung aller ca. 800 Filialen der schwedischen Supermarktkette Coop, deren Zahlungsdienstleister Visma Esscom die Software von Kaseya nutzt und dessen Kassensysteme entsprechend blockiert waren. Zudem waren in Schweden die Bahngesellschaft, eine Tankstellenkette und eine Apothekenkette betroffen. Beim BSI meldete sich ein deutsches Unternehmen als betroffen, wobei es sich auch um einen IT-Dienstleister handelte, dessen Kunden in Mitleidenschaft gezogen wurden.

3.2.6 Cyberangriff auf CodeCov

Verwendete Quelle(n): /ATN21w01, COD21w01, DEV21w01, IIT21w01, TRN21w01, WSN21w01/

Kurzüberblick

Am 1. April 2021 wurde ein IT-Angriff auf den IT-Dienstleisters Codecov entdeckt, bei dem der Bash Uploader des Unternehmens manipuliert worden war. Dadurch konnten

die Angreifer an sensible Daten der Kunden von Codecov wie IBM, Google, HPE, Atlassian und HashiCorp gelangen. Der Angriff blieb lange unbemerkt und hatte bereits zwei Monate zuvor begonnen. Codecov bietet einen gehosteten Dienst an, der es Softwareentwicklern ermöglicht zu prüfen, wie ihr Programmcode durch die automatisierten Testverfahren ihres Softwareentwicklungsprozesses verifiziert werden kann. Für Open-Source-Projekte ist Codecov kostenlos. Am 31. Januar 2021 verschafften sich Angreifer Zugriff auf die Server des Bash Uploaders von Codecov, welcher unter anderem Teil Codecov-Komponenten für Github, einem Onlinedienst zur Softwareentwicklung und Versionsverwaltung für Softwareprojekte ist. Die Angreifer modifizierten das Skript des Bash Uploaders und gelangten auf diese Weise an die Informationen. Diese wurden dann an einen von den Angreifern genutzten Server gesendet. Zu den gestohlenen Informationen gehörten Anmeldeinformationen, Tokens oder Schlüssel, sowie damit in Verbindung stehende Dienste, Datenspeicher und Anwendungscodes. Darüber hinaus wurden Informationen in Bezug auf Repositorys gestohlen, die den Bash Uploader nutzen, um an Codecov Berichte hochzuladen.

Entdeckung des IT-Sicherheitsvorfalls

Der IT-Angriff wurde von Codecov am Donnerstag, den 1. April 2021 entdeckt. Ein Kunde des Unternehmens hatte zuvor eine Diskrepanz zwischen dem Hash des von Codecov zur Verfügung gestellten Bash Uploader Skripts und dem Hash, welcher auf dem GitHub des Unternehmens ausgeführt wird, bemerkt.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Die Angreifer installierten eine Backdoor im Bash Uploader Skript, indem sie eine einzige Zeile schadhaften Programmcodes in den Uploader einfügten. Mit Hilfe dieses Programmcodes konnten dann die Kundendaten extrahiert und an den von den Angreifern genutzten Server gesendet werden. Dies war u. a. möglich, da für den Zugriff auf den Uploader keine Zwei-Faktor-Authentifizierung erforderlich war.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Am 31. Januar verschafften sich die IT-Angreifer Zugriff auf die Server des Bash Uploaders von Codecov. Aufgrund eines Fehlers im Zusammenhang mit der Softwareplattform zur Erstellung, zum Testen und Bereitstellen von Anwendungen Docker, konnten

die Angreifer entsprechende Anmeldeinformationen stehlen, die es ihnen erlaubten, den Bash Uploader zu modifizieren. Immer wenn der Entwickler eines Kunden von Codecov ein Skript zum Testen von Programmcode von den Servern des Unternehmens herunterlud, aktivierte sich die Schadsoftware auf den Testmaschinen des Kunden, exportierte Daten und sendete diese an den von den Angreifern genutzten Server. Aufgrund des geringen Umfangs des schadhaften Programmcodes, der nur aus einer Zeile bestand und der in einer größeren Serie legitimen Programmcodes des Bash Uploader Skripts versteckt war, konnten die Angreifer ihre Aktivitäten über einen Zeitraum von zwei Monaten verbergen.

Signifikante Auswirkungen

Von dem IT-Angriff sind tausende von Wirtschaftsunternehmen und Open-Source-Projekte betroffen, welche den Dienst von Codecov verwenden. Es wurden jedoch nicht alle Kunden von Codecov kompromittiert. Zu den hunderten kompromittierten Kunden gehören IBM, HPE, Atlassian und HashiCorp.

3.2.7 IT-Sicherheitsvorfall in Zusammenhang mit NPM-Paketen

Verwendete Quelle(n): /BSI22i08, CHE22w01, DEC22w01, HEI21w14, JFR22w01, JFR22w02, MEN22w01, SEC22w12, ZDN22w04, ZDN22w05/

Kurzüberblick

Unternehmen integrieren verstärkt frei verfügbare Softwarelösungen in ihre eigenen Programme. Da aber auch IT-Angreifer Zugriff auf die Repositorys der frei verfügbaren Programmpakete und Skripte haben, können sie diese manipulieren und eigene schadhafte Versionen auf die Repositorys hochladen, bevor sie von Entwicklern in eigene Software eingebunden werden. Dies stellt ein erhebliches Sicherheitsproblem dar und erleichtert Angreifern die Durchführung von Lieferkettenangriffen. Seit August 2021 laden Angreifer vermehrt schadhafte Pakete in das Repository des Unternehmens NPM Inc. (NPM Abkz. für Node Package Manager) hoch. NPM Inc. ist eine Tochtergesellschaft des Repositorys GitHub, welches im Besitz von Microsoft ist und stellt den größten Anbieter für frei verfügbare JavaScript-Pakete dar. Von August 2021 bis Anfang Februar 2022 entdeckte das IT-Sicherheitsunternehmen WhiteSource dabei insgesamt 1300 schadhafte NPM-Pakete, welche von Angreifern zum Diebstahl von Zugangsdaten und Kryptowährungen sowie zum Betreiben von Bot-Netzen genutzt werden können. Die Anzahl der

schadhaften NPM-Pakete wächst stetig und es gibt bisher kein standardmäßig automatisiertes und internes Werkzeug, das das Hochladen von Dateien in das Repository durch Nutzer von NPM verhindern oder hochgeladene Dateien überprüfen würde. Seit März 2022 zielt ein groß angelegter IT-Angriff auf Microsoft Azure-Entwickler mit Hilfe von schadhaften NPM-Paketen ab, um persönliche identifizierbare Informationen von den Entwicklern zu stehlen. Der Angreifer wird als RED-LILI bezeichnet.

Entdeckung des IT-Sicherheitsvorfalls

Im August 2021 wurden die ersten schadhaften NPM-Pakete durch die automatisierte Malwaredetektions-Plattform WhiteSource Diffend des IT-Sicherheitsunternehmens WhiteSource entdeckt. Die schadhaften NPM-Pakete, die Azure-Entwickler betreffen, wurden vom IT-Sicherheitsunternehmen JFrog am 21. März 2022 entdeckt. Das Unternehmen überwacht automatisch und kontinuierlich Repositorys, die frei verfügbare Software beinhalten.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Für den Informationsdiebstahl von den Azure-Entwicklern haben die Angreifer ein automatisiertes Skript entwickelt. Dieses greift verschiedene NPM-Bereiche an und lädt schadhafte NPM-Pakete in das Repository hoch. Um die Detektion ihrer IT-Angriffe zu erschweren, nutzen die Angreifer für das Hochladen jedes schadhaften NPM-Pakets ein eigenes Benutzerkonto. Die Payload in den schadhaften NPM-Paketen, welche auf Azure-Entwickler abzielen, dient dem Diebstahl persönlicher identifizierbarer Informationen. Wenn diese ausgeführt wird, listet sie den Inhalt verschiedener lokaler Ordner auf, erfasst Benutzernamen, Benutzerordner und den Ordner, in dem der Benutzer aktuell arbeitet, sowie die IP-Adresse des Netzwerkinterfaces und die IP-Adressen der konfigurierten DNS-Server. Alle gesammelten Informationen werden an Command-and-Control-Server der Angreifer gesendet, über den auch die Koordination des Angriffs erfolgt.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Angreifer laden Pakete aus dem Repository herunter und versehen diese mit eigenem schadhaftem Programmcode. Danach verändern sie den Namen der Pakete minimal, z.B. durch Vertauschen von Buchstaben, was als Typosquatting bezeichnet wird und laden die schadhaften Pakete auf das Repository hoch. Möchte ein Entwickler ein

Paket herunterladen lädt er möglicherweise versehentlich das schadhafte Paket herunter. Da viele Pakete pro Woche mehrere Millionen Mal heruntergeladen werden, besteht eine hohe Wahrscheinlichkeit, dass einige Entwickler Opfer des Typosquatting-Angriffs werden. Eine andere Angriffsmöglichkeit bietet die so genannte Abhängigkeitsverwirrung, bei der das schadhafte Paket mit einer sehr hohen Seriennummer ausgestattet wird. Da automatisierte Updateprozesse die aktuelle Paketversion mit der höchsten Seriennummer aus dem Repository herunterladen, wird dann die schadhafte Paketversion auf dem System des Entwicklers installiert. Insgesamt besteht der Lieferkettenaspekt im Wesentlichen somit darin, dass Abhängigkeiten bzw. externe Programmelemente von Angreifern modifiziert werden, sodass die Opfer unbemerkt illegitimen bzw. mit Schadsoftware behafteten Code einbinden.

Signifikante Auswirkungen

Die von den Azure-Entwicklern gestohlenen Informationen beinhalten IP-Adressen und den Namen des Ordners, in dem der Entwickler arbeitet. Diese Informationen könnten für spätere, schwerwiegende Lieferkettenangriffe genutzt werden, um über schadhafte NPM-Pakete Schadsoftware in den Softwareentwicklungsprozess einzuschleusen.

3.2.8 Cyberangriff auf Adesso

Verwendete Quelle(n): /ADE23w01, AKA22w01, BSI23i13, HEI23w15, INS23w01, SUE23w01/

Kurzüberblick

Anfang 2023 wurde bekannt, dass der deutsche IT-Dienstleister Adesso Opfer eines Cyberangriffs wurde, wobei im Wesentlichen durch die Angreifer Informationen eingesehen und Daten heruntergeladen wurden. Zum Kundenkreis des Unternehmens zählen neben Behörden der Bundes-, Landes- und Kommunalverwaltung (z. B. das BKA und die Bundesbank) auch Betreiber kritischer Infrastrukturen wie beispielsweise die Energieversorgungskonzerne RWE und Eon. Das BSI hat zu diesem IT-Sicherheitsvorfall eine Cyber-Sicherheitswarnung veröffentlicht, aus der hervorgeht, dass sich die Angreifer möglicherweise über Monat hinweg unerkannt im Netzwerk befanden und somit Zugriff u. a. über VPN-Verbindungen auch auf die Netzwerke der Kunden von Adesso hatten.

Entdeckung des IT-Sicherheitsvorfalls

Über die Entdeckung des IT-Sicherheitsvorfalls durch Adesso liegen keine Informationen vor. Durch die mutmaßliche Meldung des IT-Sicherheitsvorfalls eines Mitarbeiters von Adesso an das BSI sowie einige Medien wurden Informationen diesbezüglich öffentlich bekannt. Nachdem Adesso am 11. Januar 2023 die Aktivitäten der Angreifer entdeckt hat, wurden einige kompromittierte Nutzerkonten geschlossen und ein Microsoft-Ermittler-Team informiert.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Die Angreifer nutzten eine Schwachstelle bzw. einen Zero-Day-Exploit in der vom Unternehmen Atlassian entwickelten Software Confluence, die für die Dokumentation und Kommunikation von Wissen und den Wissensaustausch in Unternehmen und Organisationen verwendet wird, aus. Die Schwachstelle (CVE-2022-26134) ermöglicht potenziellen Angreifern die Ausführung beliebigen Codes (remote code execution) ohne Authentifizierung.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die Angreifer nutzten eine Schwachstelle bzw. einen Zero-Day-Exploit in der vom Unternehmen Atlassian entwickelten Software Confluence aus, welche von Adesso eingesetzt wird. Somit erlangten die Angreifer initialen Zugriff auf das Netzwerk von Adesso über deren Lieferkette, bevor weitere Angriffsschritte durchgeführt wurden und der klassische Lieferkettenangriff auf Kunden von Adesso ausgeführt wurde.

Signifikante Auswirkungen

Zu den Auswirkungen des Angriffs liegen nur begrenzt Informationen vor. Adesso selbst bestätigt, dass Angreifer Zugriff auf Informationen hatten und Daten exfiltriert wurden, wobei keine Angaben zu genaueren Inhalten oder betroffenen Kunden gemacht wurden. Zu den Kunden von Adesso zählen dabei auch Unternehmen, die ggf. im Zusammenhang mit kerntechnischen Anlagen und Einrichtungen stehen wie beispielsweise das Unternehmen RWE. Bislang liegen jedoch keine Informationen zu einem konkreten kerntechnischen Bezug vor.

3.2.9 IT-Sicherheitsvorfall im Zusammenhang mit 3CX VoIP-Desktop App

Verwendete Quelle(n): /3CX23w01, MAN23r02, SEN23r01/

Kurzüberblick

Am 20. April 2023 veröffentlichte der Informationssicherheitsdienstleister Mandiant einen umfassenden Bericht zum bekannt gewordenen IT-Angriff auf Kunden des Voice-over-IP (VoIP)-Software Anbieters 3CX, welcher am 1. April 2023 bekannt wurde. Die Angreifer erlangten Zugriff auf die Systeme von 3CX und platzierten eine mit Schadsoftware versehene Version der von 3CX bereitgestellten 3CX Desktop App auf der Webseite von 3CX. Erstmalig am 29. März bekannt geworden, war für einen unbekannten Zeitraum eine offiziell sich im Umlauf befindende Version der 3CX Desktop App für VoIP mit Schadcode versehen. Die Version war offiziell vom Hersteller signiert und wurde vom Hersteller auf dessen Webseite zur Nutzung angeboten. Es ist unbekannt, wie viele Kunden von 3CX tatsächlich betroffen waren, jedoch wurde von 3CX ausgesagt, dass *„eine signifikante Anzahl*“ ihrer Kunden betroffen sind. 3CX hat nach eigenen Angaben mehr als 600.000 Kunden. Besondere Aufmerksamkeit erhielt der Angriff, weil die ursprünglichen Zugriffe der Angreifer auf 3CX selbst durch einen Lieferkettenangriff über Software des Unternehmens Trading Technologies möglich wurde. Als Reaktion auf den Angriff wurden die Kunden aufgerufen die 3CX Desktop App von ihren Systemen zu entfernen und die Browserversion zu verwenden, später wurden bereinigte Versionen mit neuen Zertifikaten veröffentlicht.

Entdeckung des IT-Sicherheitsvorfalls

Gemäß wurde die Software 3CX Desktop App erstmalig ab dem 22 März 2023 auffällig. Die breite Öffentlichkeit wurde am 29. März 2023 durch mehrere Berichte in einschlägigen Medien auf den Fall bekannt. In den darauffolgenden Tagen erfolgten weitere Medienveröffentlichungen sowie eine Warnung von 3CX. Die Vorbereitung des Angriffs wurde womöglich bereits im Februar 2022 begonnen, als die für weiterführende Angriffe notwendige IT-Infrastruktur und Webadresse registriert wurden. Derzeit liegen keine weitergehenden Informationen mit Einzelheiten zur Entdeckung des IT-Sicherheitsvorfalls vor.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. Schwachstellen

Der IT-Angriff über die 3CX Desktop App ist ein zweistufiger Lieferkettenangriff, bei welchem auch das Unternehmen 3CX Opfer eines weiteren Lieferkettenangriffs wurde. Die Schadsoftware, mit welche 3CX selbst über die Lieferkette angegriffen wurde, ist ein Remote Access Trojaner, welcher eine persistente Backdoor für weiterführende Maßnahmen, laterale Verbreitung und dauerhaften Zugriff auf die Systeme installiert. Die in die 3CX Desktop App integrierte Schadsoftware dient dem Nachladen weiterer Schadsoftware, welche nach bisherigen Erkenntnissen insbesondere dem Auslesen und Kopieren von Daten dient. Nach bisherigen Informationen wurde der Trojaner innerhalb einer ausführbaren DLL-Datei der Software 3CX Desktop App platziert und die schadhafte Softwareversion durch offizielle Zertifikate legitimiert. Wurde die Schadsoftware aktiviert, wurde zuerst Kontakt zu einem Github – Repository aufgenommen und weitere Schadsoftware nachgeladen, was schließlich zum Nachladen der dritten Stufe der Schadsoftware führte, eine Infostealer Schadsoftware als DLL. Die Schadsoftware wurde für Windows- und MacOS-Betriebssysteme entwickelt.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Die ursprünglichen Zugriffe auf die Systeme von 3CX erfolgten über einen Lieferkettenangriff auf das Unternehmen Trading Technology, dessen Softwarepaket für die Buchhaltung X_TRADER mit einer Schadsoftware versehen war. X_TRADER wird seit 2020 nicht mehr vom Hersteller unterstützt, war jedoch noch 2022 von der Webseite herunterladbar und wurde bei 3CX auf einem einzelnen System für Buchhaltungsaufgaben genutzt. Die identifizierte schadhafte Version von X_TRADER besaß ein legitimes Zertifikat und enthielt zwei mit Schadsoftware versehene DLLs, welche zur Installation der modularen Backdoor VEILEDSIGNAL führten. Mit der frei verfügbaren Software Fast Reverse Proxy Project erlangten die Angreifer Zugriff auf weitere IT-Systeme von 3CX und ultimativ auf den Build Server, auf welchem die aktuellen Versionen der 3CX-Software gespeichert und vereinheitlicht werden. Auf dem Build-Server konnte mit Hilfe der Schadsoftware TAXHAUl und COLDCAT sowie IKEEXT die Microsoft Windows Umgebung übernommen werden, die MacOS-Umgebung mit der Schadsoftware POOLRAT und anschließend schadhafte Versionen der 3CX Desktop App erzeugt werden.

Schließlich wurden mehrere Versionen der 3CX Desktop App mit Schadsoftware versehen und den Kunden von 3CX über die offiziellen Kanäle zur Verfügung gestellt. Die

Schadsoftware führt zum Nachladen von weiteren Schadsoftwares, welche schließlich insbesondere dem Auslesen und Kopieren von Daten dienen.

Signifikante Auswirkungen

Wie viele Kunden von Trading Technologies durch die erste Stufe des Lieferkettenangriffs betroffen sind, ist nicht bekannt. Bis zur Aufdeckung der Kompromittierung von 3CX war der IT-Angriff auf Trading Technologies und die Software X_Trader nicht bekannt geworden und es sind nur sehr wenige Informationen über diesen Angriff hinaus bekannt. 3CX selbst besitzt über 600.000 Kunden in unterschiedlichen Industrie- und Dienstleistungsbranchen und gibt an, dass ein signifikanter Teil der Kunden betroffen sei. Kunden, die betroffen sind, wurden mit hoher Wahrscheinlichkeit Opfer eines Abflusses von gespeicherten und verarbeiteten Informationen.

3.2.10 Cyberangriffe auf Bitmarck

Verwendete Quelle(n): /BIT23r01, BIT23r02, BTB23w01, HEI23w14/

Kurzüberblick

Am 30. April 2023 wurde bekannt, dass der IT-Dienstleister Bitmarck Opfer eines Cyberangriffs wurde. Bitmarck selbst ist Dienstleister insbesondere für deutsche gesetzliche Krankenkassen und bearbeitet hierbei die Daten von mehr als 20 Millionen Patienten für mehr als 80 Krankenkassen. Der Cyberangriff veranlasste Bitmarck dazu, seine IT-Dienstleistungen zwischenzeitlich auszusetzen und die IT-Systeme des Unternehmens vom Netz zu nehmen. In der Folge konnten die Krankenversicherungen nicht mehr auf Patientendaten zugreifen, Krankschreibungen über die digitalen Systeme ausstellen und teilweise konnten Ärzte nicht mehr auf die elektronischen Patientenakten der bei den betroffenen Krankenkassen Versicherten zugreifen. Bereits im Januar 2023 wurde Bitmarck Opfer eines Cyberangriffes, bei welchem später bekannt wurde, dass bis zu 300.000 Kundendaten verschiedener Krankenkassen durch Angreifer entwendet wurden, darunter persönliche Daten wie Geburtsdatum, Versichertennummern und Krankenkassenkarten-Seriennummern sowie Passwortdaten, jedoch keine medizinischen Daten. Die Daten beinhalteten keine medizinischen Informationen, jedoch andere personenbezogene Daten. Gemäß Bitmarck erlangte „*ein unberechtigter Dritter*“ kurzfristig Zugriff auf ein einzelnes IT-System mittels gestohlener Zugangsdaten. Ende April wurde Bitmarck dann Opfer eines schwerwiegenden IT-Angriffes, in dessen Konsequenz

Bitmarck sämtliche IT-Systeme herunterfuhr und nach einem längeren Zeitraum wieder in Betrieb nahm. Die Wiederinbetriebnahme aller von Bitmarck geleisteten Dienstleistungen dauerte bis in den Juli 2023 an. Es ist nicht bekannt, auf welche Art die Angreifer Zugriff auf die Bitmarck Systeme für diesen Angriff erlangten oder welche schadhaften Handlungen ausgeführt wurden. Nach Angaben von Bitmarck wurden keine Daten gestohlen und der Angriff in einem frühen Stadium durch das Herunterfahren der IT-Infrastruktur unterbunden.

Entdeckung des IT-Sicherheitsvorfalls

Der IT-Angriff vom Januar 2023 wurde von Bitmarck nach bisherigen Erkenntnissen erst nachträglich aufgedeckt, als der Angreifer seine Erbeutung bekannt gab. Zugegriffen wurde über gestohlene Zugangsdaten. Der IT-Angriff vom April 2023 wurde gemäß Bitmarck frühzeitig entdeckt, worauf sich das Unternehmen zum Herunterfahren aller IT-Systemen entschied. Es wurde bisher nicht dargelegt, auf welche Weise der Cyberangriff vom April 2023 erkannt wurde, nur, dass dieser sich in einem frühen Stadium befunden hat.

Eingesetzte IT-Angriffswerkzeuge und Schadsoftwarekomponenten bzw. ausgenutzte Schwachstellen

Beim IT-Angriff im Januar 2023 wurden bereits vor dem Angriff gestohlene Zugangsdaten für den IT-Angriff angewendet, mit welchen die Angreifer Zugriff auf ein einzelnes IT-System von Bitmarck erlangten. Dabei wurde über auf unbekanntem Wege gestohlene Zugangsdaten auf mindestens ein IT-System zugegriffen. Es ist nicht bekannt, ob hierbei Schadsoftware zum Einsatz kamen oder alleinig die Zugriffsrechte für die Entwendung von Daten genutzt wurden.

Für den IT-Angriff im April 2023 gibt es derzeit keine näheren Informationen zu den IT-Angriffswerkzeugen und Schadsoftwarekomponenten.

Angriffshandlungen/spezifische Aspekte im Zusammenhang mit der Lieferkette

Bitmarck selbst ist Dienstleister innerhalb der Lieferkette für deutsche Krankenkassen. Der erste IT-Angriff gelang durch bestehende, gestohlene Zugangsdaten auf mindestens ein Einzelsystem. Die Art und Weise, wie beim zweiten Angriff vorgegangen wurde, ist bisher nicht bekannt.

Signifikante Auswirkungen

Der IT-Angriff vom Januar 2023 hatte die Folge, dass die personenbezogenen Daten von mehr als 300.000 Kunden bzw. Mitarbeitern der von Bitmarck unterstützten Krankenkassen der Öffentlichkeit zugänglich gemacht wurden. Darüber hinaus gab es keine bekannten Folgen.

Der IT-Angriff vom April 2023 führte zu einer temporären Aussetzung aller Dienstleistungen von Bitmarck für die Krankenkassen, sodass potenziell für mehr als 20.000.000 Versicherten Krankenkassendienstleistungen teilweise nicht zur Verfügung standen, teilweise auch nicht die elektronischen Patientenakten. Weiterhin gab es Einschränkungen bei den elektronischen Arbeitsunfähigkeitsbescheinigungen sowie dem elektronischen Arztbrief. Arztpraxen konnten in der Phase der Einschränkungen keine elektronischen Daten an die betroffenen Versicherungen übersenden. Auch Krankengeldzahlungen waren temporär betroffen. Die Wiederherstellung des Normalbetriebes von Bitmarck dauerte mehr als zwei Monate.

4 Analyse nationaler und internationaler Vorgehensweisen zur Sicherstellung der IT-Sicherheit in der Lieferkette

Im Rahmen des Vorhabens wurden sowohl nationale wie auch internationale Regelwerke bezüglich Anforderungen, Maßnahmen und Regelungen zur Sicherstellung der IT-Sicherheit in der Lieferkette ausgewertet. National wurden dabei zunächst das IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI), 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)“* des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit und das zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) betrachtet. Außerdem wurden einschlägige nationale Regelwerke aus Finnland, den USA und Großbritannien ausgewertet. Bezüglich des internationalen Regelwerks wurden verschiedene Dokumente der Internationalen Atomenergie-Organisation (IAEA) sowie unterschiedliche Normen ausgewertet.

Dabei ist das betrachtete Regelwerk zunächst bezüglich der jeweiligen grundlegenden Struktur und Form zu unterscheiden. Generell gibt es unterschiedliche Ansätze, wie mit Hilfe von Regelwerken bestimmte Zielvorgaben gesetzt, umgesetzt und erreicht werden können. Bei einem leistungsbasierten Ansatz („performance-based approach“) liegt der Fokus nicht auf vorgeschriebenen Prozessen, Techniken oder Verfahren, sondern auf definierten Ergebnissen. Definierte Ziele sollen dabei erreicht werden, ohne dass spezifische Anweisungen oder Maßnahmen vorgegeben werden, wie die Ziele zu erreichen sind. Dagegen werden bei einem präskriptiven Ansatz („prescriptive approach“) spezifische Schritte bzw. Maßnahmen zur Erreichung definierter Ziele konkret vorgegeben. Beide Ansätze haben jeweils Vor- und Nachteile in der konkreten Umsetzung. Der präskriptive Ansatz bietet durch konkrete Maßnahmen beispielsweise einheitliche Vorgaben, die den Adressaten der Richtlinie dadurch Orientierungshilfen für die Umsetzung bieten und deren Erfüllung unter Umständen einfacher nachzuweisen ist. Diese konkreten Vorgaben sind allerdings in dem sich sehr schnell und dynamisch entwickelnden Bereich der Cybersicherheit unter Umständen nach kurzer Zeit überholt und nicht mehr Stand von Wissenschaft und Technik. Bei einem leistungsbasierten Ansatz hat der Adressat oftmals größere Freiheiten zur Erreichung der festgesetzten Ziele und kann ggf. einzelne Maßnahmen an die im Bereich Cybersicherheit dynamischen Entwicklungen von Wissenschaft und Technik leichter anpassen. Andererseits werden einzelne

relevante Aspekte im Regelwerk ggf. nicht dediziert adressiert und die Nachweisführung zur Umsetzung gestaltet sich möglicherweise aufwändiger.

In vielen Regelwerken findet sich eine Kombination aus leistungsbasierten und präskriptiven Aspekten. Dies ist insbesondere im Zusammenhang mit dem Aspekt Cybersicherheit in der Lieferkette festzustellen, wobei hier bisher sehr wenige präskriptive Anforderungen in Regelwerken vorhanden sind und das Thema hauptsächlich im Rahmen eines leistungsbasierten Ansatzes adressiert ist. Mit der insbesondere internationalen Zunahme der Publikation neuen Regelwerks mit dediziertem Fokus auf das Themengebiet Cybersicherheit in der Lieferkette ist eine Entwicklung von rein leistungsbasierten Ansätzen in diesem Zusammenhang hin vermehrt präskriptive Vorgaben enthaltenen Regelwerken zu erwarten und in Ansätzen bereits zu erkennen. Beispielsweise gibt es neue Veröffentlichungen unter anderem der IAEA (Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain) zu diesem Thema. Im Folgenden werden die im Rahmen des Vorhabens ausgewerteten Regelwerke kurz vorgestellt und die für das Vorhaben relevanten Aspekte zusammengefasst, bevor in Abschnitt 4.3 das deutsche Regelwerk mit den internationalen Ansätzen verglichen wird.

4.1 Nationales Regelwerk

Bezüglich der Auswertung nationaler Regelwerke wurden im Rahmen des Vorhabens verschiedene Regelwerke und Dokumente aus Deutschland, den Vereinigten Staaten, Großbritannien sowie Finnland betrachtet. Dabei wurden insbesondere entsprechende Veröffentlichungen von Behörden ausgewählt, die jeweils im Zusammenhang mit der nationalen Aufsicht bzgl. kerntechnischer Anlagen und Einrichtungen stehen. Zudem wurden einschlägige Veröffentlichungen von Behörden und Institutionen betrachtet, die im Rahmen ihre Geschäftsbereiche für das Vorhaben relevante Fragen zur Cybersicherheit im Zusammenhang mit der Lieferkette adressieren.

4.1.1 Deutschland

In Deutschland ist in Bezug auf Fragen zur Cybersicherheit in allen Bereichen zunächst das Bundesamt für Sicherheit in der Informationstechnik als wichtigste Instanz zu nennen. Dabei ist der sogenannte IT-Grundschutz eine vom BSI kontinuierlich weiterentwickelte und frei verfügbare Vorgehensweise, um ein ganzheitliches Informationssicherheits-Managementsystem in Institutionen umzusetzen. In diesem Zusammenhang

enthält das IT-Grundschutz-Kompendium für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen sowie weiterführende Informationen. Da Fragen zur nuklearen Aufsicht in Deutschland in den Verantwortungsbereich des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz fallen, ist für das Vorhaben hier im Wesentlichen die vom BMU veröffentlichte „*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)*“ relevant. Zudem wurde im Jahr 2021 im Bundesgesetzblatt das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 veröffentlicht, in dem u. a. relevante Aspekte zur Sicherstellung der Cybersicherheit kritischer Infrastrukturen adressiert werden. Das Regelwerk des vom BMUV gebildeten Kerntechnischen Ausschusses in Bezug auf das Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems (KTA 3501) wurde weiterhin bezüglich für das Vorhaben relevanter Aspekte analysiert. Im Folgenden werden diese Veröffentlichungen kurz vorgestellt und hinsichtlich für das Vorhaben relevanter Aspekte analysiert.

BSI IT-Grundschutz

Das von dem Bundesamt für Sicherheit in der Informationstechnik herausgegeben IT-Grundschutz-Kompendium befasst sich mit konkreten Anforderungen zur Umsetzung des sogenannten IT-Grundschutzes. Der IT-Grundschutz stellt dabei ein fachliches Fundament und Arbeitswerkzeug zur Gewährleistung der Informationssicherheit dar. Dabei werden Methoden, Handlungsanweisungen, Empfehlungen und weltweit anerkannte Standards vereint. Das IT-Grundschutz-Kompendium besteht im Wesentlichen aus verschiedenen IT-Grundschutz-Bausteinen, die umfassende Sicherheitsaspekte der jeweiligen Themen beleuchten. Diese Bausteine sind dabei im Wesentlichen folgendermaßen aufgebaut:

1. Beschreibung/Abgrenzung des jeweiligen Sachverhalts.

2. Darstellung der jeweiligen Gefährdungslage, Angabe von Beispielen.

3. Darstellung der Sicherheitsanforderungen:

- Fundamentale Basis-Anforderungen, die stets umzusetzen sind, sofern keine gravierenden Gründe dagegensprechen.

- Zusätzlich zu erfüllende Standard-Anforderungen, die für den normalen Schutzbedarf grundsätzlich umzusetzen sind, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden.

- Anforderungen im Falle eines erhöhten Schutzbedarfes, wobei es sich um exemplarische Vorschläge handelt, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Die grobe Unterteilung dieser Bausteine beinhaltet „Prozess-Bausteine“ und „System-Bausteine“, wobei die Prozess-Bausteine weiter unterteilt werden in die Bereiche „Sicherheitsmanagement“ (ISMS), „Organisation und Personal“ (ORP) , „Konzepte und Vorgehensweisen“ (CON), „Betrieb“ (OPS), „Detektion und Reaktion“ (DER) und System-Bausteine weiter unterteilt werden in die Bereiche „Anwendungen“ (APP), „IT-Systeme“ (SYS), „Industrielle IT“ (IND), „Netze und Kommunikation“ (NET) und „Infrastruktur“ (INF). Abbildung 1 zeigt eine Übersicht über das Schichtmodell der IT-Grundschutz-Bausteine. Des Weiteren werden „Elementare Gefährdungen“ (G) betrachtet. Zudem existieren für einige der Bausteine Umsetzungshinweise, die vertiefte Informationen zur jeweiligen Umsetzung der einzelnen Maßnahmen bereitstellt. Das IT-Grundschutz-Kompendium wird vom BSI fortwähren aktualisiert und in der Regel im jährlichen Rhythmus neu veröffentlicht. Im Rahmen des Vorhabens wurde die im Jahr 2021 veröffentlichte Version des IT-Grundschutz-Kompendiums betrachtet. /BSI21r05/

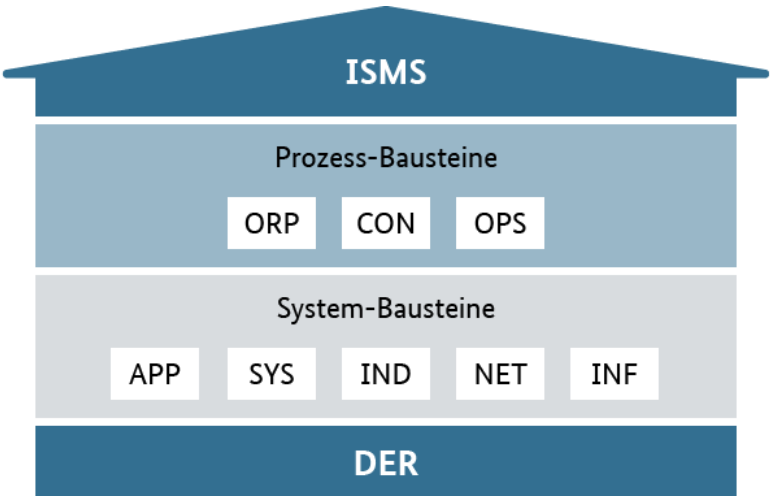

Abb. 4.1 IT-Grundschutz-Bausteine. /BSI21r05/

In Bezug auf die IT-Sicherheit der Lieferkette wurden zunächst die den einzelnen Bausteinen vorangestellten 47 elementaren Gefährdungen betrachtet, die das BSI im Rahmen des IT-Grundschutzes identifiziert. Die Abschnitte zu den elementaren Gefahren dienen dabei zur Beschreibung der jeweiligen Gefahr sowie als Referenzpunkt für die jeweiligen Grundschutz-Bausteine, die entsprechend referenziert werden. Dabei werden bezüglich einzelner Gefahren abseits von einzelnen Beispielen zur Illustration keine konkreten Szenarien sowie keine Maßnahmen zum Schutz oder zur Abwendung vorgegeben oder diskutiert. Im Wesentlichen geht es somit um die Auflistung und Beschreibung denkbarer und möglicher Gefahren in Bezug auf die Cybersicherheit.

Im Rahmen des Vorhabens wurde zunächst analysiert, ob bzw. inwieweit Gefahren in Bezug auf die Cybersicherheit im Zusammenhang mit der Lieferkette im IT-Grundschutz-Kompendium des BSI dediziert adressiert sind und entsprechend bei der Diskussion elementarer Gefahren genannt werden. Die Kompromittierung der Lieferkette von IT-Systemen ist explizit keine der 47 im IT-Grundschutz-Kompendium genannten elementaren Gefahren. Es wurden jedoch einige elementare Gefahren identifiziert, die im Kontext der Cybersicherheit der Lieferkette relevant sind. In diesem Zusammenhang ist zunächst die elementare Gefährdung G 0.11 „Ausfall oder Störung von Dienstleistern“ zu nennen. Dabei wird unter anderem auf die Gefahren eines Ausfalls von externen Dienstleistungen hingewiesen, sofern diese in Anspruch genommen werden. Ausfälle von IT-Systemen beim Dienstleister oder der Kommunikationsanbindungen zu diesem, wodurch Geschäftsprozesse beeinträchtigt werden können, werden konkret angesprochen. Die genannten beispielhaften Ursachen für Ausfälle oder Störungen handeln von allgemeinen Ereignissen, wie beispielsweise Naturgewalten oder Personalausfall sowie den Qualitätsanforderungen nicht gerecht werdende Dienstleistungen, wobei der Aspekt gezielter Cyberangriffe bzw. der IT-Sicherheit nicht explizit angesprochen wird. Weiterhin wird mit der elementaren Gefährdung G 0.20 „Informationen oder Produkte aus unzuverlässiger Quelle“ darauf hingewiesen, dass der Einsatz von Informationen, Software oder Geräten aus unzuverlässigen Quellen bzw. nicht ausreichend geprüfter Korrektheit und Herkunft hohe Gefahren birgt, die die Integrität, Vertraulichkeit und Verfügbarkeit von IT-Systemen beeinträchtigen können. Ein weiterer wichtiger Aspekt wird mit der elementaren Gefährdung G 0.28 „Software-Schwachstellen oder -Fehler“ adressiert. Demnach können Sicherheitslücken unter Umständen von Angreifern ausgenutzt werden, um Schadsoftware einzuschleusen, unerlaubt Daten auszulesen oder Manipulationen vorzunehmen.

Abseits der oben genannten elementaren Gefährdungen, welche direkt wesentliche Aspekte und Gefährdungen im Bereich der Cybersicherheit in der Lieferkette ansprechen, lassen sich auch für andere im IT-Grundschutz-Kompendium genannte allgemeine elementare Gefährdungen in Bezug auf die Cybersicherheit in der Lieferkette relevante Punkte identifizieren. Diese allgemeinen elementaren Gefährdungen, die durch eine Kompromittierung der Lieferkette begünstigen können oder von dieser ausgehen, werden im Folgenden nicht aufgeführt, da es sich um in Bezug auf die Cybersicherheit in der Lieferkette unspezifische Gefährdungen handelt, wie beispielsweise G 0.14 „Ausspähen von Informationen (Spionage)“, G 0.21 „Manipulation von Hard- und Software“ oder G 0.22 „Manipulation von Informationen“.

Für das Vorhaben sind neben der Adressierung elementarer Gefahren und der Frage der Cybersicherheit im Zusammenhang mit der Lieferkette des IT-Grundschutz-Kompendiums insbesondere konkrete Maßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette relevant. Diesbezüglich wurden die unterschiedlichen Grundschutz-Bausteine hinsichtlich für das Vorhaben relevanter Aspekte untersucht. Zunächst wurden die Prozessbausteine betrachtet, die in der Regel für sämtliche oder große Teile eines Informationsverbunds gleichermaßen gelten. Nachfolgend werden die Prozessbausteine genannt, in denen für das Vorhaben relevante Inhalte identifiziert wurden.

Der Baustein „CON“ befasst sich mit generellen Konzepten und Vorgehensweisen, beispielsweise zum Datenschutz oder zum Kryptokonzept. Für das Vorhaben sind dabei insbesondere zwei der in CON enthaltenen Bausteine relevant. Zunächst befasst sich der Baustein CON.6 mit dem Löschen und Vernichten von Daten bzw. Informationen auf Datenträgern und zielt somit insbesondere auf die letzte Phase des Lebenszyklus „Disposal“ (vgl. Abschnitt 5.1) ab. Die Gefährdungslage ergibt sich dabei im Wesentlichen durch potenzielle Vertraulichkeitsverluste durch Restinformationen auf Datenträgern. Das IT-Grundschutz-Kompendium enthält diesbezüglich unterschiedliche Basis-Anforderungen wie beispielsweise CON.6.A2, nach dem schutzbedürftige Informationen und Datenträger sicher gelöscht oder vernichtet werden müssen, bevor sie entsorgt werden. CON.6.A11 adressiert explizit den Aspekt der Löschung und Vernichtung von Datenträgern durch externe Dienstleister, wobei darauf verwiesen wird, dass ggf. beauftragte Dienstleister ausreichend sichere und nachvollziehbare Prozesse zum Löschen und Vernichten anwenden müssen und die vom externen Dienstleister eingesetzten Verfahrensweisen zum sicheren Löschen und Vernichten mindestens die institutionsinternen Anforderungen an die Verfahrensweisen zur Löschung und Vernichtung erfüllen müssen. Dies sollte entsprechend regelmäßig überprüft werden. Weiterhin werden in diesem Baustein

Mindestanforderungen an Verfahren zur Löschung und Vernichtung (CON.6.A12) sowie Anforderungen an das Vernichten von Datenträgern auf erhöhter Sicherheitsstufe (CON.6.A14) definiert.

Der zweite insbesondere für das Vorhaben relevante Baustein ist CON.8, der sich mit Software-Entwicklung befasst. Hierbei ist einschränkend zu beachten, dass sich der Baustein um die Entwicklung der individuellen Software durch die Institution selbst oder durch einen Dritten befasst, und es nicht primär um den Einsatz von fertigen, kommerziellen Softwareprodukten geht. Für das Vorhaben sind dabei hauptsächlich Maßnahmen relevant, die sich mit der Verwendung von externen Bibliotheken und der Überprüfung externer Komponenten befassen (CON.8.A6 und CON.8.A20). Demnach ist entsprechend sicherzustellen, dass diese aus vertrauenswürdigen Quellen stammen und auf potenzielle Gefahren und Konflikte überprüft werden. Zudem wird das Thema in CON.8.A8 aufgegriffen, wonach Entwickler die Software bei Verwendung externer Bibliotheken bei Veröffentlichung sicherheitskritischer Updates anpassen müssen. Für Systeme mit erhöhtem Schutzbedarf gibt es zusätzlich Anforderungen an die verwendete Entwicklungsumgebung hinsichtlich der Auswahl vertrauenswürdiger Entwicklungswerkzeuge sowie regelmäßige Integritätsprüfungen mit kryptographischen Mechanismen entsprechend dem Stand der Technik (CON.8.A17 und CON.8.A19).

Der Baustein OPS umfasst Sicherheitsaspekte betrieblicher Art und dabei insbesondere des operativen IT-Betriebs, einerseits innerhalb der Institution und andererseits auch teilweise oder komplett durch Dritte. In Bezug auf das Vorhaben ist zunächst der Baustein OPS.1.1.3 zu nennen, der sich mit dem Patch- und Änderungsmanagement befasst. Demnach liegen in der Praxis vorhandenen Sicherheitslücken oder Betriebsstörungen oftmals mangelhafte oder fehlende Patches und Änderungen zugrunde, die von Angreifern ausgenutzt werden können. Eine wesentliche Gefährdung geht in diesem Zusammenhang von der Manipulation von Daten und Werkzeugen beim Änderungsmanagement aus. Dies umfasst beispielsweise die Manipulation von Updateservern durch Angreifer oder die Nutzung von Wartungszugängen für illegitime Handlungen. Als Basis-Anforderungen werden im Bezug zum Patch- und Änderungsmanagement unter anderem zunächst organisatorische Aspekte wie die Einführung eines Konzepts sowie die regelmäßige Suche nach entsprechend aktuellen Informationen genannt (OPS.1.1.3.A1 und OPS.1.1.3.A16). Zusätzlich gibt es Anforderungen bezüglich der Etablierung von Testverfahren neuer Hardware vor dem Einsatz (OPS.1.1.3.A9), wobei sich dies hauptsächlich auf die Überprüfung der Kompatibilität bezieht. Ein für das Vorhaben hochgradig relevanter Aspekt wird zudem in OPS.1.1.3.A10 aufgegriffen, wobei es um die

Sicherstellung der Integrität und Authentizität von Softwarepaketen geht, die nur aus vertrauenswürdigen Quellen bezogen werden sollen und mit entsprechenden Verfahren wie beispielsweise Prüfsummen oder digitalen Signaturen vor der Installation überprüft werden sollen.

Für das Vorhaben ist zudem der Baustein OPS.1.2.5 relevant, in dem das Thema Fernwartung adressiert ist. Dabei wird im Wesentlichen auf die Gefahren durch unsichere und unkontrollierte Fremdnutzung von Fernwartungszugänge, die Verwendung unsicherer Protokolle sowie eine ungeeignete Nutzung von Authentisierungsverfahren bei der Fernwartung hingewiesen. Dies ist insbesondere angesichts der typischerweise tiefgreifenden Eingriffsmöglichkeiten in die IT-Systeme und Anwendungen, die sich bei der Fernwartung ergeben, problematisch. Die Absicherung von Schnittstellen zur Fernwartung (OPS.1.2.5.A3) ist dabei eine der Basis-Anforderungen, nach der unter anderem Fernwartungsverbindungen verschlüsselt werden sollten, auf das notwendige Maß beschränkt sein und nach dem jeweiligen Fernzugriff getrennt werden müssen. Dabei sollten insbesondere Authentisierungsmechanismen eingesetzt werden, die dem Mehr-Faktor-Prinzip unterliegen (OPS.1.2.5.A17). Bei der Fernwartung durch Dritte (OPS.1.2.5.A19) sollen die einzelnen Fernwartungsvorgänge aufgezeichnet werden und im Rahmen geeigneter vertraglicher Vereinbarungen über die IT-Sicherheit betroffener Systeme muss insbesondere gewährleistet werden, dass Netze verschiedener Kunden eines externen Dienstleisters nicht miteinander verbunden werden.

Das Thema Outsourcing wird darüber hinaus unter anderem in OPS.2.1 aufgegriffen, der die Auslagerung von Geschäftsprozesse und Dienstleistungen durch Institutionen ganz oder teilweise zu externen Dienstleistern adressiert, sowohl in Bezug auf Hardware als auch auf Software. Durch das Outsourcing dürfen demnach keine unkontrollierbaren Risiken für die auslagernde Institution hinsichtlich der Informationssicherheit entstehen. Die wesentlichen identifizierten Gefahren sind dabei fehlende oder unzureichende vertragliche Regelungen zur Informationssicherheit, Abhängigkeiten von einem Dienstleister bzw. bei Ausfall von Systemen des Dienstleisters sowie Schwachstellen bei der Anbindung an den Dienstleister. Standard-Anforderungen in diesem Bereich umfassen zunächst entsprechend organisatorische Aspekte wie die Auswahl geeigneter Dienstleister, die Vertragsgestaltung sowie die Planung und Aufrechterhaltung der Informationssicherheit im laufenden Outsourcing-Betrieb (OPS.2.1.A3, OPS.2.1.A4 und OPS.2.1.A11). Zudem gibt es Anforderungen, technische Sicherungsmaßnahmen über die Anbindung der jeweiligen Netzwerke sowie den Datenaustausch zwischen Outsourcing-Partnern (OPS.2.1.A9, OPS.2.1.A10). In OPS.2.1.A15 ist zudem als Anforderung

festgeschrieben, dass Outsourcing-Kunden alle Informationen und Daten nach der Beendigung der Zusammenarbeit zurückerhalten sollen und der Outsourcing-Dienstleister alle Datenbestände nach erfolgter Rückgabe sicher löschen sollte. Korrespondierende Anforderungen an die Outsourcing-Dienstleister gibt es mit dem Baustein OPS.3.1.

Neben den Prozessbausteinen wurden auch für das Vorhaben relevante System-Bausteine identifiziert, die in der Regel konkreter auf einzelne Objekte oder Gruppen angewendet werden. Dabei ist insbesondere der Baustein SYS, der die einzelnen IT-Systeme eines Informationsverbundes betrifft, relevant hinsichtlich eingebetteter Systeme (SYS.4.3) und Wechseldatenträger (SYS.4.5). In SYS.4.3 geht es explizit um informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind und Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben übernehmen, oftmals ohne dabei vom Benutzer wahrgenommen zu werden. Ein eingebettetes System bildet dabei aus Soft- und Hardware eine funktionale Einheit, die eine definierte Aufgabe erfüllt. Die wesentlichen Gefahren hinsichtlich eingebetteter Systeme umfassen dabei unter anderem ungesicherte Ein- und Ausgabe-Schnittstellen, das Einspielen von manipulierten Software-Updates, das Eindringen und die Manipulation über die Kommunikationsschnittstelle sowie den Einsatz gefälschter Komponenten. Bezüglich des Einsatzes von eingebetteten Systemen gibt es hinsichtlich der Relevanz für das Vorhaben insbesondere Anforderungen zur Auswahl einer vertrauenswürdigen Lieferanten- und Logistikkette sowie qualifizierter Hersteller für eingebettete Systeme sowie zur sicheren Aussonderung solcher Systeme und entsprechend der Löschung sämtlicher Daten (SYS.4.3.A12 und SYS.4.3.A11). Hinsichtlich des Einsatzes von Wechseldatenträgern gibt es in SYS.4.5 angesichts zahlreicher Gefahren im Umgang, wie beispielsweise die Sorglosigkeit im Umgang mit Informationen, den Diebstahl oder Verlust von Wechseldatenträgern sowie die Verbreitung von Schadprogrammen, zahlreiche allgemeine Anforderungen hinsichtlich der Informationssicherheit. Für das Vorhaben besonders relevant sind zudem erhöhte Anforderungen bzgl. des Integritätsschutzes durch Checksummen oder digitale Signaturen, des sicheren Versand sowie der Verwendung zertifizierter Produkte.

Neben diesen explizit genannten Bausteinen und Anforderungen, die als für das Vorhaben besonders relevant identifiziert wurden, enthält das Grundschutz-Kompendium weitere Anforderungen, die zur Sicherstellung der IT-Sicherheit im Zusammenhang mit der Lieferkette beitragen können, diesen Aspekt jedoch nicht explizit adressieren, sondern die für ein angemessenes Maß an Informationssicherheit im Allgemeinen sorgen. Dabei handelt es sich beispielsweise um Bausteine zum Schutz vor Schadprogrammen oder

zur Cloud-Nutzung (OPS.1.1.4 und OPS.2.2). Zudem sind in diesem Zusammenhang die im Baustein DER behandelten Aspekte der Detektion und Reaktion zu nennen. Der Einsatz von Detektionssystemen sowie die kontinuierliche Überwachung und Auswertung von Protokollierungsdaten kann ein wesentlicher Bestandteil zur Sicherstellung der IT-Sicherheit im Zusammenhang sein, ist jedoch nicht darauf beschränkt und zählt zu grundlegenden Vorgehensweisen im Bereich Cybersicherheit. Gleiches gilt für die Anforderung, allgemein zertifizierte Software und Produkte einzusetzen, die beispielsweise im Baustein NET im Zusammenhang mit Netzwerkarchitektur und Kommunikation sowie im Baustein APP im Zusammenhang mit verwendeten Anwendungen/verwendeter Software gestellt wird. Im Baustein IND zu Sicherheitsaspekten industrieller IT wie Prozessleit- und Automatisierungstechnik, allgemeine ICS-Komponente und Speicherprogrammierbaren Steuerung gibt es gleichermaßen Anforderungen, die für die IT-Sicherheit im Zusammenhang mit der Lieferkette relevant sind, die hier jedoch nicht einzeln wiedergegeben werden sollen, da dieser Aspekt nicht explizit adressiert ist. Somit lässt sich zusammenfassend sagen, dass das Grundschutz-Kompendium in Bezug auf die Sicherstellung der IT-Sicherheit in der Lieferkette einerseits dieses Thema in verschiedenen Bausteinen explizit adressiert und andererseits allgemeine Anforderungen an die Cybersicherheit bietet, die durch die Umsetzung zu diesem Thema beitragen. Die Anforderungen selbst umfassen dabei sowohl organisatorische als auch technische Aspekte und sind vom Ansatz teilweise leistungsbasiert und teilweise präskriptiv.

SEWD-Richtlinie IT

Die SEWD-Richtlinie IT /BMU13n03/ unterliegt dem Geheimschutzgrad VS-Nur für den Dienstgebrauch. Die Inhalte sind entsprechend nicht für die Öffentlichkeit frei zugänglich bzw. freigegeben. Aus diesem Grund können Einzelheiten bezüglich der Inhalte, die im Rahmen der Analyse innerhalb des Vorhabens betrachtet wurden, in diesem Bericht nicht explizit wiedergegeben werden. Im Folgenden werden daher allgemeine, zusammenfassende Aussagen bezüglich der für das Vorhaben relevanten Aspekte der SEWD-Richtlinie IT diskutiert.

Grundsätzlich beschäftigt sich die SEWD-Richtlinie IT mit Maßnahmen zum Schutz von IT-Systemen der Anlagen gegen Störmaßnahmen oder sonstige Einwirkungen Dritte. Ein solcher Schutz muss zwangsläufig auch die potenziellen Risiken eines Angriffs im Zusammenhang mit der Lieferkette von IT-Systemen berücksichtigen. Dies wird unter anderem bereits aus den Begriffsbestimmungen der Richtlinie deutlich. Die IT-Sicherheit ist dabei beispielsweise nicht auf die kerntechnische Anlage oder Einrichtung beschränkt

und der Begriff der Integrität von Informationen umfasst den gesamten Lebenszyklus der Informationen von deren Erstellung bis zu ihrer Vernichtung. Auch die Anforderungen der SEWD-Richtlinie IT an die IT-Sicherheitsorganisation und die relevanten Personen machen deutlich, dass die Lieferkette von IT-Systemen für die IT-Sicherheit eine wesentliche Rolle spielt. So zählt zu den Aufgaben und Verantwortungen beispielsweise die Sicherstellung der Anwendung geeigneter Sicherungsmaßnahmen über den gesamten Lebenszyklus schutzbedürftiger IT-Systeme. In Bezug auf diesen Lebenszyklus fordert die SEWD-Richtlinie IT unter anderem für alle Phasen des Lebenszyklus von schutzbedürftigen IT-Systemen geeignete technische und organisatorische Sicherungsmaßnahmen einzuführen, konsequent anzuwenden und bei Bedarf anzupassen. Aus dem Blickwinkel der Lieferkette sind dabei beispielsweise konkrete Anforderungen in Bezug auf die Planung, Entwicklung und Beschaffung, Integration und Inbetriebsetzung und Außerbetriebnahme relevant.

Weiterhin beinhaltet die SEWD-Richtlinie IT eine Reihe von Anforderungen an Sicherungsmaßnahmen, die direkt oder indirekt auch die Lieferkette der schutzbedürftigen IT-Systeme betreffen, beispielsweise durch die Berücksichtigung aller bekannten Angriffswege. Zudem gibt es Anforderungen bezüglich des Einsatzes und der Aufbewahrung von Servicegeräten, was für die IT-Sicherheit in der Lieferkette insbesondere in Bezug auf Handlungen wie Konfiguration, Parametrierung und dem Einspielen von Updates oder Patches relevant ist. Des Weiteren gibt es Anforderungen an IT-Systeme von Auftragnehmern und Unterauftragnehmern. Zusätzlich beinhaltet die SEWD-Richtlinie IT eine generelle Anforderung an den Genehmigungsinhaber, die den Anwendungsbereich der Richtlinie auf die Lieferkette ausdehnt.

IT-Sicherheitsgesetz 2.0

Im Mai 2021 wurde im Bundesgesetzblatt das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 veröffentlicht. Im Wesentlichen bekommt das Bundesamt für Sicherheit in der Informationstechnik damit neue und weitreichende Kompetenzen als Cyber-Sicherheitsbehörde des Bundes. Das Gesetz enthält Vorschriften und Maßnahmen, die unter anderem im Zusammenhang mit der IT-Sicherheit in der Lieferkette relevant sind.

In Artikel 1 des IT-Sicherheitsgesetzes 2.0 geht es um die Änderung des BSI-Gesetzes. Dieses Gesetz nahm seinen Ursprung im Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik im Jahr 1991 und wurde seitdem mehrfach

erweitert, unter anderem im Jahr 2015 mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bezüglich der Sicherheit in der Informationstechnik Kritischer Infrastrukturen enthält das IT-Sicherheitsgesetz 2.0 eine Ergänzung des BSI-Gesetzes, nachdem Betreiber kritischer Infrastrukturen verpflichtet sind, ab dem 1. Mai 2023 im Rahmen der angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse auch Systeme zur Angriffserkennung einzusetzen. Diese Systeme *„müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten."* Die Systeme sollen weiterhin *„dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen."* (§ 8a Absatz 1a) Die Betreiber müssen die Erfüllung dieser Anforderungen regelmäßig alle zwei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen dem BSI nachweisen. Der Ansatz des Einsatzes von Methoden zur Angriffserkennung ist nicht spezifisch bzw. ausschließlich für die IT-Sicherheit in der Lieferkette relevant, erstreckt sich jedoch auf diesen Bereich. Methoden zur Angriffserkennung können insbesondere für IT-Angriffe im Bereich der Lieferkette relevant sein, wenn bisherige konventionelle Maßnahmen nur eingeschränkt möglich sind zur Erkennung und Aufdeckung von entsprechenden IT-Angriffen. Der Anwendungsbereich dieser Vorgaben erstreckt sich gemäß § 8d nicht auf Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes, jedoch ist davon auszugehen, dass entsprechende Vorgaben diesbezüglich in Zukunft bei der Überarbeitung der SEWD-Richtlinie IT diskutiert und für kerntechnische Anlagen und Einrichtungen ebenfalls festgeschrieben werden.

Darüber hinaus verpflichtet das IT-Sicherheitsgesetz 2.0 Betreiber Kritischer Infrastrukturen den geplanten erstmaligen Einsatz einer kritischen Komponente dem Bundesministerium des Inneren, für Bau und Heimat (BMI) vor ihrem Einsatz anzuzeigen. Als kritische Komponenten gelten dabei IT-Produkte, die *„in Kritischen Infrastrukturen eingesetzt werden*", bei denen *„Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionalität Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können*" und *„die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift als kritische Komponenten bestimmt werden oder eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren."* Kritische Komponenten dürfen gemäß IT-Sicherheitsgesetz 2.0 nur eingesetzt werden, *„wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen*

Infrastruktur abgegeben hat.“ Aus dieser Garantieerklärung, die dem BMI vorzulegen ist, muss hervorgehen, „*wie der der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke der Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können*.“ Hersteller einer kritischen Komponente können zudem als nicht vertrauenswürdig eingestuft werden, wenn Sicherheitsüberprüfungen und Penetrationsanalysen an den Produkten und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt wird. Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit kann das BMI den Einsatz aller kritischen Komponenten eines Herstellers entsprechend untersagen. Für kritische Komponenten, also entsprechende IT-Produkte in Kritischen Infrastrukturen, muss der Hersteller also mittels einer Garantieerklärung glaubhaft nachweisen können, dass die Produkte bzw. deren technische Eigenschaften nicht spezifisch für IT-Angriffe verwendet werden können, was entsprechende Anforderungen an das Produkt auch hinsichtlich der Lieferkette mit sich bringt. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung werden vom BMI festgelegt.

KTA 3501

Das Regelwerk des vom BMUV gebildeten Kerntechnischen Ausschusses (KTA-Regelwerk) spezifiziert unter anderem die sicherheitstechnischen Anforderungen des übergeordneten Regelwerks beziehungsweise präzisiert diese. Die KTA-Regeln umfassen dabei unter anderem Fragen zur Elektro- und Leittechnik. Die KTA 3501 „*Reaktorschutzsystem und Überwachungseinrichtungen des Sicherheitssystems*“ beschäftigt sich nicht direkt mit der IT-Sicherheit oder der Lieferkette von IT-Systemen, schneidet allerdings für die IT-Sicherheit in der Lieferkette relevante Aspekte indirekt an.

Dies wird insbesondere bei den Bestimmungen für Geräte, die eine nachträgliche Justage oder Einstellung erfordern, deutlich. Für leittechnische Systeme und Einrichtungen, die leittechnische Funktionen der Kategorie A ausführen, wird beispielsweise gefordert, „*Alle Einstellvorrichtungen an A-Funktions-Einrichtungen […] so anzuordnen oder abzusichern, dass sie gegen eine ungewollte, unbeabsichtigte und selbsttätige Verstellung geschützt sind*.“ Darüber hinaus heißt es: „*Eine Zugriffsmöglichkeit von außerhalb des technischen Umfelds der A-Funktions-Einrichtungen (z. B. von den Verwaltungsgebäuden oder von außerhalb der Anlage), durch den Softwarefunktionen oder Daten beeinflusst werden können, darf nicht realisiert werden.“* Ähnliche Anforderungen enthält die

KTA 3501 auch für leittechnische Systeme und Einrichtungen, die leittechnische Funktionen der Kategorie B ausführen.

Auch enthält die KTA 3501 Anforderungen an die Softwarequalität und damit an die Entwicklung der entsprechenden Software. Für A-Funktions-Einrichtungen wird hierbei gefordert. „*Die Entwicklung und Qualifizierung der Software hat so zu erfolgen, dass eine durchgängige Nachweisführung der korrekten Arbeitsweise der Software gewährleistet ist*“.

4.1.2 Vereinigte Staaten

In den Vereinigten Staaten ist das National Institute of Standards and Technology (NIST) eine Bundesbehörde mit Zuständigkeiten und Aufgaben unter anderem in den Bereichen Metrologie und Informationstechnik, welches zentrale Richtlinien und Standards im Bereich der Cybersicherheit veröffentlicht, die unter anderem verpflichtend sind für alle US-Bundesbehörden. Die zentrale Bundesbehörde der Vereinigten Staaten für die Sicherheit von Informationstechnologie und kritischer Infrastrukturen (Cybersecurity and Infrastructure Security Agency, CISA) nimmt typischerweise Bezug auf Veröffentlichungen des NIST und veröffentlicht unter anderem Anleitungen zur Implementierung wie beispielsweise für das von der NIST veröffentlichte Cybersecurity Framework für den Nuklearsektor. Für das Vorhaben wurden insbesondere zwei Veröffentlichungen in diesem Zusammenhang identifiziert. Das NIST veröffentlichte im April 2015 im Rahmen einer „Special Publication“ das Dokument „*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*“ /NIS15r01/, welches im Mai 2022 in einer überarbeiteten Version (Revision 1) /NIS22r01/ mit dem Titel „*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*“ (weiterhin bezeichnet als NIST SP 800-161) veröffentlicht wurde. Zudem entwickelte das US-Verteidigungsministerium (Department of Defense, DoD) mit dem „Cybersecurity Maturity Model Certification“ (CMMC) ein Framework und Bewertungsrahmen zur Beurteilung der Einhaltung einer Reihe von durch das NIST veröffentlichte Standards /DOD20r01/. Im Folgenden werden diese Veröffentlichungen kurz vorgestellt und hinsichtlich für das Vorhaben relevanter Aspekte analysiert.

NIST SP 800-161

Bei der NIST SP 800-161 /NIS22r01/ handelt es sich um eine Anleitung zur Identifizierung, der Bewertung und den Umgang mit Lieferkettenrisiken für Bundesbehörden der

Vereinigten Staaten, wobei insbesondere das „*Cybersecurity supply chain risk management*“ (C-SCRM) im Rahmen des Risikomanagements diskutiert wird. Dieses umfasst das organisierte und zielgerichtete Management von Cybersicherheitsrisiken in der gesamten Lieferkette. In diesem Dokument wird allgemein hinsichtlich der Fragestellung der Sicherheit von Lieferketten auf die Begriffe „*Information and Communications Technology*“ (ICT), der neben Informationstechnik auch die Kommunikation umfasst, und „Operational Technology“[6] (OT) zurückgegriffen, die beide auf komplexen, globalen Lieferketten oftmals mit mehreren Ebenen des Outsourcings basieren. In NIST SP 800-161 wird somit allgemein die Bezeichnung „Cybersecurity“ bzw. Cybersicherheit in Bezug auf die Lieferkette verwendet, womit ICT und OT gleichermaßen berücksichtigt sind. Im Folgenden wird daher diese Begrifflichkeit bei der Diskussion von NIST SP 800-161 verwendet. Risiken für Lieferketten in Bezug auf die Cybersicherheit werden folgendermaßen beschrieben:

„[…] [T]he potential for harm or compromise that may arise from suppliers, their supply chains, their products, or their services. Cybersecurity risks throughout the supply chain are the results of threats that exploit vulnerabilities or exposures within products and services that traverse the supply chain or threats that exploit vulnerabilities or exposures within the supply chain itself.” /NIS22r01/

Die Veröffentlichung richtet sich an eine breite Leserschaft verschiedener Bereiche und Hintergründe mit Verbindung zu C-SCRM, unter anderem „chief information officers“, Hard- und Software-Entwickler, allgemein Vertreter der Industrie oder von Behörden, generell im Management tätige Personen bzw. Verantwortliche für Akquisition und Auditoren und ist entsprechend inhaltlich breit aufgestellt. Das Dokument gliedert sich dabei in mehrere Kapitel, die im Folgenden hinsichtlich für das Vorhaben relevanter Aspekte kurz inhaltlich zusammengefasst werden.

Das erste Kapitel dient als Einleitung, in der neben einer kurzen Einführung zunächst der Verwendungszweck der Veröffentlichung, das Zielpublikum und Zielgruppenprofile mit jeweiligen Leitfäden zur entsprechenden Nutzung des Dokuments beschrieben werden. Daneben werden auch erste inhaltliche Fragestellungen der Thematik der

---

[6] OT wird gemäß NIST SP 800-161 bzw. 800-37 folgendermaßen definiert*: Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.* (S. 9)

Cybersicherheit in der Lieferkette diskutiert. C-SCRM umfasst gemäß NIST SP 800-161 Aktivitäten, welche sich über den gesamten Lebenszyklus eines Systems erstrecken, einschließlich Forschung und Entwicklung, Design, Herstellung, Beschaffung, Lieferung, Integration, Betrieb und Wartung, Entsorgung und die gesamte Verwaltung der Produkte und Dienstleistungen. Die Verantwortlichkeiten und Haftungen für Dienstleistungen und damit verbundene Aktivitäten durch Zulieferer bzw. Dritte außerhalb des eigenen Ökosystems werden in der Regel durch Vertragsdokumente zwischen dem Unternehmen und den Lieferanten, Entwicklern, Systemintegratoren, externen Systemdienstleistern und anderen ICT-bezogenen Dienstleistern festgelegt. Gemäß NIST SP 800-161 erschwert eine Informationsasymmetrie zwischen dem akquirierenden Unternehmen und dem Lieferanten jedoch die Identifizierung potenzieller Cybersicherheitsrisiken. Den Unternehmen fehlt es demnach oft an Transparenz und Verständnis dafür, wie die erworbene Technologie entwickelt, integriert und eingesetzt wird und wie die erworbenen Dienstleistungen erbracht werden. Dies ist in Abbildung 1 veranschaulicht.

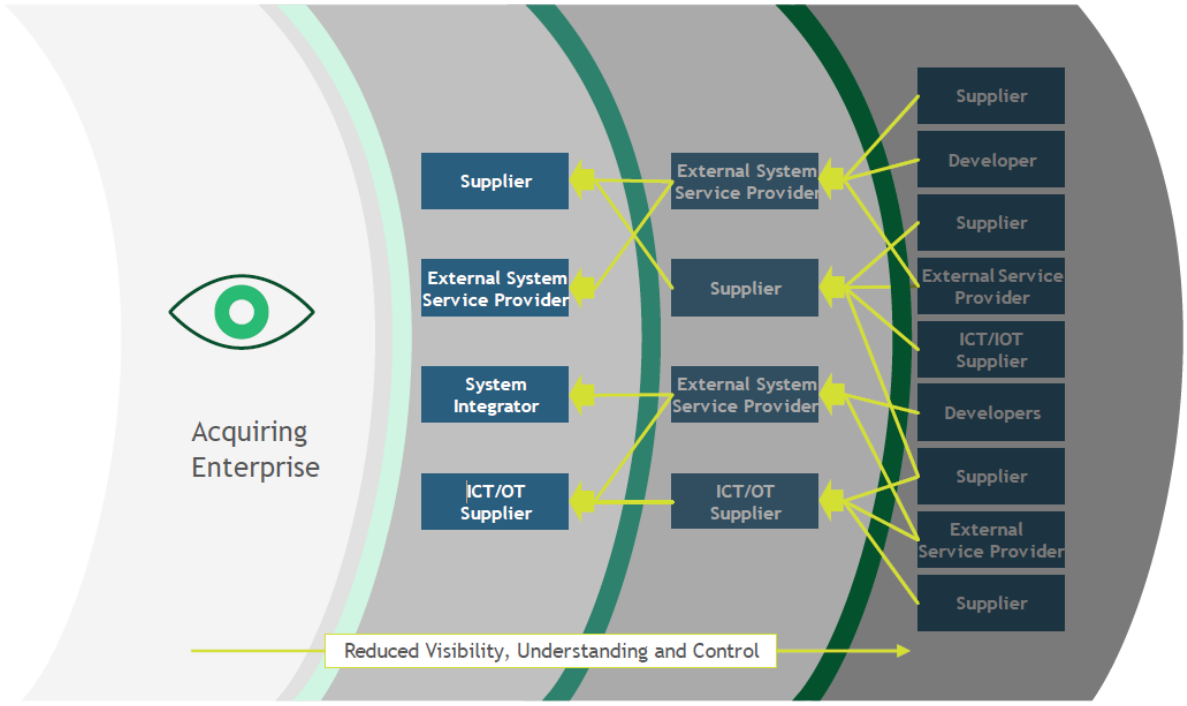

Abb. 4.2 Sichtbarkeit, Verständnis und Kontrolle der Lieferkette aus der Sicht eines Unternehmens. /NIS22r01/

In Kapitel 2 geht es neben der allgemeinen Integration von C-SCRM in das unternehmensweite Risikomanagement und der Beschreibung von Risiken für die Cybersicherheit in der Lieferkette außerdem um das sogenannte „Multilevel Risk Management“, das unter anderem im späteren Verlauf für die Beschreibung einzelner Maßnahmen zur

Sicherstellung der Cybersicherheit in der Lieferkette relevant ist. Dabei werden strategische bzw. taktische Risiken innerhalb eines Unternehmens in drei Ebenen eingeteilt (siehe Abbildung 2):

- Auf der ersten Ebene (Enterprise) geben die allgemeine C-SCRM-Strategie, die Richtlinien und der Implementierungsplan den Rahmen vor, wie C-SCRM im gesamten Unternehmen gehandhabt wird, und leiten die C-SCRM-Aktivitäten auf der Ebene der Aufgaben und Geschäftsprozesse.
- Auf Ebene 2 (Mission & Business Process) übernehmen die C-SCRM-Strategien, -Richtlinien und -Implementierungspläne der mittleren Ebene den Kontext und die Richtung, die auf Unternehmensebene festgelegt wurden, und passen sie an den spezifischen Einsatz und Geschäftsprozess an.
- Auf Stufe 3 (Operational) bilden die C-SCRM-Pläne die Grundlage für die Entscheidung, ob ein Informationssystem die geschäftlichen, funktionalen und technischen Anforderungen erfüllt und angemessen zugeschnittene Kontrollen enthält.

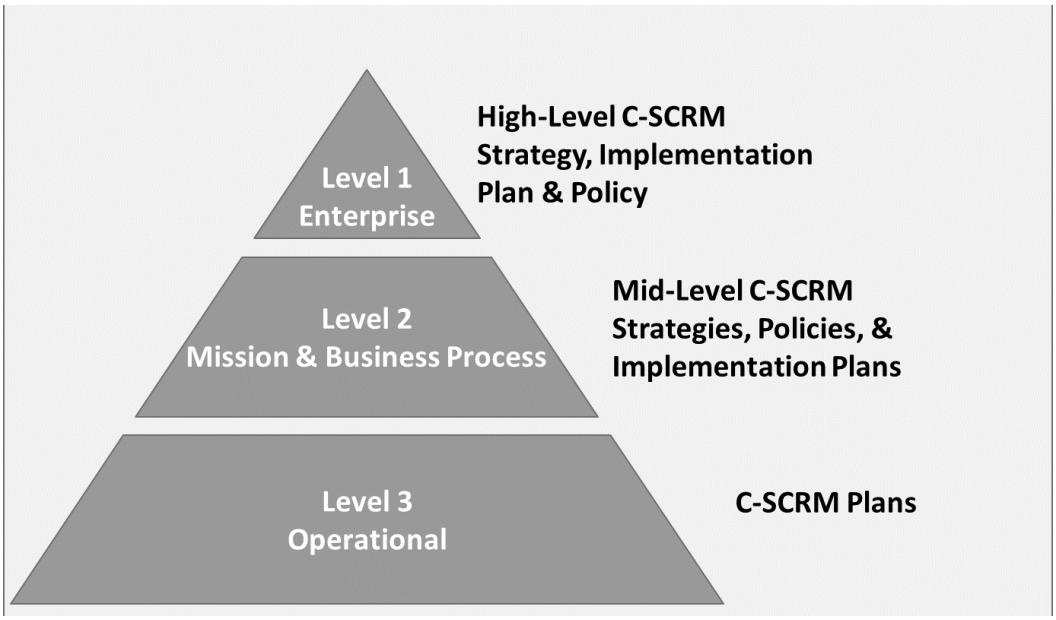

Abb. 4.3 C-SCRM im Multilevel Risk Management. /NIS22r01/

Diesen drei Ebenen werden in den folgenden Abschnitten von Kapitel 2 entsprechende Aktivitäten zugeordnet, beispielsweise die Entwicklung einer unternehmensweiten C-SCRAM-Strategie für Ebene 1, die Entwicklung entsprechender Verfahren, Leitlinien und Auflagen für Ebene 2 und die Umsetzung durch konkrete C-SCRM-Pläne und die Einführung von C-SCRM-Richtlinien und -Anforderungen für Ebene 3. Analog werden den drei Ebenen die entsprechenden Vertreter und Verantwortlichen des Unternehmens

zugeordnet, u. a. die Unternehmensführung/CEOs, CIOs usw. (Ebene 1), Projektmanagement (Ebene 2) und Systemverantwortliche/Entwickler/Ingenieure bzw. Operateure (Ebene 3).

Das dritte Kapitel beschreibt aus der Sicht des NIST sechs kritische Faktoren zur erfolgreichen Umsetzung von C-SCRM:

C-SCRM in Acquisition

Die Integration von C-SCRM-Aspekten in die Beschaffungsaktivitäten in jedem Schritt des Beschaffungs- und Vertragsmanagement-Lebenszyklus ist für die Verbesserung des Managements von Cybersicherheitsrisiken in der gesamten Lieferkette unerlässlich. Dieser Lebenszyklus beginnt damit, dass Bedarf festgestellt wird, und umfasst die Prozesse zur Planung und Formulierung von Anforderungen, zur Durchführung von Recherchen, um praktikable Bezugsquellen zu ermitteln und zu bewerten, zur Einholung von Angeboten, zur Bewertung von Angeboten, um die Konformität mit C-SCRM-Anforderungen sicherzustellen, und zur Bewertung von C-SCRM-Risiken im Zusammenhang mit dem Anbieter und dem vorgeschlagenen Produkt und/oder der Dienstleistung. Die Überwachung auf Änderungen, die sich auf die Cybersicherheitsrisiken in der Lieferkette auswirken können, sollte während des gesamten Lebenszyklus erfolgen und kann eine Neubewertung der ursprünglichen Bewertung auslösen oder eine Reaktion zur Risikominderung erfordern.

Supply Chain Information Sharing

Um die Identifizierung, Bewertung, Überwachung und Reaktion auf Cybersicherheitsrisiken in der gesamten Lieferkette zu unterstützen, sollten Unternehmen Prozesse und Aktivitäten zum Informationsaustausch in ihre C-SCRM-Programme integrieren. Dazu können Vereinbarungen über den Informationsaustausch mit anderen Unternehmen, Geschäftspartnern und Lieferanten gehören. Ein effektiver Prozess für den Informationsaustausch (Supply Chain Risk Information, SCRI) trägt dazu bei, dass Unternehmen Zugang zu Informationen erhalten, die für das Verständnis und die Minderung von Cybersicherheitsrisiken in der gesamten Lieferkette entscheidend sind, und dass relevante Informationen an andere weitergeben werden können.

C-SCRM-Training and Awareness

Zahlreiche Personen innerhalb des Unternehmens tragen zum Erfolg von C-SCRM bei. Dazu gehören unter anderem Mitarbeiter aus den Bereichen Informationssicherheit, Beschaffung, Risikomanagement, Technik, Softwareentwicklung, IT, Recht, Personalwesen und allgemeines Management. Unternehmen sollen eine allgemeine Sicherheitskultur fördern, die C-SCRM als integralen Bestandteil enthält. Dabei kann eine Vielzahl von Kommunikationsmethoden eingesetzt werden, um diese Kultur zu fördern. Jeder Einzelne in einem Unternehmen sollte eine angemessene Schulung (zum Beispiel im Rahmen der allgemeinen Schulung zum Thema Cybersicherheit) erhalten, damit er die Bedeutung von C-SCRM für sein Unternehmen, seine spezifischen Rollen und Verantwortlichkeiten sowie die Prozesse und Verfahren zur Meldung von Vorfällen versteht. Personen, die bei der Verwaltung von Cybersicherheitsrisiken in der gesamten Lieferkette eine zentrale Rolle spielen, sollen eine maßgeschneiderte C-SCRM-Schulung erhalten, die ihnen hilft, den Umfang ihrer Verantwortlichkeiten, die spezifischen Prozesse und Verfahrensimplementierungen, für die sie verantwortlich sind, zu verstehen.

C-SCRM Key Practices

C-SCRM-Schlüsselmethoden sollen eine Untergruppe der in dieser Publikation beschriebenen C-SCRM-Methoden besonders hervorheben und auf sie aufmerksam machen. Unternehmen sollten dem Erreichen einer Grundkompetenz in diesen Schlüsselpraktiken Priorität einräumen, bevor sie zu weiteren C-SCRM-Funktionen übergehen. Zu den C-SCRM-Methoden gehören die Integration von C-SCRM in das gesamte Unternehmen, die Einrichtung eines formellen Programms, die Kenntnis und Verwaltung kritischer Produkte, Dienstleistungen und Lieferanten, das Verständnis der Lieferkette eines Unternehmens, die enge Zusammenarbeit mit kritischen Lieferanten, die Einbeziehung kritischer Lieferanten in Resilienz- und Verbesserungsaktivitäten, die Bewertung und Überwachung der gesamten Lieferantenbeziehung und die Planung für den gesamten Lebenszyklus. Dazu werden grundlegende, unterstützende und verbessernde Methoden aufgeführt.

Capability Implementation Measurement and C-SCRM-Measures

Unternehmen sollen die Effizienz und Effektivität ihrer C-SCRM-Programme aktiv im Auge behalten, indem sie die Programme selbst kontinuierlich bewerten. Zusammengenommen soll dies dazu dienen, Fortschritte zu überwachen und Ergebnisse

herauszuarbeiten, die letztlich auf eine Verringerung der Risikoexposition und zu einer Verbesserung der Sicherheit des Unternehmens führen. Unternehmen sollen eine Feedbackschleife mit den Beteiligten entwickeln, um sicherzustellen, dass die ergriffenen Maßnahmen kontinuierlich die gewünschten Erkenntnisse liefern und mit den übergeordneten strategischen Zielen des Unternehmens für C-SCRM in Einklang stehen.

Dedicated Resources

Um Cybersecurity-Risiken in der gesamten Lieferkette angemessen zu begegnen, sollen Unternehmen Mittel für diese Bemühungen bereitstellen. Die Ermittlung des Ressourcenbedarfs und die Ergreifung von Maßnahmen zur Sicherstellung einer angemessenen, wiederkehrenden und zweckgebundenen Finanzierung sind wesentliche und wichtige Aktivitäten, die in die C-SCRM-Strategie und -Umsetzungsplanung integriert und in die Budgetierungs-, Investitionsprüfungs- und Mittelverwaltungsprozesse eines Unternehmens aufgenommen werden müssen. Der Zugang zu angemessenen Ressourcen ist eine entscheidende Voraussetzung für die Einrichtung und Aufrechterhaltung einer C-SCRM-Programmkapazität.

Im Rahmen des Vorhabens sind zudem insbesondere die in Anhang A von NIST SP 800-161 Rev. 1 aufgeführten C-SCRM Sicherungsmaßnahmen („Security Controls“) relevant, die folgendermaßen definiert werden:

„The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.” /NIS22r01/

Dies umfasst somit unter anderem Schutz- und Gegenmaßnahmen, um die Vertraulichkeit, Integrität und Verfügbarkeit eines IT-Systems zu schützen. Die Maßnahmen basieren auf bereits mit NIST SP 800-53 Rev. 5 eingeführte Maßnahmen zum Thema „*Security and Privacy Controls for Information Systems and Organizations“.* In Anhang A von NIST SP 800-161 Rev. 1 werden C-SCRM-bezogene Maßnahmen aus NIST SP 800-53 Rev. 5 identifiziert und durch zusätzliche Hinweise ergänzt, sowie gegebenenfalls neue Maßnahmen eingeführt. Im Zusammenhang mit C-SCRM nicht relevante Maßnahmen werden nicht aufgeführt. Die C-SCRM-Maßnahmen sind dabei in 20 Kategorien eingeteilt und umfassen über 180 allgemeine Einzelmaßnahmen aus den Bereichen Prävention, Detektion und Reaktion in Bezug auf Cybersicherheit, die jeweils um im

Zusammenhang mit C-SCRM relevante Hinweise ergänzt wurden. Die Kategorien umfassen die folgenden Themen:

- Access Control
- Awareness and Training
- Audit and Accountability
- Assessment, Autorization and Monitoring
- Configuration Management
- Contengency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Program Management
- Physical and Environmental Protection
- Planning
- Program Management
- Personell Security
- Personally Identifiable Information Processing and Transparency
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Supply Chain Risk Management

DoD Cybersecurity Maturity Model Certification

Das CMMC-Framework /DOD20r01/ bietet ein Modell für Auftragnehmer in der Verteidigungsindustrie in den Vereinigten Staaten, um Sicherheitsanforderungen der NIST SP 800-171 Rev 2 („*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations“)* zu erfüllen. Dabei ist das Thema IT-Sicherheit in der Lieferkette ein zentraler Bestandteil, wobei Prozesse und Methoden zur Erhöhung der IT-Sicherheit in der Lieferkette in 5 Ebenen unterteilt werden (siehe Abbildung 3). Die Anforderungen an die IT-Sicherheit steigen mit den Ebenen an. Dabei sind die Ebenen kumulativ, sodass

zur Erfüllung der Sicherheitsanforderungen einer Ebene auch alle Anforderungen der darunter liegenden Ebenen erfüllt werden.

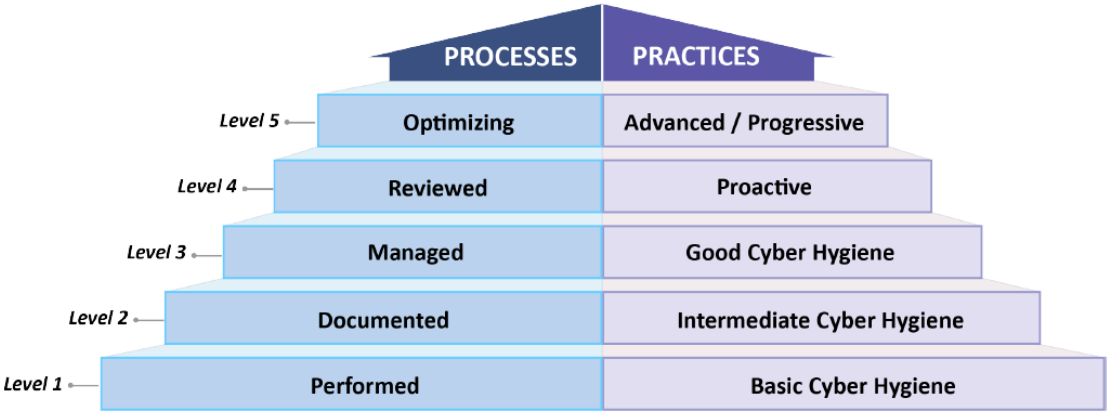

Abb. 4.4 CMMC-Ebenen. /DOD20r01/

Die einzelnen Ebenen richten den Fokus auf unterschiedliche Sicherheitsaspekte:

- **Ebene 1:** Schutz von Informationen über Bundesverträge
- **Ebene 2:** Übergangsschritt bei der Weiterentwicklung der IT-Sicherheit zum Schutz kontrollierter, nicht klassifizierter Informationen
- **Ebene 3:** Schutz kontrollierter, nicht klassifizierter Informationen
- **Ebenen 4 und 5:** Schutz kontrollierter, nicht klassifizierter Informationen und Reduzierung der Gefährdung durch Advanced Persistent Threats (APTs)

Das CMMC-Modell besteht aus insgesamt 17 Kategorien, die jeweils in Bezug auf die übergeordneten Themengebiete einzelne Sicherungsmaßnahmen beinhalten, die wiederum den oben genannten Ebenen zugeordnet werden. Dadurch ergeben sich für Auftragnehmer unterschiedliche Sicherungsmaßnahmen je nach angestrebter Ebene hinsichtlich des Vertrauensverhältnisses zwischen Auftraggeber und Auftragnehmer. Mit Hilfe zusätzlich veröffentlichter Assessment Guides werden zudem Hinweise zu den Zielen und Methoden der Bewertung für jede einzelne Sicherungsmaßnahme gegeben. Die Kategorien überlappen generell teilweise mit den in NIST SP 800-161 (s. o.) genannten Kategorien an Sicherungsmaßnahmen. Dabei gilt es zu beachten, dass sich das CMMC-Framework bezüglich der Implementierung und Umsetzung dieser Sicherungsmaßnahmen im Wesentlichen an die Auftragnehmer richtet, die ggf. entsprechende Nachweise für die Umsetzung vorlegen müssen, wohingegen sich die Sicherungsmaßnahmen in NIST SP 800-161 an die Behörden und Unternehmen selbst richten und somit deren

eigenen Geschäftsbereich betreffen. Im direkten Vergleich der beiden Dokumente ergibt sich somit bei NIST SP 800-161 eine Fokussierung auf Sicherungsmaßnahmen zur Sicherstellung der IT-Sicherheit der Lieferkette, die das Unternehmen/die Behörde im eigenen Haus umsetzen kann, wohingegen es sich beim CMMC-Framework überwiegend um allgemeine Sicherungsmaßnahmen ohne Fokussierung auf den Lieferkettenaspekt handelt, da durch die Etablierung gängiger allgemeiner Sicherungsmaßnahmen bei Auftragnehmern ein entsprechendes Sicherheitsniveau etabliert werden soll. Die Umsetzung der Maßnahmen muss ggf. nachgewiesen werden, diese liegt aber nicht direkt im Einflussbereich der Auftraggeber. Im Folgenden werden die für die verschiedenen Ebenen geforderten Sicherungsmaßnahmen kurz zusammenfassend hinsichtlich für das Vorhaben relevanter Aspekte vorgestellt.

CMMC-Ebene 1

Für diese Ebene müssen die Unternehmen die spezifizierten Methoden anwenden und umsetzen. Es handelt sich hierbei um insgesamt 17 grundlegende Sicherungsmaßnahmen zum Schutz von Informationen über Bundesverträge. Da die Unternehmen die Methoden möglicherweise nur ad hoc durchführen können und auf möglicherweise vorliegende Dokumente und Dokumentationen angewiesen sind, wird die Prozessreife für Ebene 1 nicht weiter bewertet. Die Sicherungsmaßnahmen dieser Ebene betreffen die Kategorien Access Control, Identification and Authentication, Media Protection, Physical Protection, System and Communications Protection und System and Information Integrity. Dabei geht es zunächst um die Einführung von Anforderungen an den Systemzugriff, die Kontrolle interner Systemzugriffe und von Fernzugriffen, sowie die Vergabe des Datenzugriffs an autorisierte Nutzer und Prozesse, wobei entsprechende Beschränkungen des Zugriffs eingeführt, überprüft und kontrolliert werden. Zudem gelten Sicherungsmaßnahmen zur Identifizierung und Authentifizierung von Benutzern oder Prozessen/Geräten, die neben den Maßnahmen zum physischen Schutz wie beispielsweise der Beschränkung des physischen Zugangs zu Bereichen oder IT-Systemen oder das Überwachen physischer Zutritte und Zugriffe den Zugang und Zugriff einschränken sollen. Anforderungen an den Schutz von (Wechsel)Datenträgern gelten im Wesentlichen hinsichtlich der fachgerechten Entsorgung, sodass gespeicherte Informationen nicht von unbefugten erlangt werden können. Zudem sind Sicherheitsanforderungen zur Einrichtung und Kontrolle der Kommunikation von Systemen, insbesondere bzgl. internen und externen Netzwerkgrenzen, definiert. Hinsichtlich der Integrität von Systemen und Informationen gelten Sicherheitsanforderungen zur Identifizierung und zum Umgang mit Mängeln von IT-Systemen, zur Identifizierung von schadhaftem Inhalt, zur Netzwerk- und Systemüberwachung und sowie zum erweiterten Schutz von E-Mails, wie beispielsweise die

Aktualisierung von Schutzmechanismen sowie regelmäßige Scans und Echtzeitscans von Dateien, insbesondere wenn diese aus externen Quellen stammen.

CMMC-Ebene 2

Die zweite Ebene erfordert die Einführung und Dokumentation von Methoden und Richtlinien, sodass eine reproduzierbare Wiederholung möglich ist und die Unternehmen entsprechend fortgeschrittene Fähigkeiten im Bereich der Cybersicherheit entwickeln. Technisch dient die zweite Ebene als Übergang von Ebene 1 zu Ebene 3 und bezieht sich auf den Schutz, geschützter, nicht eingestufter Informationen. Zusätzlich zu den in Ebene 1 bereits adressierten Kategorien Access Control, Identification and Authentication, Media Protection, Physical Protection, System and Communications Protection und System and Information Integrity, für die in Ebene 2 weitergehende Sicherungsmaßnahmen für jede dieser Kategorien eingeführt werden, umfasst die zweite Ebene zudem die Kategorien Audit and Accountability, Awareness and Training, Configuration Management, Incident Response, Maintenance, Personnel Security, Recovery, Risk Management und Security Assessment. Dabei umfasst Ebene zwei neben den 17 Sicherungsmaßnahmen von Ebene 1 zusätzlich 55 Maßnahmen, sodass insgesamt 72 Sicherungsmaßnahmen umgesetzt werden müssen. Im Bereich Audit and Accountability geht es dabei zunächst um die zweifelsfreie Rückführbarkeit von Aktionen zu den jeweiligen Benutzern sowie die entsprechende Aufbewahrung und Prüfung relevanter Aktivitätsdaten. Das Thema Awareness and Training umfasst die Sensibilisierung der Mitarbeiter zum Thema Cybersicherheit, wobei die Anwender entsprechend auf die mit ihren Aktivitäten verbundenen Sicherheitsrisiken und geltenden Richtlinien und Vorschriften aufmerksam gemacht werden, um die Berücksichtigung der Anforderungen der Cybersicherheit angesichts der zu erfüllenden Aufgaben sicherzustellen. In der Kategorie Configuration Management werden Grundlagen zur Durchführung eines Konfigurations- und Änderungsmanagements definiert, beispielsweise durch das Erstellen und Pflegen einer Basiskonfiguration, die Kontrolle und Überwachung der installierten Software sowie der Analyse der Auswirkung von Änderungen in Hinsicht auf die Cybersicherheit vor der Implementierung. Die Kategorie Incident Response umfasst im Wesentlichen Planung und Reaktion auf Vorfälle sowie die Erkennung und Meldung von Ereignissen anhand entsprechender Sicherungsmaßnahmen. Die Durchführung und Koordination von Wartungsarbeiten wird in der Kategorie Maintenance unter anderem durch Sicherungsmaßnahmen zur Kontrolle der Werkzeuge, Techniken und Mechanismen, insbesondere hinsichtlich Fernwartungsmöglichkeiten, adressiert. Die Kategorie Personnel Security behandelt im Wesentlichen Sicherungsmaßnahmen zur Überprüfung von Personen, bevor diese für den Zugriff auf IT-Systeme autorisiert werden, die kontrollierte, nicht klassifizierte

Informationen enthalten, sowie zur Sicherstellung, dass derartige IT-Systeme nach Personalmaßnahmen wie Kündigungen und Versetzungen entsprechend geschützt sind. Die Kategorie Recovery gibt Sicherungsmaßnahmen zur Erhaltung der Kontinuität der IT-Systeme und zur Verwaltung von Backups vor. Die Kategorien Risk Management und Security Assessment umfassen im Wesentlichen organisatorische Aspekte zur Identifizierung, Bewertung und zum Management von Risiken sowie zur Entwicklung und zum Management eines Sicherheitsplans für IT-Systeme. Dabei geht es in den Sicherungsmaßnahmen vornehmlich um die regelmäßige Bewertung der Risiken für das Unternehmen, die regelmäßige Suche nach Schwachstellen der eingesetzten IT-Systeme sowie um die Entwicklung, Dokumentation, Aktualisierung, Implementierung und Überprüfung von Sicherheitsplänen, Maßnahmen und Handlungsplänen zur Behebung von Mängeln und Schwachstellen.

CMMC-Ebene 3

Die CMMC-Ebene 3 erfordert, dass Unternehmen und Organisationen eine Sicherheitsplanung erstellen, pflegen und mit entsprechenden Ressourcen ausstatten, um die Befähigung für die praktische Umsetzung von Sicherungsmaßnahmen zu demonstrieren. Diese Ebene konzentriert sich auf den Schutz von kontrollierten, nicht klassifizierten Informationen und umfasst alle in NIST SP 800-171 spezifizierten Sicherheitsanforderungen, sowie zusätzliche Methoden aus anderen Standards und Referenzen zur Vermeidung von Bedrohungen der IT-Sicherheit. Zusätzlich zu den in Ebene 1 und 2 bereits adressierten Kategorien, für die in Ebene 3 weitergehende Sicherungsmaßnahmen eingeführt werden, umfasst die dritte Ebene zusätzlich die Kategorien Asset Management und Situational Awareness. Dabei umfasst Ebene 3 neben den 17 Sicherungsmaßnahmen von Ebene 1 und den 55 Maßnahmen von Ebene 2 58 zusätzliche Maßnahmen, sodass insgesamt 130 Sicherungsmaßnahmen umgesetzt werden müssen. Im Bereich Asset Management geht es primär um die Identifizierung und Dokumentation von Beständen und Vermögenswerten sowie deren Verwaltung. Die Maßnahmen umfassen dabei eine Definition der Prozeduren für die Handhabung von kontrollierten, nicht klassifizierten Informationen. Die Kategorie Situational Awareness greift die Beobachtung und Untersuchung der aktuellen IT-Bedrohungslage auf, realisiert unter anderem durch Maßnahmen wie die Sammlung von und Reaktion auf Informationen zu IT-Bedrohungen aus Informationsaustauschforen und -quellen und Kommunikation dieser Informationen mit allen Beteiligten.

CMMC-Ebene 4

Die Ebene 4 erfordert von den Anwendern eine Prüfung und Bewertung der Effektivität der angewendeten Methoden, sowie ggf. darüber hinaus die aktive Ausführung von Korrekturmaßnahmen und regelmäßige Information des Managements über den Status und mögliche Probleme. Ebene 4 konzentriert sich auf den Schutz von kontrollierten, nicht klassifizierten Informationen vor APTs und umfasst einen Teil der erweiterten Sicherheitsanforderungen aus dem Entwurf NIST SP 800-171B sowie andere Best Practices für die IT-Sicherheit. Diese Methoden verbessern die Erkennungs- und Reaktionsfähigkeit eines Unternehmens bezüglich IT-Angriffen, um sich an die sich ändernden Taktiken, Techniken und Verfahren von APTs anzupassen. Zusätzlich zu den 130 Sicherungsmaßnahmen der Ebenen 1 bis 3 gibt es in Ebene 4 26 zusätzliche Sicherungsmaßnahmen aus den Kategorien Access Control, Asset Management, Audit and Accountability, Awareness and Training, Configuration Management, Incident Response, Risk Management, Security Assessment, Situational Awareness, System and Communications Protections und System and Information Integrity.

CMMC-Ebene 5

Die höchste Ebene fordert von den Anwendern, die Prozessimplementierung im gesamten Unternehmen zu standardisieren und zu optimieren. Ebene 5 konzentriert sich dabei auf den Schutz von kontrollierten, nicht klassifizierten Informationen vor APTs. Die zusätzlichen Anforderungen sollen die Ausgereiftheit und den Umfang der Sicherungsmaßnahmen erhöhen. Zusätzlich zu den 156 Sicherhungsmaßnahmen der Ebenen 1 bis 4 umfasst Ebene 5 insgesamt 15 zusätzliche Maßnahmen aus den Kategorien Access Control, Audit and Accountability, Configuration Management, Incident Response, Recovery, Risk Management, System and Communication Protection und System and Information Integrity. Im Rahmen des CMMC-Modells ergeben sich für die Erreichung des höchsten Sicherheitsstandards somit insgesamt 171 zu erfüllende Sicherungsmaßnahmen.

4.1.3 Großbritannien

In Großbritannien ist das Office for Nuclear Regulation (ONR) die unabhängige britische Aufsichtsbehörde für den Nuklearbereich mit der rechtlichen Befugnis, die nukleare Sicherheit, die zivile nukleare Sicherung und die konventionelle Gesundheit und Sicherheit an den genehmigten Nuklearstandorten zu regeln. Dies umfasst bestehende Reaktoren,

Anlagen des Brennstoffkreislaufs, die Abfallentsorgung und Stilllegungsanlagen sowie den Transport von zivilem Kernmaterial und radioaktiven Stoffen auf der Straße, Schiene und Binnenwasserstraßen. Die Regulierung umfasst in Bezug auf die nukleare Sicherheit die Genehmigung von Sicherheitsvorkehrungen in der zivilen Nuklearindustrie und bietet eine Regulierungsaufsicht für die Sicherheit des Transports von zivilem Nuklearmaterial und die Verwaltung von effektiven Vorkehrungen für sensible nukleare Informationen.

Das ONR veröffentlichte in den letzten Jahren in Bezug auf die nukleare Sicherheit und Sicherung unter anderem verschiedene Leitlinien (Guides) wie beispielsweise CNS-INSP-GD-7.0 (CYBER SECURITY AND INFORMATION ASSURANCE) /ONR22r01/, CNS-TAST-GD-7.1 (EFFECTIVE CYBER AND INFORMATION RISK MANAGEMENT) /ONR20r01/ und CNS-INSP-GD-4.0 (NUCLEAR SUPPLY CHAIN MANAGEMENT) /ONR22r02/. Im Rahmen des Vorhabens wurde das Dokument NS-TAST-GD-077 (Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services, Revision 6) /ONR19r01/ ausgewertet. Im Folgenden wird diese Veröffentlichung kurz vorgestellt und hinsichtlich für das Vorhaben relevanter Aspekte analysiert.

Bei dem Dokument NS-TAST-GD-077 /ONR19r01/ handelt es sich um ein Technical Assessment Guide (TAG) des ONR, mit dem Sicherheitsnachweisen für kerntechnische Anlagen bewertet werden sollen. Allgemein werden spezifischen Fragen im Zusammenhang mit der Beschaffung von Komponenten und Systemen im Zusammenhang mit zivilen Reaktoren adressiert, insbesondere im Rahmen von Genehmigungsverfahren. Demnach steht der Genehmigungsinhaber an der Spitze der Lieferkette. Seine Aufgabe ist es Prozesse übersichtlich zu gestalten, sowie Artikel, Maßnahmen und Dienstleistungen von Lieferanten zu bestätigen und zu akzeptieren oder abzulehnen, um die Sicherheit der nuklearen Anlagen zu gewährleisten. Dabei können durch internationale Verflechtungen Sicherheitsrisiken hervorgerufen werden. Der Lizenzinhaber hat einen entsprechenden Beschaffungszyklus zu etablieren. Dieser umfasst zunächst die Erarbeitung einer Beschaffungsstrategie, der Definition der Anforderungen, der Analyse potenzieller Bezugsquellen, der Auslieferung und der Evaluierung des Prozesses für zukünftige Beschaffungszyklen. Die einzelnen Punkte werden jeweils detailliert ausgeführt und hinsichtlich für eine Prüfung relevanter Aspekte adressiert.

Strategie

Dabei geht es zunächst um die Etablierung einer effektiven Geschäfts-/Lieferketten-Strategie, um entsprechende Sicherheitsanforderungen durchzusetzen. Diese Strategie beeinflusst alle Vereinbarungen im Zusammenhang mit der Beschaffung von Komponenten oder Dienstleistungen. Dabei müssen die aktuellen und zukünftigen Sicherheitsanforderungen während der gesamten Lebensdauer und der Stilllegungsphase der Anlage nachweislich erfüllt werden. Die Vereinbarungen sollten regelmäßig überprüft werden, da sich die Anforderungen im Lauf der Zeit verändern können. Zudem geht es um die Koordinierung aller Arbeiten, die im Auftrag des Käufers durchgeführt werden. Die Hauptverantwortung für die Sicherheit einer kerntechnischen Anlage liegt beim Genehmigungsinhaber. Dieser muss in der Lage sein, ausreichende Kenntnisse des Anlagendesigns und der Sicherheitsanforderungen für alle Anlagen und Tätigkeiten am genehmigten Standort nachzuweisen. Der Genehmigungsinhaber muss die Aktivitäten an seinem Standort koordinieren, die mit ihnen verbundenen Gefahren verstehen und wissen, wie diese kontrolliert werden können. Um ein effektives Lieferketten-Management zu erreichen, sollte der Genehmigungsinhaber die Notwendigkeit der Dienstleistungen eines Auftragnehmers auf jeder Ebene der Lieferkette vollständig verstehen und in der Lage sein, entsprechende Anforderungen zu spezifizieren und Arbeiten zu beaufsichtigen. Der Genehmigungsinhaber muss die Arbeiten während und nach der Implementierung technisch überprüfen.

Spezifizierung und Definition von Anforderungen

Der Käufer muss sicherstellen, dass die Spezifikationen die benötigten Komponenten oder Dienstleistungen angemessen beschreiben, die Sicherheitsanforderungen erfüllen und das erforderliche Maß an Qualitätssicherung angeben. Die Verfasser der Spezifikationen müssen geschult und kompetent sein, um eine Verifizierung und Validierung durchführen zu können, die der Sicherheitsbedeutung der spezifizierten Komponente oder der spezifizierten Dienstleistung gerecht werden. In der Vorvertragsphase muss der Käufer sicherstellen, dass potenzielle Lieferanten in der Lage sind zu garantieren, dass die zu beschaffenden Komponenten oder Dienstleistungen die nukleare Sicherheit gewährleisten. Der Genehmigungsinhaber oder der Käufer muss Spezifikationen festlegen, die die Expertise der Lieferanten berücksichtigen, insbesondere bezüglich der Umsetzbarkeit von Anforderungen. Der Käufer sollte alle behördlichen Anforderungen, erforderlichen Designrichtlinien und -standards aufführen und technische Spezifikationen erstellen, die die zu beschaffenden Komponenten oder Dienstleistungen zusammen mit

anderen allgemeinen Vertragsanforderungen vollständig beschreiben. Für Komponenten oder Dienstleistungen, die für die Gewährleistung der nuklearen Sicherheit wichtig sind, können zusätzliche Gewährleistungs- und Inspektionsvorkehrungen erforderlich sein, die über die grundlegende Einhaltung etablierter Vorschriften und -normen hinausgehen. Der Käufer muss sicherstellen, dass spezifische Sicherheitsanforderungen (wie Diversität, Redundanz usw.) in den Spezifikationen widergespiegelt und während der gesamten Beschaffung und Herstellung eingehalten werden. Auswirkungen auf die Sicherheitsanforderungen infolge von Änderungen in der Lieferkette (z. B. Fusionen, Übernahmen) müssen mit dem Lizenzinhaber besprochen werden. Wenn technische Spezifikationen für Komponenten oder Dienstleistungen mit nuklearsicherheitstechnischer Relevanz von Auftragnehmern im Auftrag des Käufers erstellt werden, sollten diese von Mitarbeitern des Käufers mit entsprechenden Kompetenzen überprüft werden, um zu bestätigen, dass die Spezifikationen die Entwurfsabsicht richtig widerspiegeln sowie alle Vorschriften und -normen und die Sicherheitsanforderungen erfüllen. Diese Prüfung muss vor Auftragsvergabe durchgeführt werden. Nach Erhalt der Bestellung muss der Lieferant eine Überprüfung der Vertragsdokumentation durchführen, um sicherzustellen, dass er alle technischen, verfahrenstechnischen und geschäftlichen Anforderungen des Vertrags erfüllen kann. Der Lieferant muss den Käufer über alle Änderungen seiner Möglichkeiten bezüglich der Vertragserfüllung (auch die Zwischenlieferanten betreffend) informieren. Der Käufer muss einen Änderungskontrollprozess etablieren der sicherstellen soll, dass alle Änderungen an Spezifikationen, Design oder Verträgen vor der Umsetzung der Änderung ordnungsgemäß kontrolliert und genehmigt werden. Die Auswirkungen auf die nukleare Sicherheit und die Herstellungs- oder Lieferprozesse, einschließlich aller Änderungen an der Dokumentation (z. B. Qualitätsplanung), müssen vollständig berücksichtigt werden.

Auswahl von Bezugsquellen und Lieferanten

Bevor Verträge abgeschlossen werden ist sicherzustellen, dass Lieferanten über die organisatorischen und technischen Möglichkeiten, Kapazitäten und Sicherheitskultur verfügen, um die zuvor festgelegten Spezifikationen zu erfüllen. Lieferanten sollten vom Käufer anhand vordefinierter Kriterien ausgewählt werden. Die Kriterien prüfen die organisatorischen und technischen Möglichkeiten des Lieferanten, welche in dessen Managementsystem enthalten sein müssen, die Anforderungen zu erfüllen und sollten vom Lieferanten bereitgestellte Informationen berücksichtigen, die einen objektiven Nachweis seiner Fähigkeiten und Kapazitäten darstellen. Eine Bewertung eines potenziellen Lieferanten muss die nukleare Sicherheitskultur des Lieferanten umfassen, um

sicherzustellen, dass die Sicherheitsanforderungen des Käufers erfüllt werden. Als Teil des Auswahlprozesse muss der Käufer sicherstellen, dass die Lieferanten über angemessene Aufsichts- und Sicherungsvorkehrungen für ihre eigenen Lieferanten verfügen. Der Käufer und die Lieferanten sollten über eine Zertifizierung nach anerkannten Managementsystemanforderungen verfügen, um sicherzustellen, dass ein geeignetes Qualitätsmanagement vorhanden ist und in der gesamten Lieferkette angewendet wird. Zusätzlich muss der Käufer jede Ebene der Lieferkette eigenständig bewerten oder eine Aufsicht und Kontrolle der Arbeiten durchführen. Alle Verträge müssen dieses Zugriffsrecht des Käufers detailliert beschreiben. Käufer müssen sich vergewissern, dass ihre Lieferanten über kompetentes Personal verfügen, insbesondere solche, die Schlüsselfunktionen wie Vertragsprüfung, Fertigung und Inspektionen ausführen. Die Beurteilung der Kompetenz sollte auf Qualifikationen, Ausbildung und Erfahrung beruhen.

Allgemein müssen Zulieferer über ein Qualitätsmanagement verfügen, das den Sicherheitsanforderungen angemessen und mit diesen konsistent ist. Käufer müssen sicherstellen, dass Lieferunternehmen über Qualitäts-, Umwelt- und Sicherheitsmanagementsysteme verfügen, die für die zu liefernden Komponenten oder Dienstleistungen geeignet sind und die relevanten nationalen oder internationalen Anforderungen erfüllen, insbesondere bezüglich der nuklearen Sicherheit. Die Verwendung von Qualitätssicherungsplänen, die vom Lieferanten entwickelt und mit dem Käufer vereinbart wurden, ist unerlässlich, um sicherzustellen, dass Artikel auf geplante und kontrollierte Weise hergestellt, montiert, getestet und inspiziert werden und dass die erforderlichen Integritätsgrade erreicht und nachgewiesen werden können. Qualitätssicherungspläne sollten die gesamten Schritte zur Lieferung der Komponente oder der Dienstleistung aufzeigen und Einzelheiten zur Freigabe von Haltepunkten enthalten. Diese müssen den beteiligten Parteien vor Beginn der Arbeiten rechtzeitig zur Überprüfung zur Verfügung stehen. Qualitätssicherungspläne sollten Prozess- oder Herstellungsanweisungen, Tests und Inspektionen sowie deren Dokumentation, die dem Käufer zur Verfügung gestellt wird, eindeutig festlegen. Die Bedeutung der Aufbewahrung von Konstruktions-, Beschaffungs-, Herstellungs-, Fertigungs- und Inspektionsaufzeichnungen kann nicht genug betont werden, da diese den Sicherheitsnachweis unterstützen. Sie belegen die Prüfungshandlungen des Lieferanten, der Unterlieferanten und des Käufers. Aufzeichnungen sind Teil des Nachweises, dass Anlagen und Systeme die Konstruktionsabsichten und die Sicherheitsanforderungen erfüllen. Die Identifizierung, Generierung, rechtzeitige Fertigstellung, Übergabe und Aufbewahrung von Aufzeichnungen im Zusammenhang mit der Lieferung von Komponenten oder Dienstleistungen sollte Teil der vertraglichen Vereinbarungen zwischen Käufer und Lieferant auf allen Ebenen der Lieferkette sein.

Auslieferung

Lieferanten identifizieren und kategorisieren Abweichungen von den spezifizierten Anforderungen und teilen diese dem Käufer mit, der eine entsprechende Bewertung durchführt. Abweichungen von den Anforderungen des Käufers können durch eine Reihe von Maßnahmen, einschließlich Inspektionen, Audits oder Überwachungen, identifiziert werden. Sie müssen dem Käufer gemeldet und behoben werden. Alle Organisationen innerhalb der Lieferkette sollten als Teil ihrer Qualitätsmanagementvereinbarungen einheitliche, vom Käufer beaufsichtigte Vorkehrungen zur Kategorisierung und Behebung von Abweichungen treffen. Käufer auf jeder Ebene der Lieferkette sollten sicherstellen, dass ihre Lieferanten über angemessene Vorkehrungen für die Identifizierung, Kategorisierung und Behebung von Abweichungen bei Artikeln oder Dienstleistungen verfügen, insbesondere wenn die Abweichungen die nukleare Sicherheit betreffen. Es muss eine umfassende Dokumentation zu allen genehmigten Abweichungen sowie systematische, übergreifende Protokolle zur Verfolgung von Abweichungen existieren. Der Käufer muss wirksame Vorkehrungen für die Kontrolle der Tätigkeiten des Lieferanten während der gesamten Vertragslaufzeit treffen und sicherstellen, dass Artikel oder Dienstleistungen dem festgelegten Zweck entsprechen. Der Käufer muss sicherstellen, dass er über ausreichende Kapazitäten verfügt, um die Arbeiten auf allen Ebenen der Lieferkette zu überwachen und zu kontrollieren. Diese Aktivitäten müssen die Inspektion, Prüfung, Freigabe, Annahme und Lagerung von Komponenten und Dienstleistungen mit hohem Risiko, insbesondere bezüglich der nuklearen Sicherheit, umfassen. Das vom Käufer eingesetzte Maß an Aufsicht und Sicherheit muss sich an den Aufgaben des Lieferanten oder der Lieferkette und den Sicherheitsanforderungen orientieren. Wenn die erbrachten Leistungen hinter den Erwartungen zurückbleiben, muss der Käufer die Kontrollen erhöhen, bis die Leistungen des Lieferanten den Erwartungen entsprechen oder er muss den Vertrag mit dem Lieferanten beenden. Die Annahme von Artikeln oder Dienstleistungen kann eine Überprüfung oder Bewertung durch Zweit- oder unabhängige Drittorganisationen beinhalten. Dieser Ansatz bietet ein zusätzliches Maß an Sicherheit.

Der Käufer oder Lieferant sollte je nach Umfang, Komplexität, Internationalität seiner Lieferkette oder der nuklearen Sicherheitsanwendung für seine Artikel oder Dienstleistungen geeignete Maßnahmen ergreifen, um zu verhindern, dass CFSI (Counterfeit, Fraudulent & Suspect Items) Auswirkungen auf seine Lieferkette haben. Mögliche Maßnahmen umfassen unter anderem:

- Robuste Beschaffungsprozessvereinbarungen, einschließlich effektiver Überwachung und Sicherung der Lieferkette.

- Prüfungen und Inspektionen.
- Rückverfolgbarkeit von Material oder Komponenten bis zum Ursprungslieferanten, einschließlich Verifizierungstests durch spezialisierte Drittorganisationen für Artikel mit hohem Risiko.
- Schulungen und Sensibilisierung der Mitarbeiter innerhalb der Lieferkette bezüglich CFSI.
- Prozesse und Verfahren zur Identifizierung, Untersuchung und Aufzeichnung von CFSI-Vorfällen und zum Austausch von gewonnenen Erkenntnissen.
- Die Vernichtung nicht konformer Artikel, um zu verhindern, dass sie wieder in die Lieferkette gelangen.

Evaluierung des Prozesses

Die Evaluierung des Prozesses beinhaltet im Wesentlichen die Erfassung und Reaktion auf das Feedback bezüglich betrieblicher Erfahrungen aus der Lieferkette und deren Management. Die vorherigen Schritte sind entsprechend anzupassen. Zudem sollten die gewonnenen Informationen innerhalb des eigenen Unternehmens, mit den Vertragspartnern der Lieferkette und weiteren Industriezweigen entsprechend geteilt werden. •Die Betriebserfahrungen des Käufers sollten gegebenenfalls einen breiteren Austausch relevanter Lieferanten- und Lieferketten-Erfahrungen mit anderen Genehmigungsinhabern und der breiteren Industrie ermöglichen. Es sollten Vorkehrungen getroffen werden, um Betriebserfahrungen, die von anderen Genehmigungsinhabern und weiteren verwandten Branchen geteilt werden, auf Auswirkungen innerhalb der eigenen Lieferkette hin zu bewerten.

4.1.4 Finnland

Die Radiation and Nuclear Safety Authority (STUK) ist die finnische Aufsichtsbehörde in Bezug auf die nukleare Sicherheit sowie den Strahlenschutz. In diesem Zusammenhang obliegt ihr die Definition detaillierter Sicherheitsanforderungen für die Umsetzung eines angemessenen Sicherheitsniveaus gemäß dem Gesetz zur Nuklearenergie. In Bezug auf die Informationssicherheit wurde der Leitfaden YVL A.12 „*Information Security Management of a Nuclear Facility*“ /STU21r01/ veröffentlicht, der für nukleare Anlagen in allen Phasen ihres Lebenszyklus sowie für Organisationen, die möglicherweise Einfluss auf die Informationssicherheit von nuklearen Anlagen haben, gedacht. Der Leitfaden

besteht im Wesentlichen aus konkreten Anforderungen zur Sicherstellung der Informationssicherheit. Im Folgenden werden für das Vorhaben relevante Aspekte des Leitfadens kurz zusammengefasst.

Zunächst wird das Thema Informationssicherheitsmanagement allgemein in /STU21r01/ adressiert. Hinsichtlich des Themas IT-Sicherheit in der Lieferkette sind folgende Anforderungen relevant: Das geforderte Informationssicherheits-Managementsystem, das Richtlinien, Verfahren, Leitlinien und damit verbundene Ressourcen und Aktivitäten umfasst, soll Leitfäden für und die Überwachung von externen Organisationen in Bezug auf die Informationssicherheit umfassen. Das Informationssicherheits-Managementsystem soll dabei die Informationssicherheitsorganisation beschreiben. Diese Beschreibung muss auch externe Parteien und deren Verantwortlichkeiten berücksichtigen. Soweit erforderlich, sind allgemein die Aufgaben und Verantwortungsbereiche zu trennen, um das Risiko einer unbefugten oder versehentlichen Änderung oder eines Missbrauchs der geschützten Vermögenswerte der Organisation zu verringern. Zudem gibt es eine Anforderung im Zusammenhang mit dem Geheimschutz, nach der eine zentrale Regierungsbehörde im Voraus sicherstellen muss, dass der Schutz eines Verschlusssachen-Dokuments ordnungsgemäß organisiert ist, wenn die Behörde einer anderen Partei als der zentralen Regierungsbehörde Zugang zu einem Verschlusssache-Dokument gewährt. Vor der Weitergabe von Unterlagen, die Informationen enthalten, die von einer Behörde als vertraulich eingestuft oder die von so eingestuften Informationen abgeleitet wurden, an Dritte muss der Lizenznehmer die Genehmigung der Behörde für Strahlenschutz und nukleare Sicherheit für die Weitergabe der Informationen einholen.

Weitere Anforderungen zur Informationssicherheit im Zusammenhang mit der Lieferkette finden sich im Abschnitt zum Thema Ressourcenmanagement. Demnach ist nicht nur das gesamte Personal der kerntechnischen Anlage, sondern auch externer Organisationen in Fragen der Informationssicherheit in dem für die Erfüllung ihrer Aufgaben erforderlichen Umfang zu sensibilisieren. Entsprechende Schulungen sollen dokumentiert werden. Bei der Nutzung externer Ressourcen soll der Genehmigungsinhaber sicherstellen, dass das Niveau der Informationssicherheit und die Zuordnung von Verantwortlichkeiten mindestens den Standards des Genehmigungsinhaber für ähnliche Tätigkeiten entsprechen. Der Genehmigungsinhaber soll zudem über Prozeduren zur Überwachung der Informationssicherheit relevanter externer Ressourcen verfügen. Bei der Überwachung sind untergeordnete Teilabschnitte der Lieferkette mit einzubeziehen. Für Leitfäden zur Überwachung von Lieferanten allgemein wird zudem auf weiterführende Dokumente (YVL A.3 „*Leadership and management for safety*“ und YVL A.5

„*Construction and commissioning of a nuclear facility*“) verwiesen. Zum Thema Genehmigungsverfahren gibt es zudem die Anforderung, dass Informationen zum beabsichtigten Vorgehen hinsichtlich der Überwachung der Informationssicherheit bei Lieferanten vorgelegt werden sollen.

4.2 Internationales Regelwerk

Neben nationalen Regelwerken wurden im Rahmen des Vorhabens internationale Veröffentlichungen der IAEA sowie verschiedene Normen aus dem Bereich der Cybersicherheit betrachtet.

4.2.1 IAEA

Die IAEA veröffentlichte und überarbeitete in den letzten Jahren verschiedene technische Leitfäden, die sich mit dem Thema Cybersicherheit im Nuklearbereich befassen. Dabei wurden je nach Veröffentlichung unterschiedliche Schwerpunkte gesetzt, beispielsweise mit Fokus auf der allgemeinen nuklearen Sicherheit oder Sicherung im Zusammenhang mit Cybersicherheit oder speziell im Zusammenhang mit Mess-, Steuerungs- und Regelungstechnik. Im Rahmen des Vorhabens wurden die Veröffentlichungen Computer Security at Nuclear Facilities (NSS 17) /IAE11n02/, Computer Security of Instrumentation and Control Systems at Nuclear Facilities (NSS 33-T) /IAE18n02/, Computer Security for Nuclear Security (NSS 42-G) /IAE21n01/ und Computer Security Techniques for Nuclear Facilities (NSS 17-T /IAE21n03/, ersetzt mittlerweile NSS 17) hinsichtlich für das Vorhaben relevanter Aspekte ausgewertet. Kürzlich wurde das Thema Cybersicherheit in der Lieferkette durch die IAEA in der Veröffentlichung „*Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain“* (IAEA-TDL-011) /IAE22n01/ explizit adressiert. Die betrachteten Veröffentlichungen der IAEA werden im Folgenden kurz vorgestellt, bevor die für das Vorhaben relevanten Inhalte aller Dokumente zusammengefasst werden.

Die Veröffentlichung Computer Security at Nuclear Facilities (NSS 17) enthält Leitfäden für kerntechnische Anlagen zur Umsetzung und Etablierung eines Programms zur Informationssicherheit und zur Evaluierung bestehender Programme. Zur Zeit der Veröffentlichung im Jahr 2011 hatte das Thema Cybersicherheit in kerntechnischen Anlagen noch nicht die heutige Dringlichkeit und Präsenz, auch weil der Einsatz digitaler Komponenten in derartigen Anlagen in den vergangenen Jahren stark zugenommen hat. In diesem

Zusammenhang stellt das Dokument als eine frühe Veröffentlichung in diesem Bereich der Informationssicherheit in kerntechnischen Anlagen als Schlüsselkomponente der Anlagensicherung dar. Der technische Leitfaden NSS 33-T (Computer Security of Instrumentation and Control Systems at Nuclear Facilities) bietet Leitlinien für die Anwendung von Sicherungsmaßnahmen auf Leittechniksysteme in kerntechnischen Anlagen, wodurch diese Systeme während ihres gesamten Lebenszyklus vor böswilligen Handlungen durch Bedrohungsakteure geschützt werden sollen. Dabei steht die Anwendung der Sicherungsmaßnahmen auf die Entwicklungs-, Simulations-, Anwendungs- und Wartungsumgebung im Vordergrund. In der Nuclear Security Series Nuclear Security Series 42-G – Computer Security Techniques for Nuclear Facilities werden allgemeine Aspekte der Computersicherheit für alle Bereiche der nuklearen Sicherheit, wie beispielsweise die Sicherheit von Kernmaterial und kerntechnischen Anlagen sowie radioaktivem Material und zugehörigen Anlagen behandelt. Die Veröffentlichung enthält dabei detaillierte Leitlinien für die Entwicklung, Umsetzung und Integration der Computersicherheit als Schlüsselkomponente der nuklearen Sicherheit. Der Anwendungsbereich umfasst computergestützte Systeme, deren Kompromittierung die nukleare Sicherung oder die nukleare Sicherheit beeinträchtigen könnte. Die Nuclear Security Series 17-T – Computer Security Techniques for Nuclear Facilities bietet einen technischen Leitfaden für die Einführung oder Verbesserung, Entwicklung, Umsetzung, Aufrechterhaltung und Pflege der Informationssicherheit im Zusammenhang mit der nuklearen Sicherheit in kerntechnischen Anlagen. Die Veröffentlichung befasst sich mit der Verwendung risikobasierter Ansätze zur Festlegung und Verbesserung von Strategien zur Verbesserung der Informationssicherheit und beschreibt insbesondere die Integration der Informationssicherheit in das Managementsystem einer Anlage. Ausgehend von einem systematischen Ansatz zur Ermittlung von Anlagenfunktionen und geeigneter Sicherungsmaßnahmen sollen digitale Komponenten vor den Folgen von Cyberangriffen geschützt werden. Die Veröffentlichung ersetzt mittlerweile die Veröffentlichung NSS 17. Für das Vorhaben relevante Inhalte aller oben genannten Veröffentlichungen sind in den nächsten Abschnitten hinsichtlich verschiedener Themenkomplexe zusammengefasst.

Vertrag zwischen Anlagenbetreiber, Herstellern, Auftragnehmern und Lieferanten

Anlagenbetreiber, Hersteller, Auftragnehmer und Lieferanten müssen die staatlichen Anforderungen an die IT-Sicherheit im nuklearen Sektor erfüllen. Der Anlagenbetreiber muss mit den Herstellern, Auftragnehmern und Lieferanten von I&C-Systemen einen Vertrag abschließen, in dem die Fragen zur Realisierung der Sicherheit der I&C-Systeme und deren Komponenten, unter Berücksichtigung ihrer jeweiligen Sicherheitseinstufung,

geklärt werden. Die beteiligten Organisationen müssen im Sinne des IT-Sicherheitsplans der Anlage arbeiten und über robuste und verifizierbare IT-Sicherheitsprozesse verfügen. Dies betrifft auch Wartungsverträge. Sie benötigen einen IT-Sicherheits-Managementprozess und müssen alle vom Anlagenbetreiber spezifizierten Sicherungsmaßnahmen, sowohl bei Arbeiten in der Anlage und an externen Arbeitsstätten als auch bei Transfervorgängen und Lagerungen, umsetzen. Anbieter, Auftragnehmer und Lieferanten müssen über sichere technische Umgebungen verfügen und das Prinzip Security by Design bei der Herstellung, Beschaffung und Lieferung von Geräten und der Inanspruchnahme von Dienstleistungen befolgen. Änderungen der Sicherheitsregeln und Prozeduren müssen den Vertragspartnern rechtzeitig mitgeteilt werden. Verträge mit Anbietern, Auftragnehmern und Lieferanten müssen diese verpflichten, dem Betreiber die Durchführung von Prüfungen und Inspektionen zu gestatten. /IAE18n02, IAE21n01, IAE21n03/

Bei der Anschaffung neuer Geräte und Systeme müssen die Sicherheitsanforderungen mit den Lieferanten vertraglich festgelegt werden. Für weitere Einzelheiten wird aus die Norm ISO/IEC 15408 (Evaluationskriterien für IT-Sicherheit) sowie das Dokument „*Cyber Security Procurement Language for Control Systems*“ des US Department of Homeland Security verwiesen. /IAE11n02/

Weiterhin muss ein Prozess eingerichtet werden, der es dem Anlagenbetreiber und den Herstellern, Auftragnehmern und Lieferanten ermöglicht, sich gegenseitig über Schwachstellen zu unterrichten, sich über geeignete Gegenmaßnahmen und vorbeugende Maßnahmen zu einigen und diese umzusetzen. Dieser Prozess muss während der gesamten Vertragsdauer bestehen und gegebenenfalls darüber hinaus, um eine geeignete Unterstützung während der Lebensdauer des I&C-Systems sicherzustellen. /IAE18n02/

Wenn sensible Daten nicht unter direkter Kontrolle des Anlagenbetreibers stehen, dann müssen die Anforderungen an den Zugriff anderer Organisationen auf die betreffenden Systeme vertraglich festgelegt werden. Auf diese Weise ist sicherzustellen, dass keine unautorisierten Zugriffe oder Manipulationen erfolgen können. Diese Anforderungen betreffen die Zugriffskontrolle, Verfügbarkeit, Datentrennung, Datenvernichtung, Kommunikationsschnittstellen, Hardware, Software und administrative Prozesse. Darüber hinaus muss der Anlagenbetreiber eigene Sicherheitsvorkehrungen treffen. /IAE21n01/

Anlagenbetreiber, Hersteller, Auftragnehmer und Lieferanten sollten regelmäßig Audits und Bewertungen zur IT-Sicherheitslage durchführen und von den Ergebnissen berichten. In den Verträgen des Anlagenbetreibers mit Herstellern, Auftragnehmern und Lieferanten muss festgelegt werden, dass diese falls nötig sensible Informationen zu ihren Produkten mit dem Anlagenbetreiber teilen. /IAE11n02, IAE18n02/

IT-Sicherheits-Management

Jede Organisation inklusive des Anlagenbetreibers, die an Aktivitäten während der Lebensdauer eines I&C-Systems beteiligt ist, muss die IT-Sicherheit für I&C-Systeme innerhalb ihres integrierten Managementsystems berücksichtigen. Wenn Zweifel bestehen muss überprüft werden, dass die IT-Sicherheit durch das Management-System des Vertragspartners angemessen abgedeckt wird. Die Methoden und Maßnahmen des Vertragspartners müssen den Anforderungen des Management-Systems entsprechen. Maßnahmen zur Erfüllung der IT-Sicherheit von sicherheitsrelevanten I&C-Systemen, Subsystemen und Komponenten müssen überprüfbar sein. Ihre Einhaltung muss während der Lebensdauer der I&C-Systeme, Subsysteme und Komponenten regelmäßig kontrolliert werden. Darüber hinaus müssen zusätzliche Kontrollen erfolgen, die sicherstellen, dass die Maßnahmen wie im Qualitätssicherungsplan des Anlagenbetreibers beschrieben durchgeführt werden. Das technische Personal muss vom Anbieter eine Bestätigung einholen, dass die an die Einrichtung gelieferten Produkte in einer sicheren Umgebung entwickelt wurden. /IAE11n02, IAE18n02, IAE21n02/

Das technische Personal muss ein Verfahren zur Überprüfung der technischen Produktdokumentation, zur Annahme von Produktsendungen vor Ort und zum Testen von Produkten festlegen und befolgen, um sicherzustellen, dass die Anforderungen an die IT-Sicherheit erfüllt werden. Vorentwickelte Produkte können vorentwickelte Hardware und Software von Organisationen beinhalten, die entweder über kein angemessenes IT-Sicherheits-Management verfügen oder nicht bereit sind Informationen über ihr IT-Sicherheits-Management zu teilen. In diesen Fällen ist es erforderlich die IT-Sicherheitseigenschaften der Produkte zu analysieren und den Einsatz der Produkte entsprechend zu rechtfertigen. /IAE18n02, IAE21n02/ Das Beschaffungspersonal muss das technische Personal darüber informieren, wenn die Unterstützung eines Anbieters, Auftragnehmers oder Lieferanten für ein sensibles, digitales Gerät nicht mehr verfügbar ist oder in absehbarer Zeit nicht mehr verfügbar sein wird. /IAE21n02/

Alle Aktivitäten während der Lebensdauer eines I&C-Systems müssen aufgezeichnet und mit den IT-Sicherheitsanforderungen verglichen werden. Die Aufzeichnungen müssen alle aufgetretenen IT-Sicherheitsvorfälle und gegensteuernden Maßnahmen beinhalten. Autorisierte Individuen, die physischen oder softwarebezogenen Zugriff auf I&C-Systeme haben, müssen Sicherheitsüberprüfungen, IT-Sicherheitsunterweisungen und Verhaltensbegutachtungen durchlaufen. Für weitere Anforderungen an das Managementsystem wird auf IAEA-Sicherheitsstandards in der Veröffentlichung *„Leadership and Management for Safety“,* IAEA Safety Standards Series No. GSR Part 2, 2016 verwiesen. /IAE18n02/

IT-Sicherheits-Richtlinie

Die IT-Sicherheitsrichtlinie muss Anforderungen beinhalten, die sich mit der IT-Sicherheit von I&C-Systemen befassen. Entsprechend müssen diese Anforderungen von allen an Aktivitäten während der Lebensdauer des I&C-Systems beteiligten Organisationen (Anlagenbetreiber, Hersteller, Auftragnehmer und Lieferanten) eingehalten werden. Jede an Aktivitäten während der Lebensdauer des I&C-Systems beteiligte Organisation muss die erforderlichen Standards und Prozeduren identifizieren, dokumentieren und einhalten, die mit den IT-Sicherheitsrichtlinien übereinstimmen. Auf diese Weise ist sicherzustellen, dass Hardware, Software und Firmware keine schadhaften Funktionen und/oder Programmcode enthalten, die Angreifern den Zugriff auf das betreffende I&C-System erleichtern könnten. /IAE18n02/

Sicherungsmaßnahmen

Der Anlagenbetreiber muss sicherstellen, dass die Hersteller, Auftragnehmer und Lieferanten von I&C-Systemen die relevanten Sicherungsmaßnahmen umsetzen, um die Anzahl möglicher Schwachstellen zu minimieren und einen IT-Angriff über die Lieferkette zu verhindern. Die entsprechenden Methoden, Prozesse und Werkzeuge der Hersteller, Auftragnehmer und Lieferanten müssen geprüft werden. Dazu gehören auch, je nach vertraglicher Festlegung mit dem Anlagenbetreiber, Werksabnahmeprüfungen, IT-Sicherheitsinspektionen oder Audits. Sicherungsmaßnahmen können den drei folgenden Kategorien zugeordnet werden: /IAE21n01/

- Technische Kontrollmaßnahmen: Hardware- und/oder Softwarelösungen zum Schutz vor, zur Erkennung und zur Abschwächung von und zur Wiederherstellung nach IT-Sicherheitsvorfällen oder anderen schadhaften Einwirkungen.

- Physische Kontrollmaßnahmen: Physische Barrieren zum Schutz vor physischem Schaden oder physischem, unautorisierten Zugriff. Zu diesen Maßnahmen gehören der Einsatz von Wachpersonal, Schlösser, Zäune, Tore, Einfassungen, Manipulationsanzeigen und Isolationsräume.
- Administrative Kontrollmaßnahmen: Richtlinien, Prozeduren und Praktiken zur Kontrolle personeller Handlungen und Verhaltensweisen. Zu den Kontrollmaßnahmen gehören Management- und Betriebsmaßnahmen sowie die Etablierung einer starken Sicherheitskultur.

Wenn IT-Systeme nur ein geringes Maß an Sicherheit erfordern, dann ist der externe Remote-Zugriff durch autorisierte Benutzer unter der Voraussetzung gestattet, dass zuvor geeignete Sicherungsmaßnahmen umgesetzt wurden. Die physische Verbindung von Drittgeräten mit Systemen und Netzwerken wird technisch kontrolliert. Diese Schnittstellen zu übergeordneten Systemen werden unabhängig voneinander charakterisiert und bewertet, um die Einhaltung der IT-Sicherheitsarchitektur sicherzustellen. /IAE21n03/

Es sollten nur sichere, vertrauenswürdige Update-Mechanismen verwendet werden. Es muss sichergestellt sein, dass das Risiko minimal ist, dass die Aktualisierung als Angriffsroute für das zu aktualisierende System verwendet wird. Zum Beispiel indem Systemaktualisierungen durch verschlüsselte Signaturen autorisierter Anbieter identifiziert werden. Anbieter veröffentlichen Sicherheitsupdates für IT-Systeme typischerweise in Form von Patches, um Schwachstellen zu beheben, die in ihren Systemen identifiziert wurden. Da Änderungen an Sicherheitssystemen ressourcenintensiven Verfahren unterliegen, ist die sofortige Installation eines Patches möglicherweise nicht möglich, wodurch das System für einige Zeit gefährdet bleibt. Dies ist entsprechend zu berücksichtigen. /IAE21n03/

Schulungsprogramm zur IT-Sicherheit und Beobachtung der IT-Sicherheitslage

Die eigenen Mitarbeiter und die Mitarbeiter von Subunternehmen und Drittanbietern müssen ein Schulungsprogramm zur IT-Sicherheit durchlaufen. Dieses sollte die folgenden Punkte berücksichtigen: /IAE11n02/

- Der erfolgreiche Abschluss des Schulungsprogramms muss eine Voraussetzung für den Zugriff auf IT-Systeme sein. Die Schulung sollte der Sicherheitsebene des Systems und der zugedachten Rolle des Teilnehmers entsprechen.

- Für Individuen, welche Schlüsselrollen bei der IT-Sicherheit einnehmen, müssen erweiterte Schulungen und Qualifikationen erfolgen.
- Zur Berücksichtigung neuer Sicherungsmaßnahmen und aufgrund der Entwicklung der IT-Sicherheitslage, müssen die Schulungen regelmäßig wiederholt werden.
- Das Personal muss seine jeweiligen Verantwortlichkeiten zur Erfüllung der IT-Sicherheit erkennen und bestätigen.
- Die Effektivität der Schulungen muss überprüft werden. Darüber hinaus müssen die Schulungen regelmäßig überarbeitet und verbessert werden.

- Die Schulungen zur IT-Sicherheit sollten die folgenden Inhalte vermitteln: /IAE21n01/
- Bewusstsein zur IT-Bedrohungslage und den möglichen Angriffstechniken
- Bewusstsein über die möglichen Folgen von Social Engineering und Anleitungen diesem zu widerstehen
- Erkennung und Reaktion auf einen IT-Angriff
- Individuelle Verantwortlichkeiten zur Einhaltung der IT-Sicherheit und Strafen bei Nichteinhaltung
- Mögliche Auswirkungen von IT-Angriffen auf die nukleare Sicherheit und Sicherung
- Maßnahmen zur Einhaltung der IT-Sicherheit
- Gebrauch von tragbaren Geräten und Wechselmedien
- Gebrauch sozialer Medien
- Änderungen des Ausmaßes oder der Art der IT-Bedrohungslage oder der Risiken

Das Schulungsprogramm muss sich auf Arbeiten sowohl in als auch außerhalb der Anlage beziehen.

Es muss eine Ereignisbearbeitung für relevante IT-Sicherheits-Vorfälle eingerichtet werden. Anlagenbetreiber, Hersteller, Auftragnehmer und Lieferanten müssen die aktuelle IT-Sicherheitslage und bekannt gewordene relevante IT-Sicherheitsvorfälle, auch

außerhalb des nuklearen Sektors, berücksichtigen, sich darüber austauschen und ihre weitere Vorgehensweise koordinieren. /IAE11n02, IAE21n01/

Notfallpläne

Anlagenbetreiber, Hersteller, Auftragnehmer und Lieferanten müssen bei einem IT-Angriff die von staatlichen Institutionen für den nuklearen Sektor festgelegten Maßnahmen ergreifen. Organisationen inklusive des Anlagenbetreibers, die an Aktivitäten während der Lebensdauer eines I&C-Systems beteiligt sind, müssen Notfallpläne und Prozeduren entwickeln, um bei IT-Sicherheitsvorfällen ein weiteres Fortschreiten und eine weitere Eskalation des Vorfalls zu verhindern. Um dies zu realisieren, muss die Möglichkeit zur Informationsbeschaffung bei einem Vorfall gegeben sein. Zu den Notfallplänen und Prozeduren gehören Backups und Sicherungskopien von Software, wichtigen Daten und Konfigurationsdateien. Diese Kopien müssen vom Ursprungsort physisch getrennt aufbewahrt und durch Sicherungsmaßnahmen geschützt werden, um eine Manipulation oder ein Löschen der Daten zu verhindern. Die Notfallpläne und Prozeduren müssen regelmäßig auf Schwachstellen überprüft und gegebenenfalls nachgebessert werden. /IAE18n02, IAE21n01/

Entwicklung von I&C-Systemen in gesicherten Entwicklungsumgebungen

Sowohl für interne als auch für externe Organisationen gilt, dass die Entwicklung von I&C-Systemen innerhalb einer gesicherten Entwicklungsumgebung erfolgen muss. Die Zuweisung dieser Umgebung zu einer Sicherheitsstufe muss die Sicherheitseinstufungen des betreffenden I&C-Systems, anderer in der Entwicklungsumgebung befindlicher Systeme und die der verwendeten Entwicklungswerkzeuge berücksichtigen. Die Sicherungsmaßnahmen für die Entwicklungsumgebung müssen ihrer Sicherheitseinstufung entsprechen. Die Entwicklungsumgebung muss als eigenständige Umgebung verstanden werden, die physisch und logisch von den Betriebs- und Geschäftsumgebungen zu trennen ist. Dazu sind die folgenden Aspekte zu erfüllen: /IAE18n02/

- Administrative Kontrollmaßnahmen z.B. in Form einer Konfigurationskontrolle oder eines geeigneten Asset Managements
- Physische Kontrollmaßnahmen zur Kontrolle des Zugriffs auf die Entwicklungsumgebung

- Es ist sicherzustellen, dass Testausrüstungen und unterstützende Ausrüstungen nicht dazu verwendet werden können schadhaften Programmcode oder schädliche Daten in die Entwicklungsumgebung einzuschleusen.
- Sicherungsmaßnahmen dienen dazu die Integrität der Entwicklungsumgebung beim Austausch mit anderen Umgebungen sicher zu stellen, das Einbringen schadhaften Programmcodes zu verhindern und sensible Daten des I&C-Systems zu schützen. Sie sollten sowohl administrative als auch technische Kontrollmaßnahmen, wie z.B. automatisierte Zugriffskonfigurationssysteme, beinhalten.
- Werkzeuge von Herstellern und Drittanbietern, die in der Entwicklungsumgebung eingesetzt werden sollen, müssen der Sicherheitseinstufung der Entwicklungsumgebung entsprechend angemessen getestet, verifiziert und geschützt werden.

Bewertung und Management der Lieferkette

Die Bewertung und das Management der Lieferkette sind erforderlich, um sicherzustellen, dass der verifizierte Beschaffungsprozess von Geräten und Dienstleistungen konsequent befolgt und nicht manipuliert wird. Vor der Vereinbarung von Verträgen müssen Anbieter, Auftragnehmer und Lieferanten überprüft werden. Solche Überprüfungen können eine Analyse der Prozesse umfassen, die verwendet werden, um sensible, digitale Geräte zu entwerfen, zu entwickeln, zu testen, zu implementieren oder zu unterstützen, oder die Bewertung der Schulung und Erfahrung bei der Entwicklung von sensiblen, digitalen Geräten auf der erforderlichen IT-Sicherheitsebene. Die Überprüfungen können auch dabei helfen die Vertrauenswürdigkeit des Vertriebswegs zu ermitteln. Sie sind dann Teil des Risikomanagements und dienen dazu festzustellen, ob primäre Anbieter, Auftragnehmer oder Lieferanten Sicherungsmaßnahmen ergriffen haben, um die Vertrauenswürdigkeit untergeordneter Anbieter, Auftragnehmer und Lieferanten ordnungsgemäß zu bewerten und ob die vertrauenswürdige Herkunft von sensiblen, digitalen Geräten und deren Komponenten sowie Software und Updates sichergestellt ist. Alle Anbieter, Auftragnehmer und Lieferanten von sensiblen, digitalen Geräten müssen über Verfahren verfügen, um den Betreiber im Falle von Vorfällen in der Lieferkette zu benachrichtigen, die sich auf die Geräte auswirken können (z. B. Kompromittierung von Komponenten, Technologie, Entwicklungsprozesse oder sensiblen Informationen). Sie müssen entsprechende Maßnahmen umsetzen, um auf Risiken reagieren zu können, die sich aus Änderungen oder Beeinträchtigungen von Sicherheitssystemen aufgrund von Umwelt- oder Strukturänderungen ergeben. /IAE21n03/

4.2.2 Normen

Im Rahmen des Vorhabens wurden internationale Normen aus den Bereichen IT-Sicherheit, Leittechnik und Cybersicherheit in der Industrie hinsichtlich des Aspekts der IT-Sicherheit in der Lieferkette analysiert. Dabei handelt es sich um zwei Normen und eine Normenreihe: Die ISO/IEC 27001 bzw. 27002 ist in der Anwendung hinsichtlich verschiedener Unternehmen und Organisationen aus unterschiedlichen Branchen und Bereichen weit verbreitet und befasst sich im Wesentlichen mit Anforderungen für Einführung und Etablierung eines dokumentierten Informationssicherheits-Managementsystems. Die Norm IEC 62645:2019 /DIN20n01/ legt Anforderungen und Leitfäden für die Entwicklung und das Management hauptsächlich digitaler leittechnischer Komponenten im kerntechnischen Umfeld fest. Die Normenreihe IEC 62443 behandelt allgemein industrielle (Kommunikations-)Netze hinsichtlich des Aspekts der Cybersicherheit. Im Folgenden werden die im Rahmen des Vorhabens relevanten Aspekte aus den jeweiligen Normen kurz zusammengefasst.

ISO/IEC 27001/27002

Der Fokus der Norm ISO 27001 „Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen“ /ISO17n02/ liegt auf der Festlegung von Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS). Ein solches ISMS *„verfolgt eine ganzheitliche, koordinierte Betrachtung der Risiken in der Informationssicherheit eines Unternehmens, um eine umfassende Sammlung von Maßnahmen zur Informationssicherheit im Rahmen eines einheitlichen Managementsystems einführen zu können“* /ISO17n02, ISO17n03/. In einem normativen Anhang listet die ISO 27001 Referenzmaßnahmen auf. Diese Referenzmaßnahmen werden in der Norm ISO 27002 *„Informationstechnik – Sicherheitsverfahren – Leitfaden für Informationssicherheitsmaßnahmen“* /ISO17n03/ wieder aufgenommen und jeweils durch eine Anleitung zur Umsetzung und weitere Informationen ergänzt.

Die ISO 27001 geht hierbei zunächst auf die Grundlagen eines ISMS in Form der Verantwortlichkeiten für Vorgaben und Unterstützung für die Informationssicherheit ein. Hierbei wird bereits in der ersten Referenzmaßnahme deutlich, dass sich diese Vorgaben nicht ausschließlich auf die Organisation beziehen, die das ISMS einführt, sondern dass unter anderem einen Zusammenhang mit externen Organisationen besteht: *„Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt,*

herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht“ /ISO17n02/. Für die IT-Sicherheit in der Lieferkette von IT-Systemen ist der Lebenszyklus der IT-Systeme von besonderer Bedeutung. Daher verfolgt die ISO 27001 auch das Ziel, sicherzustellen, dass Informationssicherheit im Entwicklungszyklus von Informationssystemen geplant und umgesetzt ist. Hierzu listet sie nicht nur Anforderungen an die organisationsintern angesiedelten Abschnitte des Lebenszyklus auf, sondern fordert: *„Die Organisation beaufsichtigt und überwacht die Tätigkeit ausgegliederter Systementwicklung“* /ISO17n02/. ISO 27002 spezifiziert diese Aussage noch genauer und listet Punkte auf, die *„über die gesamte externe Lieferkette der Organisation berücksichtigt werden“* sollen /ISO17n03/. Neben vertraglichen *„Anforderungen bezüglich des sicheren Entwurfs, der Programmierung und der Überprüfungspraxis*“ zählen hierzu insbesondere auch die *„Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um zu gewährleisten, dass bei Auslieferung kein vorsätzlich oder versehentlich eingefügter Schadcode enthalten ist“* sowie die *„Vorlage von Nachweisen, dass ausreichende Überprüfungen durchgeführt wurden, um das Vorhandensein bekannter Schwachstellen auszuschließen“* /ISO17n03/.

Zusätzlich widmet die ISO 27001 den Beziehungen zu Lieferanten einen eigenen Abschnitt, in dem sowohl die Informationssicherheit in Lieferantenbeziehungen als auch die Steuerung von deren Dienstleistungen angesprochen werden. Die erste hierbei genannte Referenzmaßnahme *„Informationssicherheitsanforderungen zur Verringerung von Risiken im Zusammenhang mit dem Zugriff von Lieferanten auf Werte der Organisation werden mit dem Zulieferer vereinbart und sind dokumentiert“* /ISO17n02/ zielt darauf ab, dass die Beziehungen zu Lieferenten aus dem Blickwinkel der Informationssicherheit spezifisch geregelt und abgesichert sind. Dies schließt unter anderem die *„Festlegung der jeweiligen Art und Weise der Informationszugriffs für die verschiedenen Arten von Lieferanten sowie Überwachung und Kontrolle des Zugriffs“* und *„Mindestanforderungen an die Informationssicherheit für jede Informations- und Zugriffsart“* ebenso ein wie *„Prozesse und Verfahren zur Überwachung der Einhaltung der festgelegten Anforderungen an die Informationssicherheit für jede Lieferanten- und Zugriffsart, einschließlich Überprüfung durch Dritte und Produktvalidierung“* /ISO17n03/. Darüber hinaus werden *„Genauigkeits- und Vollständigkeitskontrollen zur Sicherstellung der Integrität der Informationen bzw. der von den einzelnen Parteien vorgenommenen Informationsverarbeitung“* gefordert /ISO17n03/.

Eine weitere Referenzmaßnahme beschäftigt sich mit der Behandlung der Informationssicherheit in Bezug auf Lieferanten durch Festlegung entsprechender Vereinbarungen:

„Alle relevanten Informationssicherheitsanforderungen werden mit jedem Lieferanten, der Zugang zu Information der Organisation haben könnte, diese verarbeiten, speichern, weitergeben könnte oder IT-Infrastrukturkomponenten dafür bereitstellt, festgelegt und sind vereinbart“ /ISO17n02/. Zu den zu treffenden Vereinbarungen zählen beispielsweise die *„Verpflichtung der Vertragsparteien zur Umsetzung einer Reihe vereinbarter Maßnahmen, die Zugangssteuerung, Leistungsüberprüfung, Überwachung, Meldung und Auditierung umfassen“*, das *„Recht zur Überprüfung der Lieferantenprozesse und Maßnahmen im Zusammenhang mit dem Vertrag“* sowie die *„Verpflichtung des Lieferanten, in regelmäßigen Abständen einen unabhängigen Bericht zur Wirksamkeit der Maßnahmen vorzulegen und Zusicherung, relevante Probleme zu beheben, die im Bericht erwähnt werden“* /ISO17n03/. Speziell eingegangen wird hierbei auch auf Einzelaspekte wie *„Anforderungen und Verfahren für die Handhabung von Vorfällen (insbesondere Benachrichtigung und Zusammenarbeit bei der Behebung von Vorfällen)“* und *„relevante Vorschriften für Unteraufträge, einschließlich der umzusetzenden Maßnahmen“* /ISO17n03/.

Eine weitere Referenzmaßnahme der ISO 27001 zielt auf die Festlegung von *„Anforderungen für den Umgang mit Informationssicherheitsrisiken, die mit Informations- und Kommunikationsdienstleistungen und der Produktlieferkette verbunden sind, werden in Vereinbarungen mit Lieferanten aufgenommen*“ /ISO17n02/. ISO 27002 führt detailliert aus, welche Themen in den Lieferantenvereinbarungen im Zusammenhang mit der Sicherheit der Lieferkette zu berücksichtigen sind /ISO17n03/:

- *„Festlegung der Anforderungen an die Informationssicherheit, die bei Informations- und Kommunikationstechnologie-Produkten oder dem Ankauf von Diensten zusätzlich zu den allgemeinen Anforderungen an die Informationssicherheit bei Lieferantenbeziehungen Anwendung finden“;*

- *„Anforderungen an die Lieferanten von Informations- und Kommunikationstechnologie-Produkten, die Sicherheitsanforderungen der Organisation innerhalb der gesamten Lieferkette weiterzugeben für den Fall, dass die Lieferanten Unterlieferanten für Teile der Informations- und Kommunikationstechnologie beauftragen, die für die Organisation bereitgestellt werden“;*

- *„Anforderungen an die Lieferanten von Informations- und Kommunikationstechnologie-Produkten, entsprechende Sicherheitspraktiken innerhalb der gesamten Lieferkette weiterzugeben für den Fall, dass diese Produkte Komponenten beinhalten, die von anderen Lieferanten zugekauft wurden";*

- *„Umsetzung eines Überwachungsprozesses sowie geeigneter Methoden zur Sicherstellung, dass die bereitgestellten Informations- und Kommunikationstechnologie-Produkte den festgelegten Sicherheitsanforderungen entsprechen";*

- *„Umsetzung eines Prozesses zur Festlegung von Produkt- oder Dienstkomponenten, die zur Aufrechterhaltung der Funktion wesentlich sind und daher einer besonderen Aufmerksamkeit und Prüfung bedürfen, wenn sie außerhalb der Organisation erstellt werden, insbesondere wenn der führende Lieferant bestimmte Aspekte der Produkt- oder Dienstkomponenten an andere Lieferanten untervergibt";*

- *„Einholen der Zusicherung, dass kritische Komponenten und ihr Ursprung über die gesamte Lieferkette verfolgt werden können";*

- *„Einholen der Zusicherung, dass die bereitgestellten Informations- und Kommunikationstechnologie-Produkte wie erwartet funktionieren und keine unerwarteten oder unerwünschten Eigenschaften aufweisen";*

- *„Festlegung von Regeln für die Mitteilung von Informationen bezüglich der Lieferkette und möglicher Probleme und Kompromisse zwischen der Organisation und den Lieferanten";*

- *„Umsetzung spezifischer Prozesse für das Management des Lebenszyklus und der Verfügbarkeit von Komponenten der Informations- und Kommunikationstechnologie sowie der damit verbundenen Sicherheitsrisiken. Dazu gehört der Umgang mit Risiken durch Komponenten, die nicht mehr erhältlich sind, da deren Anbieter nicht mehr geschäftlich tätig sind oder diese Komponenten aufgrund des technischen Fortschritts nicht mehr bereitstellen".*

Ein weiterer für die Informationssicherheit in der Lieferkette relevanter Aspekt, der in ISO 27001 behandelt wird, ist die Überwachung und Überprüfung von Lieferantendienstleistungen: *„Organisationen überwachen, überprüfen und auditieren die*

Dienstleistungserbringung durch Lieferanten regelmäßig“ /ISO17n02/. Hierbei stellt die ISO 27002 noch einmal klar, dass die gesamte Lieferkette, also auch die Beziehung der Lieferanten zu deren Lieferanten zu betrachten ist. Zusätzlich betrachtet die ISO 27001 die Handhabung der Änderungen von Lieferantendienstleistungen: *„Änderungen bei der Bereitstellung von Dienstleistungen durch Lieferanten werden gesteuert. Solche Änderungen umfassen auch die Pflege und Verbesserung bestehender Informationssicherheitsrichtlinien, -verfahren und –maßnahmen. Dabei werden die Kritikalität der betroffenen Geschäftsinformation, -systeme und -prozesse und eine erneute Risikobeurteilung beachtet“* /ISO17n02/.

Weiterhin beinhalten ISO 27001 und ISO 27002 auch Anforderungen an die Außerbetriebnahme-Phase des Lebenszyklus von IT-Systemen. In Bezug auf die Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln wird gefordert, *„alle Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten“* zu überprüfen, *„um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind“* /ISO17n02/. Hierzu wird ausgeführt, dass *„Speichermedien, die vertrauliche oder urheberrechtlich geschützte Informationen enthalten, […] anstelle der Anwendung der standardmäßigen Lösch- oder Formatierungsfunktion physisch zerstört oder die Informationen […] mittels geeigneter Verfahren dergestalt zerstört, gelöscht oder überschrieben werden“* sollten, *so „dass die ursprünglichen Informationen nicht wiederhergestellt werden können“*. Es wird auch darauf hingewiesen, dass sich *„zusätzlich zur sicheren Datenträgerlöschung […] durch Gesamtverschlüsselung des Datenträgers das Risiko einer Offenlegung vertraulicher Informationen bei der Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln“* unter Einhaltung bestimmter Voraussetzungen verringern lässt. /ISO17n03/. Für Datenträger gibt es ebenfalls eine Anforderung an deren sichere Entsorgung. Zusätzlich dazu wird im Hinblick auf Datenträger mit einer Anforderung an deren Schutz während des Transports auch noch auf eine weitere Phase des Lebenszyklus eingegangen: *„Datenträger, die Information enthalten, sollten während des Transports vor unbefugtem Zugriff, Missbrauch oder Verfälschung geschützt werden“* /ISO17n02/ Hierbei ist anzumerken, dass die ISO 27002 zu den Datenträgern nicht nur Wechseldatenträger, sondern beispielsweise auch Papierdokumente zählt.

Auch wenn es sich bei den Anforderungen in ISO 27001 und damit letztlich den Anforderungen in ISO 27002 im Hinblick auf die Lieferkette von IT-Systemen um formale Punkte handelt, die im Rahmen eines ISMS Beachtung finden müssen, zeigen vor allem die in ISO 27002 spezifizierte Aspekte zu Lieferantenvereinbarungen im

Zusammenhang mit der Sicherheit der Lieferkette deutlich, welch großen Stellenwert die Informationssicherheit in der Lieferkette für die Informationssicherheit einer Organisation besitzt.

IEC 62645:2019

Grundsätzlich erstreckt sich der Anwendungsbereich der IEC 62645 *„Kernkraftwerke - Leittechnische und elektrische Systeme - Anforderungen an die Cybersicherheit“* /DIN20n01/ zwar auf die IT-Sicherheit von IT-Systemen, aber nicht zwangsläufig auf alle Aspekte der Lieferkette dieser IT-Systeme*: „Dieses Dokument ist auf die in Kernkraftwerken eingesetzten programmierbaren digitalen leittechnischen Systeme begrenzt, einschließlich der vor Ort vorhandenen Wartungs- und Konfigurationswerkzeuge. Es zielt nicht unmittelbar auf Entwicklungswerkzeuge und Gerätefamilien ab, die typischerweise bei Lieferanten vorhanden sind. Dennoch könnten Entwicklungswerkzeuge und Gerätefamilien von dem vorliegenden Dokument betroffen sein, um die entwickelten leittechnische Systeme und Architekturen so herzustellen, dass sie seine Anforderungen erfüllen.“* /DIN20n01/

Die DIN IEC 62645 beinhaltet dennoch an mehreren Stellen Anforderungen, die direkt oder indirekt auf die IT-Sicherheit in der Lieferkette von IT-Systemen ausgerichtet sind. So gibt es Anforderungen an die Lieferkette von IT-Systemen beispielsweise im Bereich der Verantwortlichkeiten. Da während der Auslegungs- und Entwicklungsphase verschiedene Unternehmen für die Entwicklung der unterschiedlichen leittechnischen Systeme verantwortlich sein können, wird gefordert, *„die Pflichten der Leittechnikzulieferer bezüglich der IT-Sicherheit eindeutig“* festzulegen und zu *„überprüfen, dass sie erfüllt werden“.* Weiterhin müssen *„alle an irgendwelchen Teilabschnitten des Lebenszyklus von programmierbaren digitalen leittechnischen Systemen beteiligten Organisationen […] den Organisationsaufbau und die zugehörigen Verantwortlichkeiten jeder Position in der Organisation, die zum IT-Sicherheitsprogramm dieser Systeme beiträgt, dokumentieren.“*/DIN20n01/

Darüber hinaus bezieht sich eine der Anforderungen an das IT-Sicherheitsprogramm für programmierbare digitale leittechnische Systeme auch auf die Lieferkette. Konkret gefordert wird hierbei die „*Einführung von Sicherheitsanforderungen für die Vorbereitung und Formalisierung der Übergabe von Hardware, Daten, Software, Code oder Informationen zwischen unterschiedlichen Standorten der Auslegenden oder zwischen einem Auslegenden und einer dritten Person oder zwischen dem Auslegenden und dem*

Kraftwerk.“ Auch an den IT-Sicherheitsplan der Leittechnik gibt es in DIN IEC 62645 Anforderungen, die sich auf die Lieferkette der IT-Systeme beziehen /DIN20n01/:

- *„Der IT-Sicherheitsplan der Leittechnik muss für die primäre Auslegungsorganisation und alle dritten Parteien oder Unterauftragnehmer gelten, die am Projekt arbeiten.“*

- *„Es muss ein Projekt-IT-Sicherheitsplan der Auslegung erstellt werden, der den Lizenznehmer/Betreiber, aber auch dritte Parteien und externe Instanzen die in dem Projekt involviert sind, abdeckt.“*

- *„Insbesondere muss der Auslegende zeigen, dass*

  a) eine Sicherheitsstrategie etabliert ist;

  b) eine solche Strategie an jedem ihrer Entwicklungsstandorte gilt;

  c) sie über örtliche Aspekte hinweg vollständig ist;

  d) *sie sicherstellt, dass ihre eigenen dritten Parteien ein adäquates Sicherheitsniveau einhalten.“*

Auch wenn es sich bei den Anforderungen in DIN IEC 62645 im Hinblick auf die Lieferkette von IT-Systemen um allgemeine und formale Punkte handelt, macht insbesondere die letztgenannte Forderung deutlich, dass sich IT-Sicherheitsbetrachtungen auch auf die Lieferkette von IT-Systemen erstrecken müssen und die Verantwortlichkeit hierfür letztlich bei den kerntechnischen Anlagen und Einrichtungen liegt, die diese IT-Systeme einsetzen. Dies wird auch im Abschnitt zur Außerbetriebsetzung von IT-Systemen deutlich, in dem unter anderem beschrieben wird, dass die Außerbetriebssetzungsphase primär der Verantwortung des Anlagenmanagements unterliegen muss und Prozeduren zur Außerbetriebssetzung von programmierbaren digitalen leittechnischen Gerätschaften und zur kontrollierten Entsorgung von Speichermedien und installierter Software zur Verhinderung der Freigabe vertraulicher Information vorhanden sein müssen.

IEC 62443

Die Normenreihe „IEC 62443“ befasst sich mit dem Thema der Cybersecurity in der Industrieautomatisierung, wobei ein ganzheitlicher Ansatz für Hersteller, Integratoren und Betreiber verfolgt wird. Betrachtet werden dabei sogenannte ,,Industrial Automation and Control Systems“ (IACS). Dies umfasst alle Bestandteile, die für den zuverlässigen und sicheren Betrieb von einer automatisierten Produktionsanlage benötigt werden, wie beispielsweise Systeme, Komponenten und Prozesse. Die Ursprünge dieser Normenreihe gehen auf die Automatisierungstechnik der Prozessindustrie zurück, wobei die Anwendungsbereiche inzwischen aber alle Industriebereiche inklusive der kritischen Infrastruktur abdecken.

Die Normenreihe besteht aus sechs verschiedenen Teilen, wobei sich die Teile fünf und sechs, sowie verschiedenen den Teilen 1-4 zugeordneten Normen noch in der Vorbereitungsphase befinden (Stand Juli 2022). Abbildung 4 zeigt eine grafische Übersicht der sechs Teile und den ihnen zugehörigen Normen.

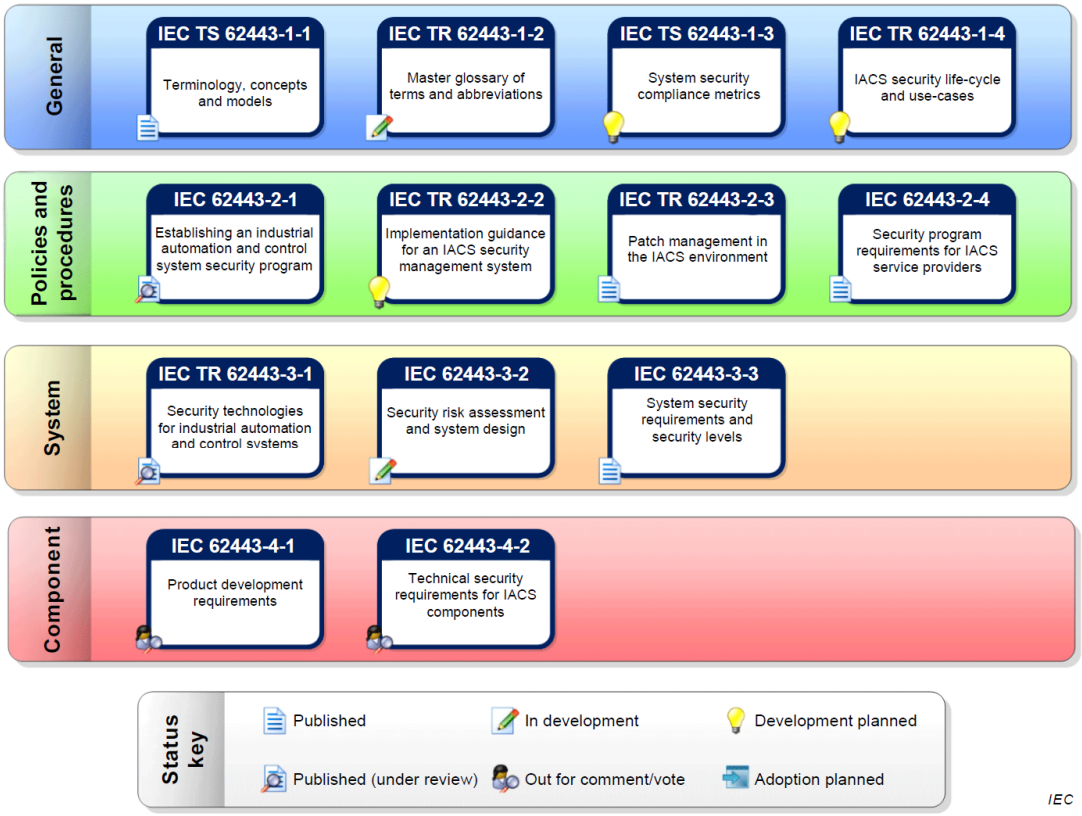

Abb. 4.5 Übersicht über den Aufbau der Normenreihe 62443. /DIN18n01/

Im Rahmen der Bearbeitung der Normenreihe wurden Teile der Normenreihe identifiziert, die für das Vorhaben Relevanz besitzen und entsprechend das Thema IT-Sicherheit in der Lieferkette behandeln. Dabei wurden im Wesentlichen die Teile 2 (Sicherheitsanforderungen für Betreiber und Dienstleister) und 4 (Sicherheitsanforderungen an Automatisierungskomponenten) betrachtet, wobei insbesondere die Teile 2-3 (Patch management in the IACS (Industrial Automation and Control Systems) environment) /IEC15n01/, 2-4 (Security program requirements for IACS service providers) /DIN20n05/ und 4-1 (Secure product development lifecycle requirements) /DIN18n01/ für das Vorhabend relevante Inhalte aufweisen. Im Folgenden werden diese drei Teile hinsichtlich des Aspekts der IT-Sicherheit in der Lieferkette zusammengefasst.

Der Teil „Patch management in the IACS environment“ behandelt die Aspekte des Patch-Managements für IACS bezüglich der Cybersicherheit. Das Patch-Management ist essenzieller Teil der Cybersicherheitsstrategie und umfasst die Installation von Patches bzw. Softwareupdates, Softwareupgrades, Firmwareupgrades, Service-Packs, Hotfixes, BIOS-Updates und anderer digitaler Updates beispielsweise zur Behebung von Bugs und Schwachstellen. Das Dokument richtet sich dabei in seinen Anforderungen an Betreiber und Hersteller für IACS-Produkte. Der Fokus liegt auf dem Thema Kompatibilität und ordnungsgemäßen Patch-Vorgängen, jedoch wird das Thema IT-Sicherheit in einigen Abschnitten adressiert.

In Abschnitt 4 der Norm geht es beispielsweise im Wesentlichen um die Durchführung von Patches für IACS, dabei auftretende Probleme, die möglichen Auswirkungen von mangelhaftem Patch-Management, Lebenszyklen von Patches und die Problematik, wenn keine Patches mehr für verwendete IACS mit bekannten Sicherheitslücken und Schwachstellen vorliegen. Generell stellt das Patchen eines laufenden Systems immer eine Veränderung dar, die möglicherweise negative Folgen haben kann, beispielsweise wenn der Patchvorgang fehlerhaft durchgeführt wird oder der Patch selbst fehlerhafte oder sicherheitstechnisch fragwürdige Eigenschaften hat. Dies ist insbesondere bezüglich der Frage der IT-Sicherheit in der Lieferkette relevant, da Patches möglicherweise kompromittiert sein oder auch ungewollt Angreifern ein Einfallstor bieten können. Als wesentliche Auswirkung von mangelhaftem Patch-Management wird dabei generell ein erhöhtes Risiko zur Kompromittierung von IACS-Systemen gesehen. Im Gegensatz zur Kompromittierung von regulärer Büro-IT stellt eine Kompromittierung von IACS-Systemen ein wesentlich höheres Risiko dar, da möglicherweise Sicherheitssysteme, die Integrität und Sicherheit erzeugter Produkte oder die physische Sicherheit von Personen gefährdet ist.

In Abschnitt 5 der Norm werden empfohlene Anforderungen für Anlagenbetreiber bezüglich des Patch-Managements genannt. Demnach haben Betreiber die Verpflichtung, die Sicherheit, Zuverlässigkeit, Betriebsfähigkeit, Gefahrenabwehr und Qualität ihres Betriebs zu gewährleisten. Die Gewährleistung der Cybersicherheit durch das Patchen von IACS-Anlagen ist demnach ein wichtiger Teil dieser Verpflichtung. Relevante Anforderungen umfassen beispielsweise das Testen von Patches vor der Installation, sodass sichergestellt wird, dass die Zuverlässigkeit und Betriebsfähigkeit des IACS nicht beeinträchtigt wird (Sandboxing) und sowie, dass generell Patches installiert und weitere Maßnahmen vorbereitet werden, um Schwachstellen in den IACS zu mitigieren.

Abschnitt 6 der Norm beschreibt die empfohlenen Anforderungen des Patch-Managements für Hersteller. Als wesentliche Aufgabe für den Hersteller zur Sicherstellung des sicheren Betriebs von IACS in Anlagen wird angegeben, dass die Hersteller Patches und Informationen bereitstellen und diese auch entsprechend testen. Relevante Anforderungen in diesem Bereich beinhalten, dass alle Patches durch den Hersteller hinsichtlich der Anwendbarkeit und Kompatibilität überprüft und insbesondere verifiziert werden, einschließlich der Patches, die vom Hersteller des verwendeten Betriebssystems und von allen Anbietern von Drittsoftware veröffentlicht werden. Zudem sollen die Hersteller Anlagenbetreiber frühzeitig darüber informieren (mindestens zwei Jahre im Voraus), wenn Cybersicherheits-Patches für das Produkt nicht mehr zur Verfügung gestellt werden.

Bezüglich der Anforderungen an Betreiber und Hersteller stellt die Norm in den Anhängen B (Betreiber) und C (Hersteller) weitere Informationen und Empfehlungen zur Verfügung, die im Rahmen des Vorhabens relevant sind. Dabei geht es unter anderem um das Monitoring und die Identifikation von sicherheitsrelevanten Patches. Betreiber sollen demnach eine Auflistung aller verwendeten Systeme (Hardware und Software) und zugehöriger Patch- und Schwachstellen-Informationen erstellen. Dies ist insbesondere nach dem Bekanntwerden von Schwachstellen relevant, sodass die Betreiber stets auf dem aktuellen Informationsstand sind, was mögliche Schwachstellen in Patches angeht. Dazu gehört auch ein regelmäßiger und zuverlässiger Kontakt mit dem Hersteller, sodass sichergestellt wird, dass die Informationen und ggf. ausgetauschten Patches und Dateien vertrauenswürdig sind. Diesbezüglich geht es zudem unter anderem um das Thema Sicherstellung der Authentizität von Patch-Dateien. Diese sollen demnach vor dem Test- und Installationsprozess auf ihre Authentizität und den Ursprung aus einer vertrauenswürdigen Quelle hin untersucht werden. Zunächst soll entsprechend sichergestellt werden, dass der Patch direkt vom Hersteller oder Lieferanten stammt und in Fällen, wo dies nicht möglich ist, soll die Quelle dokumentiert werden. Bezüglich der

Dateien selbst soll überprüft werden, ob Parameter wie die Dateigröße, Hashwerten und digitale Signaturen korrekt und verifiziert sind. Gerade die Überprüfung von Hashwerten bzw. der Vergleich mit Herstellerangaben stellt in der Regel sicher, dass die Dateien auf dem Weg zwischen Hersteller und Betreiber nicht modifiziert wurden. Abschließend wird darauf hingewiesen, dass Virenscans mit aktueller Antivirussoftware durchgeführt werden sollen. Weiterhin wird eine Empfehlung für den Betrieb eines IACS-Patch-Management-Programms und entsprechende Informationen zu Härtungsmaßnahmen gegeben. Bezüglich des Patch-Managements wird dabei auf Sicherungsmaßnahmen und die Entfernung nicht benötigter Komponenten, Features und Rechte verwiesen. Ein expliziter Bezug oder konkrete Maßnahmen bezüglich der IT-Sicherheit in der Lieferkette werden nicht genannt. Vielmehr wird gefordert, insbesondere die Software auf das Mindestmaß bzw. Notwendigste zu reduzieren, und nicht benötigte Software zu entfernen, sodass dort keine vermeidbaren Patch-Vorgänge, die ein potenzielles Risiko darstellen, durchgeführt werden müssen. Zudem werden Empfehlungen für Hersteller/Lieferanten und Service-Provider von IACS-Produkten bezüglich des Patch-Managements gegeben. Hinsichtlich der potenziellen Gefahren bei IT-Angriffen über die Lieferkette wird zur Verteilung von Cybersicherheitsupdates empfohlen, diese über sichere Kanäle bereitzustellen, Sicherheitsinformationen zur Überprüfung der Integrität wie Hash-Werte bereit zu stellen und die entsprechenden Informationen auch für Drittanbieter-Software weiterzugeben, die im IACS-Produkt eingesetzt wird.

Der Teil “Security program requirements for IACS service providers” handelt im Wesentlichen von Sicherheitsanforderungen bezüglich der Maßnahmen und Fähigkeiten von IACS-Dienstleistern. Diese sind im Anhang A themenspezifisch aufgelistet.

Die Unterteilung erfolgt anhand folgender Themen der Sicherheitsanforderungen:

- Training
- Background Checks
- Personnel assignments
- Solution components
- Security tools and software
- Hardening guidelines
- Risk assessment
- Network design
- Solution components
- Devices (all, workstations, network, wireless, control and instrumentation)

- Data protection
- User interface
- Events (security compromises, security related, alarms & events)
- Accounts (user and service accounts, administrator, default, user)
- Passwords
- Manual process
- Portable media
- Patch list
- Security Patch
- Restore
- Backup

Dazu gibt es noch 40 Unterthemen, unter anderem zu den Bereichen Zugriffskontrolle, (externe) Kommunikation, Konnektivität, Kryptographie, Detektion von Events, Installation beispielsweise von Software, Logging, Schadsoftware und Verifizierung. Insgesamt werden über 120 Sicherheitsanforderungen aufgeführt. Die sich in den oben genannten Kategorien und Unterkategorien einsortieren lassen. Darunter finden sich allgemeine organisatorische Anforderungen, wie beispielsweise, dass nur berechtigte und (sicherheits-)überprüfte Personen Zugriff haben und dass auch für beauftragte Drittunternehmen nur vertrauenswürdige Organisationen engagiert werden und dies auch geprüft wird. Es gibt dagegen auch spezifische technische Anforderungen wie beispielsweise bezüglich der Eigenschaften sicherer Passwörter, die Anforderung keine Standardpasswörter zu verwenden und bei mobilen Datenträgern dafür zu sorgen, dass diese frei von Schadsoftware sind und nur für vorgesehene (dienstliche) Zwecke eingesetzt werden.

Der Teil „Secure product development lifecycle requirements“ legt Anforderungen an einen sicheren Produktentwicklungslebenszyklus fest, die von Herstellern von Komponenten und Systemen industrieller Automatisierungs- und Steuerungstechnik einzuhalten sind, wobei auch Aspekte der IT-Sicherheit in der Lieferkette adressiert werden. Zunächst geht es in Abschnitt 5 um die Implementierung eines sicheren Entwicklungsprozesses, der die gesamte Lieferkette berücksichtigt. Hersteller müssen dabei sicherstellen, dass Sicherheitsanforderungen in jeder Phase des Entwicklungslebenszyklus berücksichtigt werden. Dies beginnt mit der Auswahl und Bewertung von Lieferanten und Komponenten und beinhaltet die Konzeption, das Design, die Implementierung, Tests und die Wartung. Dabei dürfen nur nachweislich vertrauenswürdige Lieferanten ausgewählt werden, wobei neben üblichen Nachweispflichten auch Audits und

Sicherheitsbewertungen bei den Lieferanten durchzuführen sind, um entsprechende Sicherheitsprogramme und -prozesse zu überprüfen. Generell ist die Definition angemessener Sicherheitsanforderungen, die auch für externe Komponenten und Dienstleistungen gelten, ein wesentlicher Aspekt, der in Abschnitt 6 aufgegriffen wird. Hersteller müssen dabei sicherstellen, dass ihre Lieferanten diese Anforderungen angemessen umsetzen und dies durch Sicherheitskontrollen überprüfen. Die Implementierung von Prozessen zur Kontinuierlichen Überwachung und Bewertung der Sicherungsmaßnahmen, auch in der Lieferkette, wird in Abschnitt 8 diskutiert. Dabei sind Hersteller angehalten, regelmäßig Risikoanalysen durchzuführen und potenzielle Schwachstellen zu identifizieren, was die Lieferkette einschließt. Die Themen Umgang und Behebung von Sicherheitslücken werden in den Abschnitten 10 und 11 aufgegriffen und adressieren im Wesentlichen Schwachstellen, die entsprechend erkannt, kommuniziert und behoben werden müssen. Dies ist durch den Hersteller auch in Bezug auf Lieferanten sicherzustellen. Für weiterführende Informationen hinsichtlich der Lieferkette wird zudem auf die Norm ISO/IEC 27036-3:2023 (Cybersecurity — Supplier relationships) verwiesen.

4.3 Vergleich des deutschen Regelwerks mit internationalen Vorgehensweisen

Der Vergleich der in den Abschnitten 4.1 und 4.2 betrachteten Regelwerke und Vorgehensweisen ist aufgrund der unterschiedlichen Strukturen, Herangehensweisen und Inhalte hinsichtlich der Fragestellung der Anforderungen in Bezug zur IT-Sicherheit in der Lieferkette und einzelner Sicherungsmaßnahmen nur qualitativ sinnvoll. Dabei wird im Wesentlichen das Gesamtbild des jeweiligen Regelwerks und der darin enthaltenen Vorgaben und Anforderungen betrachtet, wobei je nach Fragestellung auch einzelne Aspekte verglichen und diskutiert werden. Die Auswahl der im Rahmen des Vorhabens betrachteten Dokumente erfolgte hinsichtlich verschiedener Schwerpunkte und Sichtweisen, um einen möglichst breiten Überblick über das Themenfeld zu erfassen. Dazu zählen unter anderem technische Leitfäden mit konkreten Sicherungsmaßnahmen und -anforderungen, auf vertragliche und organisatorische Aspekte ausgelegte Regelwerke sowie einerseits auf das Thema IT-Sicherheit in der Lieferkette fokussierte und andererseits breiter angelegte Dokumente, beispielsweise zu den Themen Cybersicherheit oder Lieferkettenmanagement. Generell ist die Sicherstellung der IT-Sicherheit in der Lieferkette ein zentraler Aspekt der Cybersicherheitsstrategien weltweit, sodass sich in jedem der betrachteten Dokumente direkte oder indirekte Aspekte wiederfinden. Verschiedene Länder und Organisationen verfolgen in den Regelwerken dabei teilweise unterschiedliche Herangehensweisen, um die Herausforderungen in diesem Zusammenhang zu

adressieren. Dabei lässt sich zunächst ein allgemeiner zentraler Punkt identifizieren, der in unterschiedlich detaillierter Ausprägung in allen Herangehensweisen gleichermaßen hervorgehoben wird: die Lieferkette muss bezüglich Fragen der Informationssicherheit im Rahmen der Risikoanalyse und des Risikomanagements adressiert werden. Daneben existierende weitere Gemeinsamkeiten sowie Unterschiede werden im Folgenden diskutiert.

Das betrachtete deutsche Regelwerk adressiert das Thema IT-Sicherheit in der Lieferkette im Wesentlichen als relevanten Teilaspekt innerhalb allgemeinerer Regelwerksdokumente. Das Thema wird in allen betrachteten Dokumenten aufgegriffen und überwiegend im Rahmen leistungsbasierter Anforderungen behandelt. Dies gilt insbesondere für die SEWD-Richtlinie IT. Hier werden im Wesentlichen allgemeine, nicht spezifisch auf die Lieferkette ausgerichtete Sicherheitsanforderungen für Lieferanten und externe Dienstleister ausgeweitet und die Sicherstellung entsprechender Umsetzungen durch diese gefordert, sodass insgesamt ein vergleichbares Sicherungsniveau vorliegen soll. Dies ist vergleichbar mit dem finnischen Ansatz in YVL A.12 (siehe Abschnitt 4.1.4), wobei der Genehmigungsinhaber hier ausgehend von allgemeinen IT-Sicherheitsanforderungen bei der Nutzung externer Ressourcen sicherstellen soll, dass das externe Niveau der Informationssicherheit mindestens den Standards des Genehmigungsinhaber für ähnliche Tätigkeiten entsprechen. Im IT-Sicherheitsgesetz 2.0 sowie in der KTA 3501 finden sich spezifische leistungsbasierte Anforderungen hinsichtlich der Etablierung eines Systems zur Angriffserkennung, der sorgfältigen Auswahl und Anzeige kritischer Komponenten bei Behörden und des Verbots externer Zugriffsmöglichkeiten auf Systeme mit sicherheitskritischen Funktionen. Daneben gibt es viele weitere konkrete Anforderungen, die die IT-Sicherheit in der Lieferkette betreffen, im IT-Grundschutz. Hier werden diverse Aspekte der Cybersicherheit, einschließlich der IT-Sicherheit in der Lieferkette, sowohl mit dem leistungsbasierten wie auch mit dem präskriptiven Ansatz adressiert. Innerhalb der modularen Struktur des IT-Grundschutzes finden sich dabei sowohl Bausteine, die direkt die IT-Sicherheit in der Lieferkette betreffen wie beispielsweise zum Thema Outsourcing oder Fernwartung, als auch Bausteine, die allgemeine Themen der Cybersicherheit behandeln aber für die Lieferkette ebenfalls relevant sind wie zum Beispiel zum Thema Softwareentwicklung oder Kryptokonzept.

Die betrachteten Regelwerke aus den Vereinigten Staaten und Großbritannien adressieren das Thema IT-Sicherheit in der Lieferkette teilweise explizit. In NS-TAST-GD-077 (siehe Abschnitt 4.1.3) werden dabei im Wesentlichen allgemeine vertragliche Aspekte im generellen Zusammenhang mit der Lieferkette diskutiert. Der Bezug zur IT-Sicherheit

wird nicht konkret benannt, jedoch erstreckt sich der Anwendungsbereich auf die Beschaffung sämtlicher Komponenten und Systeme um Zusammenhang mit zivilen Reaktoren. Da dabei der Fokus insbesondere auch auf Genehmigungsverfahren liegt, geht es überwiegend um die Erfüllung von Anforderungen und Umsetzung von (technischen) Spezifikationen innerhalb entsprechender vertraglicher Vereinbarungen. Im Zentrum steht dabei ein Beschaffungszyklus, der durchlaufen wird und dessen Erfahrungen zur Verbesserung zukünftiger Beschaffungen berücksichtigt werden sollen. In ähnlicher Weise stellt das CMMC-Modell des U.S. DoD (siehe Abschnitt 4.1.2) eine Reifegradmodell zur Sicherstellung der Cybersicherheit in der Lieferkette dar, das ein mehrstufiges Zertifizierungssystem umfasst, bei dem Lieferanten verschiedene Sicherheitsebenen erreichen. Dabei ist eine regelmäßige Überprüfung und Rezertifizierung erforderlich. In beiden Fällen geht es somit um die Sicherstellung eines gewissen Sicherheitsniveaus bei Lieferanten, das insbesondere durch vertragliche Vereinbarungen definiert und überprüft wird. Durch die Auflistung unterschiedlicher Sicherungsmaßnahmen in verschiedenen Kategorien innerhalb des CMMC-Modells werden zudem technische Aspekte adressiert. Dies wird in der NIST SP 800-161 (siehe Abschnitt 4.1.2), die thematisch konkret auf die Cybersicherheit in der Lieferkette ausgerichtet ist, durch die dort diskutierten Sicherungsmaßnahmen zudem vertieft betrachtet. Verschiedene relevante Aspekte der Thematik werden hier ausführlich diskutiert und durch die Fokussierung auf die Cybersicherheit in der Lieferkette umfassend betrachtet. Ein solcher Detaillierungsgrad in diesem Zusammenhang durch relevante Veröffentlichungen ausschließlich zu dieser Fragestellung liegt in diesem Umfang für Deutschland insbesondere im nuklearen Kontext bisher nicht vor. Dagegen ergeben sich bezüglich der Aufteilung von Sicherungsmaßnahmen in einzelne Kategorien in einem Ansatz, der sowohl leistungsbasierte als auch präskriptive Aspekte enthält, unter anderem inhaltliche Gemeinsamkeiten mit dem IT-Grundschutz des BSI, der nicht exklusiv die Fragestellung der IT-Sicherheit in der Lieferkette behandelt, diese jedoch in verschiedenen Bausteinen und Abschnitten adressiert (siehe Abschnitt 4.1.1).

Die im Rahmendes Vorhabens betrachteten relevanten Veröffentlichungen der IAEA befassen sich nicht ausschließlich mit dem Aspekt der IT-Sicherheit in der Lieferkette. Die allgemeinen Aspekte bezüglich der IT-Sicherheit sowie in Bezug auf leittechnische Systeme in kerntechnischen Anlagen werden im deutschen Regelwerk an unterschiedlichen Stellen abgedeckt. Inhalte zur IT-Sicherheits-Richtlinie und entsprechenden Sicherungsmaßnahmen werden insbesondere im kerntechnischen Bereich von der SEWD-Richtlinie IT aufgegriffen. Dies trifft ebenso auf die allgemeine Anforderung der Sicherstellung der IT-Sicherheit in der Lieferkette zu, wobei keine konkreten Maßnahmen

vorgeschrieben werden. Darüber hinaus gibt es konkrete Anforderungen in Bezug auf Fragestellungen zur IT-Sicherheit in der Lieferkette wie beispielsweise Patches und (Software)Entwicklung im IAEA-Regelwerk, die sich in Deutschland im Wesentlichen auch in einzelnen Bausteinen des IT-Grundschutz Kompendiums des BSI wiederfinden. Anforderungen in Bezug auf die Auswahl und Bewertung von sicheren Quellen von Hardware- und Softwareprodukten, die in den betrachteten IAEA-Dokumenten diskutiert werden, werden auch in Deutschland, unter anderem neuerdings im IT-Sicherheitsgesetz 2.0 hinsichtlich kritischer Komponenten diskutiert. Die allgemeinen Themengebiete zu Vertragsangelegenheiten, Schulungen und Notfallplänen (siehe Abschnitt 4.2.1) werden im deutschen Regelwerk nicht direkt in den im Rahmen des Vorhabens betrachteten Dokumenten hinsichtlich der IT-Sicherheit in der Lieferkette adressiert, sondern ergeben sich teilweise indirekt aus den entsprechenden Anforderungen zu den jeweiligen Gebieten.

Im Hinblick auf die betrachteten Normen ist zunächst festzuhalten, dass die ISO/IEC 27001/27002 in Bezug auf Anforderungen an Informationssicherheits-Managementsysteme Ähnlichkeiten zum IT-Grundschutz Kompendium des BSI aufweist, wobei letzterer allgemein in der Auswahl abgedeckter Themenbereiche und im Detaillierungsgrad darüber hinausgeht und umfangreicher ist. Beispielsweise ist es mit Hilfe eines vom BSI zertifizierten ISO 27001-Grundschutz-Auditors möglich, die ISO 27001-Zertifizierung auf Basis vom IT-Grundschutz zu erwerben. Dementsprechend finden sich viele der Inhalte dieser Norm in Bezug auf die Sicherstellung der IT-Sicherheit in der Lieferkette auch im BSI-Grundschutz Kompendium des BSI wieder. Bezüglich der Norm IEC 62645:2019 sind die Forderungen bzgl. der Betrachtung des gesamten Lebenszyklus und eines adäquaten Sicherheitsniveaus für Leittechniksysteme bei der Involvierung dritter bzw. externer Parteien in ähnlicher Weise in der deutschen SEWD-Richtlinie IT adressiert, die im Wesentlichen Vorgaben zum Sicherheitsniveau für Dienstleistungen durch Dritte macht und entsprechende Sicherungsmaßnahmen für alle Phasen des Lebenszyklus schutzbedürftiger IT-Systeme vorsieht. Auch im Rahmen des Vorhabens relevante Aspekte der Normenreihe IEC 62443 werden im deutschen Regelwerk adressiert. Dabei ist insbesondere das Thema „Patch-Management“ zu nennen, das ausführlich in Teil 2 der Normenreihe diskutiert wird. Dieses Thema wird im IT-Grundschutz Kompendium unter anderem in einem dedizierten Baustein aufgegriffen. Außerdem werden viele der in der Normenreihe Themen hinsichtlich Sicherheitsanforderungen durch entsprechende Maßnahmen des IT-Grundschutzes abgedeckt, wobei die Normenreihe einen deutlicheren Fokus auf Industriesysteme setzt, wohingegen der IT-Grundschutz breiter aufgestellt ist

und neben industriellen Umgebungen auch konventionelle IT als Schwerpunkt betrachtet.

Zusammenfassend lässt sich sagen, dass die Sicherstellung der IT-Sicherheit in der Lieferkette ein komplexes Thema ist, das in der deutschen Vorgehensweise in verschiedenen Regelwerken integriert ist und sowohl technische wie auch organisatorische Aspekte beinhaltet. Die Herangehensweise entspricht dabei im Wesentlichen einem leistungsbasierten Ansatz, der teilweise – insbesondere im Rahmen des IT-Grundschutz Kompendiums des BSI – präskriptive Aspekte beinhaltet. Im Vergleich zu internationalen Ansätzen zeigt sich, dass in den im Rahmen des Vorhabens betrachteten Regelwerken ähnliche Prinzipien und Vorgehensweisen angewandt werden, jedoch oftmals mit unterschiedlichen Schwerpunkten und Detaillierungsgraden. Während beispielsweise die Vereinigten Staaten ein mehrstufiges Zertifizierungssystem, konkrete Sicherungsmaßnahmen und umfassende Bewertungskriterien mit dedizierten Regelwerken etabliert haben, legen andere betrachtete nationale Regelwerke wie in Großbritannien den Fokus auf Vertragsangelegenheiten. Internationale Normen legen unter anderem Schwerpunkte auf die Definition und Durchsetzung von entsprechenden Sicherungsmaßnahmen. Insgesamt lässt sich feststellen, dass trotz unterschiedlicher Ansätze das Thema IT-Sicherheit in der Lieferkette international direkt oder indirekt adressiert wird und die Notwendigkeit einer robusten Sicherheitsstrategie entlang der Lieferkette insgesamt erkannt und betont wird. Die deutsche Vorgehensweise deckt dabei viele relevante Aspekte ab und ist vergleichbar mit internationalen Best Practices, wobei spezifische Anforderungen und Ansätze je nach nationalem Kontext variieren.

5 Generische Angriffsmuster und Untersuchung der Eignung und Wirksamkeit von Sicherungsmaßnahmen in Bezug auf die IT-Sicherheit in der Lieferkette

Ausgehend von den in Kapitel 3 betrachteten IT-Sicherheitsvorfällen im Zusammenhang mit der Lieferkette wurden im Rahmen des Vorhabens Angriffsmöglichkeiten im Zusammenhang mit der Cybersicherheit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems sowie Gemeinsamkeiten, generischen Aspekten und abgeleitete Sicherungsmaßnahmen betrachtet. Weiterhin wurde im Rahmen des Vorhabens untersucht, inwieweit die in Kapitel 4 beschriebenen internationalen Vorgehensweisen - insbesondere im Rahmen des deutschen Ansatzes – dazu geeignet sind, IT-Angriffe im Zusammenhang mit der Lieferkette mit präventiven oder reaktiven Sicherungsmaßnahmen bzw. Maßnahmen zur Detektion zu erschweren, zu verzögern, zu detektieren, zu mitigieren oder zu verhindern. Dazu wurden zunächst, ausgehend von den Angriffsmöglichkeiten und generischen Aspekten der betrachteten IT-Sicherheitsvorfälle, generische Angriffsmuster definiert, bevor die Eignung und Wirksamkeit der unterschiedlichen Sicherungsmaßnahmen für diese Angriffsmuster analysiert und die Abdeckung der Angriffsmuster und Sicherungsmaßnahmen durch das Regelwerk betrachtet wurde. Im Folgenden werden zunächst die Angriffsmöglichkeiten im Zusammenhang mit der Cybersicherheit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems sowie Gemeinsamkeiten, generischen Aspekten und abgeleitete Sicherungsmaßnahmen aufgezeigt. Im Anschluss werden die im Rahmen des Vorhabens definierten Angriffsmuster erläutert und anschließend die Sicherungsmaßnahmen hinsichtlich der verschiedenen Angriffsmuster diskutiert.

5.1 Betrachtung von Angriffsmöglichkeiten im Zusammenhang mit der Cybersicherheit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems

Im Zuge der Analyse der betrachteten und ausgewerteten IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette in den Abschnitten 3.1 und 3.2 gilt es zunächst, verschiedene Angriffsmöglichkeiten im Zusammenhang mit der Cybersicherheit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems zu betrachten. Grundsätzlich unterscheiden sich Supply-Chain-Angriffe unter anderem dadurch, an welcher Stelle der Lieferkette, d. h. in welchem Stadium der Softwareerstellung bzw. Hardwarefertigung der Angriff erfolgt. IT-Systeme „*unterliegen Lebenszyklen, in denen sie konzipiert, festgelegt,*

entworfen, entwickelt, getestet, umgesetzt, genutzt, gepflegt und schließlich ausgemustert und entsorgt werden. Informationssicherheit sollte in jeder Phase berücksichtigt werden" /ISO17n03/. Prinzipiell kann ein Angriff in jedem Stadium erfolgen, wie unter anderem in den Abschnitten 3.1 und 3.2 anhand der betrachteten IT-Sicherheitsvorfällen illustriert ist. Bei den untersuchten IT-Sicherheitsvorfällen zielten Angreifer auf unterschiedliche Phasen im Lebenszyklus von IT-Systemen ab. Um die unterschiedlichen Angriffe zu strukturieren und im Kontext der Cybersicherheit in der Lieferkette einzuordnen, werden im Folgenden zunächst die einzelnen Phasen des Lebenszyklus beschrieben und hinsichtlich der sich daraus ergebenden Angriffsmöglichkeiten analysiert. Dabei wurden nicht nur die im Rahmen der IT-Sicherheitsvorfälle beobachteten, sondern auch im Zusammenhang mit der jeweiligen Phase des Lebenszyklus potenziell denkbare Angriffsmöglichkeiten betrachtet. Die genaue Einteilung verschiedener Phasen im Lebenszyklus von IT-Systemen ist abhängig vom spezifischen Anwendungsfall, wodurch sich in den einzelnen Phasen im Detail bzw. in der Unterteilung ggf. jeweilige Unterschiede ergeben. Für die folgenden Betrachtungen wird der generelle Lebenszyklus von IT-Systemen (Software und Hardware) durch die Phasen „Design", „Development", „Production", „Distribution", „Acquisition", „Deployment", „Operation", „Maintenance" sowie „Disposal" abgebildet. Aufgrund der Internationalität des Themas und zur besseren Vergleichbarkeit mit anderen Veröffentlichungen zu diesem Thema werden hier und im weiteren Verlauf die englisch-sprachigen Begriffsbezeichnungen verwendet.

Die Phasen „Design", „Development" und „Production" werden zusammenhängend betrachtet und umfassen den Soft- und Hardwareentwicklungsprozess bis hin zum fertigen, getesteten Release bzw. Produkt. Das Soft- bzw. Hardwaredesign ist dabei ein elementarer Bestandteil des „Developments". Die Angriffsmöglichkeiten für Cyberangriffe im Zusammenhang mit der Lieferkette umfassen dabei im Wesentlichen:

- Die Kompromittierung des Designs von Hardware- oder Softwarebestandteilen (Spezifikation, Anforderungen, Designprozess).
- Die Manipulation von Entwicklungswerkzeugen oder der Entwicklungsumgebung.
- Die Manipulation von Testwerkzeugen.
- Die Manipulation von Quellcode Repositories.
- Die Injektion von Schadsoftware in legitime Softwarekomponenten vor dem Release.
- Die Manipulation des Build-Prozesses.
- Die Kompromittierung des Herstellungsprozesses von Hardwarebestandteilen.

- Die Manipulation von Quellcode in über Abhängigkeiten eingebundenen externen Softwarebestandteilen.
- Die Kompromittierung von über Abhängigkeiten eingebundenen externen Softwarebestandteilen.
- Das Einbringen von Schadsoftware auf Hardware vor der Auslieferung.
- Die Beschaffung von Informationen über entwickelte Soft- oder Hardwarekomponenten oder andere für die Entwicklung/Einbringung von Schadsoftware relevante Aspekte (z. B. Social Engineering, Diebstahl, Spionage).

Die Phase „Distribution“ umfasst sämtliche Prozesse zur Verteilung, Auslieferung und Übertragung auf der Hersteller- bzw. Händlerseite. Die Angriffsmöglichkeiten für Cyberangriffe im Zusammenhang mit der Lieferkette umfassen dabei im Wesentlichen:

- Den Diebstahl von Zertifikaten zum Signieren manipulierter Software.
- Die betrügerische Beschaffung oder Fälschung von Zertifikaten.
- Andere Manipulation des Signierungsprozesses (einschließlich kryptographischer Hash-Werte).
- Die Injektion von Schadsoftware in legitime, zum Download oder zur Verteilung bereitgestellte Softwarereleases
- Den Eingriff in die Auslieferung, Manipulation während des Transits.
- Den Austausch von legitimen Softwarereleases durch manipulierte Versionen durch Manipulation auf Hersteller- oder Händlerseite.
- Die Manipulation von Updatemechanismen oder Mechanismen zur Verteilung der Software.
- Den Verkauf manipulierter Produkte an legitime Händler.
- Die Kompromittierung von auf Händler- bzw. Herstellerseite eingesetzten Installations- und Inbetriebnahmewerkzeugen.
- Die Manipulation während der durch Händler- bzw. Herstellerseite durchgeführten Installation bzw. Inbetriebnahme.

Die Phasen „Acqusition“ und „Deployment“ werden zusammenhängend betrachtet und umfassen Prozesse zur Beschaffung auf Kundenseite, Integrations-, Installations- und Inbetriebnahmeprozesse. Die Angriffsmöglichkeiten für Cyberangriffe im Zusammenhang mit der Lieferkette umfassen dabei im Wesentlichen:

- Die Injektion von Schadsoftware auf Kundenseite.

- Den Austausch von legitimen Softwarereleases durch manipulierte Versionen auf Kundenseite (USB- Sticks, Servicegeräte etc.).
- Den Verkauf manipulierter Produkte an legitime Händler.
- Die Manipulation von Updatemechanismen.
- Die Kompromittierung von auf Kundenseite eingesetzten Installations- und Inbetriebnahmewerkzeugen.
- Die Manipulation während der durch Kundenseite durchgeführten Installation bzw. Inbetriebnahme.

Die Phasen „Operation“ und „Maintenance“ werden zusammenhängend betrachtet und umfassen Prozesse bei Betrieb und Wartung. Bei der Betrachtung der Phasen „Operation“ und „Maintenance“ ist insbesondere zu berücksichtigen, dass Updates, Patches bzw. ein Hardwareaustausch dabei nicht nur in diese Phase fallen, sondern einen eigenen Lebenszyklus haben. So durchläuft jedes Update zunächst die früheren Phasen des Lebenszyklus von der Softwareentwicklung an, bevor es nach dem Einspielen (Deployment) in die Phasen „Operation“ und „Maintenance“ eintritt. Es ist außerdem zu beachten, dass jede Software und jede Hardware mindestens so lange Verbindungen zu dieser und allen früheren Phasen besitzen, bis sie vom Hersteller nicht mehr unterstützt werden. Selbst nach diesem Zeitpunkt sind in der Praxis Verbindungen in die Phasen „Operation“ und „Maintenance“ üblich. Die Angriffsmöglichkeiten für Cyberangriffe im Zusammenhang mit der Lieferkette umfassen dabei im Wesentlichen:

- Die Kompromittierung von Zugangsdaten für die Fernwartung oder sonstige legitime Zugriffsmöglichkeiten Dritter.
- Die Manipulation in Zusammenhang mit Softwareänderungen (Updates, Patches).
- Die Manipulation von Konfigurationsdaten, Virensignaturen oder anderen von extern eingelesenen Datensätzen.
- Die Manipulation von Wartungs- und Analysewerkzeugen (Hardware/Software).

Die Phase „Disposal“ umfasst Prozesse bei Ausmusterung, Vernichtung, Wiederverwendung, sowie Analyseprozesse beispielsweise bei auftretenden Defekten. Die Angriffsmöglichkeiten für Cyberangriffe im Zusammenhang mit der Lieferkette umfassen dabei im Wesentlichen:

- Die Kompromittierung während oder nach der Entsorgung.
- Die Kompromittierung vor oder bei der Wiederverwendung.

- Die Manipulation der Deinstallation.
- Die Beschaffung von Informationen über ausgemusterte, fehlerhafte oder defekte Soft- und Hardwarekomponenten oder andere für die Entwicklung/Einbringung von Schadsoftware relevante Aspekte.

Im Rahmen von Cyberangriffen im Zusammenhang mit der Lieferkette können Angreifer potenziell auf jede Phase des Lebenszyklus abzielen, eine oder mehrere der oben genannten Angriffsmöglichkeiten einzelner oder mehrerer Phasen einsetzen und sind nicht auf einzelne Phasen oder Angriffsmöglichkeiten beschränkt. Zudem ist zu beachten, dass derartige Angriffe nicht auf ein Ziel und eine Ebene der Lieferkette beschränkt sein müssen, sondern dass beispielsweise auch der Zulieferer eines Zulieferers betroffen sein kann mit entsprechend weitreichenden Folgen für alle mit den betroffenen und direkt oder indirekt über mehrere Ebenen hinweg in Verbindung stehenden Unternehmen (siehe den IT-Sicherheitsvorfall im Zusammenhang mit 3CX (Abschnitt 3.2.9).

An welcher Stelle der Lieferkette bzw. in welchem Stadium der Softwareerstellung oder Fertigung der Hardware die Kompromittierung erfolgt, bringt sowohl für die Angreifer als auch die Angriffsziele unterschiedliche Herausforderungen mit sich. Generell sind die Herausforderungen sowohl bei der Ausführung eines Supply-Chain-Angriffs als auch bei dessen Detektion umso größer, je früher im Entwicklungsprozess bzw. Lebenszyklus der Angriff ansetzt. So ist beispielsweise aus Angreifersicht der Austausch eines auf einer Webseite zum Download bereitstehenden Updates durch eine manipulierte Version mit wesentlich einfacheren Mitteln zu realisieren als ein Eingriff in den Build-Prozess einer Software. Gleichzeitig stehen auf Seiten eines angegriffenen Unternehmens zumeist mehr Detektionsmöglichkeiten zur Verfügung, um ein im letzten Moment ausgetauschtes Update zu entdecken, als ein bereits im Build-Prozess manipuliertes Update zu identifizieren.

5.2 Gemeinsamkeiten und generische Aspekte der betrachteten IT-Sicherheitsvorfälle und abgeleitete Sicherungsmaßnahmen

Ausgehend von den in Abschnitt 3.1 und 3.2 analysierten IT-Sicherheitsvorfällen sowie den in Abschnitt 5.1 betrachteten Angriffsmöglichkeiten im Zusammenhang mit der Lieferkette in Abhängigkeit vom Lebenszyklus eines IT-Systems ergeben sich Gemeinsamkeiten und generische Aspekte, die im Folgenden kurz diskutiert werden. Generell zielt ein Cyberangriff im Zusammenhang mit der Lieferkette im Wesentlichen darauf ab, mit schwächeren Sicherungsmaßnahmen geschützte Glieder auszunutzen, um Zugang zu

sensiblen Daten zu erlangen, Zugriffsmöglichkeiten zu generieren oder Systeme und Netzwerke zu manipulieren. Insgesamt geht es typischerweise darum, anstelle des eigentlichen, typischerweise besser geschützten Angriffsziels ein schwächer geschütztes Glied in der Lieferkette anzugreifen und über diesen Umweg Zugang zum eigentlichen Angriffsziel zu erhalten. Dazu wird ein Vertrauensverhältnis zwischen verschiedenen Akteuren einer Lieferkette ausgenutzt, da sich Angreifer dadurch eine Umgehung von Sicherungsmaßnahmen bzw. leichter zu realisierende Zugriffsmöglichkeiten erhoffen. Zudem erreichen Angreifer mit einem erfolgreichen Angriff auf einen Akteur der Lieferkette oftmals einen Kaskadeneffekt, sodass verschiedene weitere Akteure betroffen sind, die mit dem ursprünglichen Angriffsziel nicht direkt, sondern über ein Zwischenziel in Verbindung stehen. Dies kann sowohl gezielt als auch ungezielt erfolgen. Generell erschwert die Komplexität der Lieferkette die Sicherstellung der Cybersicherheit für die Opfer dahingehend, dass einerseits gewisse Aspekte wie beispielsweise die Verwendung oder Einbindung etablierter oder externer Softwarekomponenten teilweise nicht in seinem Einwirkungsbereich liegen und andererseits der Aufwand für entsprechende Informationsbeschaffung über Kompromittierungen und Schwachstellen entsprechend steigt. Ein besonders lohnendes Ziel für Angreifer stellen in diesem Zusammenhang beispielsweise IT-Dienstleister dar, da diese in der Regel spezialisierte Werkzeuge einsetzen, Zugriff auf mehrere potenzielle Opfer ermöglichen und die in Anspruch genommenen Dienstleistungen in diesem Bereich vermehrt im Management- oder Sicherheitsbereich liegen, wodurch Angreifern entsprechende Zugriffsmöglichkeiten zur Verfügung stehen. Daneben dürfen gezielte Angriffe auf die Lieferkette einzelner Unternehmen nicht vernachlässigt werden, da auch derartige IT-Sicherheitsvorfälle zunehmen und gleichermaßen schwerwiegende bzw. auch gravierendere Auswirkungen haben können, insbesondere wenn es sich um technisch versierte und hoch spezialisierte Angreifer handelt, die ggf. auch von staatlichen Akteuren unterstützt werden.

Angreifer nutzen die Lieferkette von IT-Systemen oftmals, um den initialen Zugriff auf ihr eigentliches Ziel oder mehrere untergeordnete Ziele zu erlangen. Dabei gibt es eine Vielzahl unterschiedlicher Möglichkeiten, wie die Angreifer den initialen Zugriff auf das erste Ziel der Lieferkette erlangen können. Beispielsweise können Angreifer über einen weiteren Zulieferer diesen initialen Zugriff erlangen, sodass es sich um einen Angriff über die Lieferkette eines weiteren Zulieferers handelt. Ein bedeutendes Einfallstor für Angreifer stellen in diesem Zusammenhang zudem Softwareschwachstellen dar. Dabei können von Angreifern sowohl Schwachstellen in einer vom Ziel verwendeten Software als auch in Drittanbieter-Software oder externen Softwarebestandteilen ausgenutzt werden. Insbesondere von Zero-Day-Schwachstellen, für die zum Zeitpunkt des Angriffs

noch keine Patches oder sonstige Maßnahmen verfügbar sind, geht in diesem Zusammenhang ein enormes Bedrohungspotenzial aus. Ein weiteres weit verbreitetes Einfallstor stellen Social-Engineering-Techniken dar, bei denen Angreifer Mitarbeiter von Zielen oder Lieferanten dazu bringen wollen, sensible Informationen preiszugeben oder mit Schadsoftware behaftete Dateien auszuführen. Nach Erlangung des initialen Zugriffs stehen den Angreifern dann je nach den genauen Umständen weitere mögliche Angriffsschritte offen. Diese sind abhängig von den jeweiligen kompromittierten Systemen und Netzwerken sowie von den etablierten Sicherungsmaßnahmen. Die in Abschnitt 3.1 und 3.2 betrachteten IT-Sicherheitsvorfälle wurden bezüglich der für die jeweiligen Vorfälle relevanten Sicherungsmaßnahmen analysiert. Dabei wurden sowohl konkrete Maßnahmen betrachtet, die angesichts der IT-Sicherheitsvorfälle ergriffen wurden, wie auch generische Maßnahmen, die in den jeweiligen Fällen weitere Angriffsschritte der Angreifer erschwert, verhindert oder aufgedeckt hätten. Die Maßnahmen wurden entsprechend inhaltlicher Überschneidungen und Gemeinsamkeiten in übergeordneten Kategorien zusammengefasst, die im Folgenden diskutiert werden. Dabei ist zu beachten, dass prinzipiell jede Sicherheitsmaßnahme zur Verhinderung oder Erschwerung von Cyberangriffen generell und speziell im Zusammenhang mit der Lieferkette beitragen kann. Einzelne Maßnahmen sind somit im Rahmen eines umfassenden Cybersicherheitskonzepts nicht isoliert zu betrachten. Die im Rahmen des Vorhabens gewählte Gruppierung dient dabei somit zur Beleuchtung und Diskussion verschiedener Aspekte und zur Analyse von Sicherungsmaßnahmen, die einem bestimmten Schwerpunkt zur Erreichung eines angemessenen Cybersicherheitsniveaus zugeordnet werden. Dies ist insbesondere für den Vergleich mit den im Regelwerk vorgesehenen Maßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette (siehe Kapitel 4) hilfreich, sowie in Vorbereitung der Diskussion der Eignung und Wirksamkeit von Sicherungsmaßnahmen zur Verhinderung, Detektion und Mitigation von IT-Angriffen im Zusammenhang mit der Lieferkette (siehe Abschnitt 5.1).

Die folgenden übergeordneten Gruppen von Sicherungsmaßnahmen wurden identifiziert:

- Maßnahmen zur Echtzeitüberwachung und Detektion
- Reaktive Sicherungsmaßnahmen und Forensik
- Update- und Patchmanagement
- Überprüfung von Code auf Schadsoftware
- Grundlegende Sicherungsmaßnahmen

Dabei sind Maßnahmen zur Echtzeitüberwachung des Datenverkehrs von Netzwerken und somit zur Detektion auffälligen Datenverkehrs oder auffälliger Aktivitäten von elementarer Bedeutung, um Kompromittierungen und Angriffe rechtzeitig zu erkennen und Maßnahmen einzuleiten. In der Mehrzahl der betrachteten IT-Sicherheitsvorfälle waren derartige Maßnahmen hinsichtlich der durch die Angreifer ausgeführten Handlungen relevant und haben entsprechende Reaktionsmaßnahmen ermöglicht bzw. könnten zur rechtzeitigen oder frühen Erkennung beitragen, wenn die technische Realisierung hinreichend fortgeschritten und implementiert ist. Bei diesem Punkt geht es somit nicht um eine präventive Maßnahme zur Verhinderung eines Angriffs, sondern um eine möglichst frühzeitige Erkennung, die eine Eindämmung und weitere Reaktionsmaßnahmen ermöglicht. Das zentrale Ziel ist dabei, Angriffshandlungen zu erkennen, bevor die Angreifer ihr Ziel vollständig oder teilweise erreicht haben und somit einerseits bisher nicht betroffene Bereiche zu schützen und die Auswirkungen auf die betroffenen Bereiche zu minimieren.

Im Rahmen der betrachteten IT-Sicherheitsvorfälle wiesen reaktive Sicherungsmaßnahmen und der Aspekt der Forensik eine hohe Relevanz auf. Dazu zählen unter anderem die frühzeitige Einschaltung oftmals externer, auf den Umgang mit IT-Angriffen spezialisierter Unternehmen sowie von Behörden. Dies dient unter anderem der Sicherstellung von Spuren der Angreifer im Netzwerk zur Identifikation betroffener Bereiche sowie des Infektionspfades, wie auch zur Einleitung von Wiederherstellungsmaßnahmen zur Wiederaufnahme des Betriebs der Systeme. Dazu gehören beispielsweise das Entfernen von Schadsoftware, die Daten- bzw. Systemwiederherstellung und Durchführung von Funktionstests. Derartige Maßnahmen dienen ebenso wenig wie Maßnahmen zur Detektion und Echtzeitüberwachung zur Prävention von Angriffen, haben beim Umgang mit den Auswirkungen von Cyberangriffen jedoch ein hohes Maß an Bedeutung.

Die dritte Gruppe von besonders relevanten Sicherungsmaßnahmen hinsichtlich der betrachteten IT-Sicherheitsvorfälle umfasst die Themen Patches und Updates. Patches sind dabei im Wesentlichen auf die Korrektur von Software-Fehlern und die Schließung von Sicherheitslücken ausgelegt, wohingegen Updates diese Funktion auch ausfüllen können, jedoch oftmals umfangreichere Aktualisierungen beispielsweise zur Erweiterung des Funktionsumfangs einer Software oder Verbesserung der Performance umfassen. Eine regelmäßige Überprüfung der verwendeten Software auf Schwachstellen und diesbezüglich veröffentlichte Updates und Patches ist ein wichtiger Bestandteil, um Cyberangriffe im Zusammenhang mit der Lieferkette präventiv mit Sicherungsmaßnahmen zu begegnen. Schwachstellen stellen oftmals das Einfallstor dar, mit deren Ausnutzung

Angreifer initiale Zugriffsmöglichkeiten auf die Zielsysteme schaffen. Für Softwareschwachstellen sollte es somit ein umfangreiches Patch- und Updatemanagement geben, sodass verfügbare Patches und Updates möglichst zeitnah installiert oder ggf. Ersatzmaßnahmen ergriffen und dokumentiert werden.

Die Kompromittierung einer Software durch Angreifer kann möglicherweise durch eine Überprüfung des Codes auf Schadsoftwarekomponenten und -abschnitte erkannt werden. Maßnahmen diesbezüglich sind hinsichtlich einiger der betrachteten IT-Sicherheitsvorfälle relevant, jedoch sind diese in der Regel schwer zu realisieren. Zunächst können die jeweiligen Hersteller der Software prinzipiell bereits während der Entwicklung möglichst automatisiert den Code auf Manipulationen prüfen, die möglicherweise durch eine Kompromittierung des Systems durch Angreifer, die entsprechende Zugriffsmöglichkeiten haben, erfolgt sind. Da Softwareentwicklungen in der heutigen Zeit sehr umfangreich und komplex aufgebaut sind und oftmals auch externe Komponenten und Bestandteile besitzen, ist eine dauerhafte und vollständige Überprüfung nicht derartig umsetzbar, dass Kompromittierungen ausgeschlossen werden können. Für die Kunden sind Maßnahmen zur Überprüfung des Codes der eingesetzten Software zudem sehr schwer oder überhaupt nicht realisierbar, da die entsprechenden Fachkenntnisse für die jeweiligen Produkte in der Regel nur beim Hersteller selbst liegen und Informationen dazu beispielsweise nicht offengelegt werden. Zudem sind möglicherweise durch den Entwickler bereitgestellte Codeabschnitte bereits kompromittiert, wenn Angreifer den Entwicklungsprozess manipuliert haben, sodass dies für den Anwender nicht feststellbar ist.

Die letzte Gruppe umfasst grundlegende Sicherungsmaßnahmen, die im Bereich der Cybersicherheit standardmäßig etabliert sein sollten, dies aber häufig nicht in allen Bereichen sind oder die nicht vollständig oder sachgerecht angewendet werden. Dazu gehören unter anderem angemessene Passwortrichtlinien, Multi-Faktor-Authentifizierung, Zugangs- und Rechteverwaltung, Kryptografie, Backup-Management und angemessene Prozesse und Regelungen zum Einsatz von Wechseldatenträgern. Derartige Maßnahmen sind essenziell und liegen grundlegend im Verantwortungsbereich aller Unternehmen, Behörden und Betreiber kritischer Infrastrukturen im Rahmen eines grundlegenden Cybersicherheitskonzepts. In Bezug auf die Lieferkette sind solche Maßnahmen ebenso relevant, da eine angemessene Umsetzung Supply-Chain-Angriffe mindestens erschweren oder verlangsamen kann und den für die Angreifer erforderlichen Aufwand erhöht. Andererseits sind IT-Angriffe im Zusammenhang mit der Lieferkette dadurch gekennzeichnet, dass ein Großteil derartiger Sicherungsmaßnahmen umgangen werden kann. Insgesamt sind die grundlegenden Sicherungsmaßnahmen somit nicht zu

vernachlässigen, aber in Bezug auf die Verhinderung oder Mitigation von Cyberangriffen im Zusammenhang mit der Lieferkette üblicherweise nicht vollständig ausreichend.

5.3 Generische Angriffsmuster

Die sich im Rahmen der betrachteten IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette ergebenden Angriffsmöglichkeiten und Gemeinsamkeiten wurden zur Strukturierung und besseren Abgrenzung der IT-Angriffe bei der Diskussion der Eignung und Wirksamkeit entsprechender Sicherungsmaßnahmen in vier verschiedene Angriffsmuster aufgeteilt, die im Wesentlichen mit den unterschiedlichen Phasen des Lebenszyklus von IT-Systemen verknüpft sind bzw. die sich auf Abhängigkeiten und externe Komponenten beziehen. Diese Struktur der Einteilung ermöglicht es, die unterschiedlichen Phasen und Angriffsmöglichkeiten im Zusammenhang mit der Lieferkette zu identifizieren und die Sicherungsmaßnahmen gezielt hinsichtlich der verschiedenen Phasen und Umstände zu betrachten. Jedes Angriffsmuster beleuchtet damit spezifische Aspekte der Angriffsvektoren und deren potenziellen Auswirkungen sowie der Skalierbarkeit, Übertragbarkeit und Anforderungen an die Zugriffsmöglichkeiten, Fähigkeiten und Tatmittel der Angreifer. Die folgenden Angriffsmuster im Zusammenhang mit dem Lebenszyklus wurden definiert:

- **Upstream-Angriffe**, welche die Phasen Design, Development, Production und somit den Soft- und Hardwareentwicklungsprozess bis hin zum fertigen, getesteten Produkt/Release umfassen.
- **Midstream-Angriffe** umfassen die Phase der Distribution und beinhalten die Prozesse zur Verteilung, Auslieferung und Übertragung auf der Hersteller- bzw. Händlerseite.
- **Downstream-Angriffe**, welche die Phasen Acquisition, Deployment, Operation, Maintenance und Disposal umfassen und dabei alle Prozesse zur Beschaffung auf der Kundenseite, Integrations-, Installations- und Inbetriebnahme-Prozesse, Prozesse bei Betrieb und Wartung, Updates, Patches und Hardwareaustausch sowie Prozesse bezüglich der Ausmusterung, Vernichtung und Wiederverwendung beinhalten.

Darüber hinaus wurde ein Angriffsmuster im Zusammenhang mit Abhängigkeiten, externen Komponenten und Dienstleistungen definiert, welches für alle Phasen des Lebenszyklus relevant ist:

- **Angriffe im Zusammenhang mit Abhängigkeiten, externen Komponenten und Diensten**, wobei hierbei Schwachstellen, die sich aus der Einbeziehung von Softwarekomponenten oder Bibliotheken ergeben, die von externen Entwicklern oder Lieferanten bereitgestellt werden, sowie die Manipulation externer Softwarekomponenten, die vom eigentlichen Ziel des Angriffs verwendet werden, betrachtet werden.

Dabei ist zu beachten, dass die Einteilung nicht exklusiv zu verstehen ist und einzelne IT-Angriffe im Zusammenhang mit der Lieferkette durch mehrere Angriffsmuster charakterisiert sein können. Somit können gegebenenfalls verschiedene Aspekte eines IT-Angriffs jeweils einem oder mehreren Angriffsmustern zugeordnet werden. Der Sinn der Einteilung ist somit nicht eine Unterteilung der betrachteten und in den Abschnitten 3.1 und 3.2 vorgestellten IT-Sicherheitsvorfälle, sondern eine Kategorisierung der verschiedenen beobachteten und generischen Angriffsmöglichkeiten und Angriffsvektoren der potenziellen Angreifer. Dadurch können verschiedene für das Vorhaben relevante Aspekte und Fragestellungen, beispielsweise hinsichtlich der Anforderungen an die Täter, der potenziellen Auswirkungen und der Wirksamkeit von Sicherungsmaßnahmen, vergleichend diskutiert werden. Obwohl sich die Definition der vier Angriffsmuster im Wesentlichen aus den gewonnenen Erkenntnissen bei der Analyse der betrachteten IT-Sicherheitsvorfälle ergeben hat, sind die Angriffsmuster losgelöst von einzelnen IT-Sicherheitsvorfällen zu betrachten und können gegebenenfalls bei der Analyse einzelner Aspekte eines IT-Angriffs im Zusammenhang mit der Lieferkette herangezogen werden. Im Rahmen der nachfolgenden Diskussion der einzelnen Angriffsmuster werden neben der allgemeinen Beschreibung sowie Überlegungen bezüglich der Skalierbarkeit und Übertragbarkeit auch Anforderungen an Täter und Tatmittel und der potenziellen Auswirkungen entsprechend einzelne Beispiele aus den Abschnitten 3.1 und 3.2 zur Illustration des jeweiligen Angriffsmusters und zur Veranschaulichung des Bezugs zur aktuellen IT-Bedrohungslage aufgegriffen.

5.3.1 Upstream-Angriffe

Beschreibung

Upstream-Angriffe zielen auf die frühen Phasen des Lebenszyklus von Soft- und Hardware-Produkten (Design, Development, Production) ab. Dabei infiltrieren Angreifer die Lieferkette durch Manipulationen in diesen Phasen, um beispielsweise Schwachstellen oder Schadsoftwarekomponenten einzuschleusen, die später im weiteren Verlauf

schwer zu erkennen und zu entfernen sind, insbesondere durch den Anwender. Grundsätzlich sind Softwaremanipulationen in der Regel umso schwerer zu erkennen, je früher sie im Entwicklungsprozess vorgenommen wurden, wodurch eine Detektion unwahrscheinlicher wird. Allerdings setzt dies üblicherweise ein langfristiges, persistentes und fachkundiges Vorgehen der Angreifer voraus, abhängig von der Professionalität und der Sicherheitskompetenz der Entwickler bzw. Hersteller. Der Zugriff auf das Produkt durch die Angreifer und die erste Manipulation findet dabei beim Hersteller statt.

Skalierbarkeit, Übertragbarkeit und potenzielle Auswirkungen

Upstream-Angriffe sind hochgradig skalierbar, da eine einmal durchgeführte Manipulation beispielsweise durch vorgenommene Veränderungen, eine eingebrachte Schwachstelle oder eine eingeschleuste Schadsoftware in allen abgeleiteten Produkten vorhanden oder wirksam sein kann. Dies kann somit unter Umständen mehrere Produkte eines Herstellers – auch über einen längeren Zeitraum – umfassen, wenn beispielsweise die Entwicklungsumgebung oder der Build-Prozess kompromittiert ist. Die Übertragbarkeit ist ebenfalls hoch, da die manipulierten Komponenten in verschiedenen Produkten und Diensten verwendet werden können. Upstream-Angriffe können weitreichende Folgen haben, da die eingeschleusten Schwachstellen oder Schadsoftwarekomponenten bzw. die vorgenommenen Veränderungen unbemerkt in diversen Produkten oder Dienstleistungen integriert sein können. Die Detektion von Manipulationen bei derartigen Angriffen kann typischerweise sehr komplex oder durch den Anwender gar nicht möglich sein, sodass Angreifer, wenn dies ihre Strategie ist, gegebenenfalls über sehr lange Zeiträume unbemerkt agieren können, um beispielsweise Informationen zu stehlen bzw. generell bis zur Ausführung destruktiver oder disruptiver Handlungen unentdeckt zu bleiben. Dadurch ergibt sich insbesondere die besondere Problematik von Upstream-Angriffen, wenn für Anwender ein kompromittiertes Produkt nicht als solches zu erkennen ist und selbst der Hersteller dies nicht erkennt, sofern er die Kompromittierung des eigenen Systems nicht erkannt hat. Dies kann somit beim Einsatz schwerwiegende Konsequenzen haben und über den Verlust der Informationssicherheit (einschließlich Verlust der Verfügbarkeit, Vertraulichkeit und Integrität von Informationen) hinaus gegebenenfalls auch zu physischen Schäden führen. Die bisher beobachteten IT-Sicherheitsvorfälle in diesem Zusammenhang hatten im Wesentlichen langfristige Spionage und die unentdeckte Informationsbeschaffung zum Ziel.

Anforderungen an Täter und Tatmittel

Upstream-Angriffe erfordern ein hohes Maß an technischen Fähigkeiten und ein tiefes Wissen über den Entwicklungsprozess sowie Zugang zu den Entwicklungswerkzeugen und Umgebungen. Angreifer müssen dabei ein umfassendes Verständnis von Entwicklungsprozessen haben, um Schwachstellen in frühen Phasen der Entwicklung auszunutzen und zu ihren Gunsten einzusetzen. Dazu gehören unter anderem vertiefte Kenntnisse in Design und Programmierung von Softwarearchitekturen und in der Nutzung von Entwicklungswerkzeugen. Kompetenzen im Bereich der Entwicklung von Schadsoftware, die unentdeckt bleibt und effektiv ihre beabsichtigte Funktion erfüllt sind dabei essenziell. Dazu ist in der Regel umfangreiches Wissen über die Zielumgebung erforderlich, sodass Angreifer entsprechende Kenntnisse in Reverse-Engineering-Techniken oder analoge Aufklärungsfähigkeiten besitzen. Upstream-Angriffe erfordern typischerweise eine langfristige Planung und Koordination, da die Angriffe selbst oftmals lange vor der eigentlichen Nutzung der kompromittierten Software stattfinden. Dazu benötigen Angreifer zudem eine (persistente) Zugriffsmöglichkeit auf die Zielsysteme, beispielsweise durch kompromittierte Zugänge, Schwachstellen oder wissentlich bzw. unwissentlich agierende Innentäter. Derartig komplexe Angriffe erfordern entsprechende Ressourcen in materieller, finanzieller, personeller und organisatorischer Hinsicht, die typischerweise eine professionell organisierte APT-Gruppierung voraussetzt. Insgesamt erfordern Upstream-Angriffe in der Regel ein komplexes und umsichtiges Vorgehen hochqualifizierter Angreifer, wobei insbesondere auch Verschleierungstaktiken in Bezug auf die durchgeführten Angriffshandlungen zur Tarnung und Vermeidung der Entdeckung essenziell sind.

Upstream-Angriffe in Bezug auf Hardware-Komponenten erfordern Wissen der Täter zum Design und der Entwicklung des Produkts, sowie Fähigkeiten zur physischen Manipulation vor Ort beim Hersteller.

Beispiele

Ein typisches Beispiel eines Upstream-Angriffs ist die Kompromittierung von Entwicklungsumgebungen oder die Manipulation von Softwarebestandteilen, die für das Produkt essenziell und entsprechend tiefgreifend im Produkt verankert sind. Als wesentliches Beispiel ist hier der IT-Sicherheitsvorfall im Zusammenhang mit SolarWinds Orion Produkten aus dem Jahr 2020 zu nennen (siehe Abschnitt 3.2.2). Dabei kompromittierten Angreifer zunächst unbemerkt eine Reihe von Softwareversionen der SolarWinds

Software Orion im Rahmen des Build-Prozesses beim Hersteller, woraufhin die kompromittierte Software mit legitimen digitalen Signaturen ausgestattet und über die offiziellen Server vertrieben wurde. Da die Manipulation in diesen frühen Phasen des Lebenszyklus erfolgte und die Angreifer durch ihr geschicktes Vorgehen zunächst keine sichtbaren Spuren hinterließen, gab es für die Anwender keine Möglichkeit, eine Kompromittierung zu erkennen, sodass sich die Angreifer über einen langen Zeitraum über Monate hinweg unbemerkt in den Systemen der Opfer bewegen konnten. Ein ähnlicher IT-Sicherheitsvorfall wurde im April 2021 im Zusammenhang mit dem IT-Dienstleister Codecov aufgedeckt (siehe Abschnitt 3.2.6). In diesem Fall war es den Angreifern gelungen, Zugriff auf die Server des Bash Uploaders zu bekommen und sensible Kundendaten zu stehlen, sobald ein Kunde Daten von den kompromittierten Servern übertrug. Auch hier konnten die Angreifer durch ihr umsichtiges Vorgehen über Monate hinweg unentdeckt agieren.

5.3.2 Midstream-Angriffe

Beschreibung

Bei Midstream-Angriffen konzentrieren sich die Angreifer auf den Prozess der Auslieferung und Verteilung (Distribution), der zwischen der Erstellung/Herstellung bzw. Erzeugung beim Hersteller und der Anwendung beim Endnutzer liegt. Dabei versuchen die Angreifer, die Integrität der Lieferung zu beeinträchtigen, indem sie beispielsweise Hardware oder Software während des physischen oder digitalen Transports manipulieren. Diese Art von Angriffen kann entsprechend durch logistische bzw. physische oder digitale Manipulationen erfolgen. Hardware (bzw. Software auf mobilen Datenträgern) kann beispielsweise bei der Auslieferung abgefangen und manipuliert oder ausgetauscht werden, wohingegen Software typischerweise über digitale Kanäle verteilt wird, wobei beispielsweise die Website zur Bereitstellung manipuliert sein kann. Da das Produkt erst nach Fertigstellung durch den Hersteller manipuliert bzw. ausgetauscht wird, gibt es im Gegensatz zu Upstream-Angriffen bei Midstream-Angriffen für Anwender bzw. gegebenenfalls den Hersteller selbst prinzipiell die Möglichkeit, die Integrität zu überprüfen und Manipulationen zu erkennen. Der Zugriff auf das Produkt durch die Angreifer und die erste Manipulation findet beim Übergang zwischen Hersteller und Anwender statt.

Skalierbarkeit, Übertragbarkeit und potenzielle Auswirkungen

Bei Midstream-Angriffen ergibt sich eine ähnliche Skalierbarkeit wie bei Upstream-Angriffen. Generell haben Midstream-Angriffe im Zusammenhang mit der Lieferkette eine

hohe Verbreitung. Einerseits ist der Aufwand für derartige Angriffe für Angreifer hinsichtlich der Persistenz, Komplexität und Fachkunde verglichen mit Upstream-Angriffen in der Regel nicht so hoch, da keine unbemerkte Manipulation des Entwicklungsprozesses erforderlich ist. Andererseits umgehen die Angreifer durch die Manipulation des Produktes, bevor es beim Anwender ankommt, potenziell dessen Sicherungsmaßnahmen, sodass die Manipulation zunächst typischerweise unabhängig von einzelnen Zielen implementiert werden kann und möglicherweise für mehrere Ziele anwendbar ist. Dadurch ergeben sich weitreichende Konsequenzen, da Angreifer durch derartige Angriffe potenziell eine Vielzahl möglicher Ziele erreichen, die beispielsweise eine kompromittierte Softwareversion herunterladen und einsetzen. Die potenziellen Auswirkungen können zudem die Sicherheit und Funktionalität der Produkte erheblich beeinträchtigen und zu direkten Schäden führen, beispielsweise indem kompromittierte Hardware eingesetzt wird. Insgesamt sind Midstream-Angriffe weit verbreitet und stellen in diesem Zusammenhang häufig den ersten Schritt der Angreifer zur Erlangung des initialen Zugriffs auf die Netzwerke ihrer Opfer dar. Darauffolgend können weitere Angriffsschritte beispielsweise zur Informationsbeschaffung oder Manipulation bzw. Störung von Systemen ausgeführt werden.

Anforderungen an Täter und Tatmittel

Die Anforderungen an die Täter und Tatmittel bei Midstream-Angriffen setzen zunächst generell wie bei den anderen Angriffsmustern umfangreiche Kenntnisse in der Manipulation von Software voraus, sodass diese im besten Fall für die Angreifer zunächst nicht erkannt wird. Dies erfordert tiefgehende Kenntnisse in der Software-Entwicklung und ggf. Reverse-Engineering für die unerkannte Manipulation von Software-Releases nach der Entwicklung. Dabei kommen bei Midstream-Angriffen erforderliche Kenntnisse bzgl. der Übertragung von Software und dabei möglicherweise vorhandener Schwachstellen hinzu. In diesem Zusammenhang sind für Angreifer insbesondere digitale Signaturen und Integritätsprüfungen relevant, da die heutige Softwareverteilung typischerweise durch derartige Mechanismen geschützt ist und Angreifer entsprechend Schritte zur Umgehung oder Fälschung beherrschen müssen. Dabei erfordern Midstream-Angriffe oftmals eine koordinierte Vorgehensweise, insbesondere wenn mehrere Schritte und Akteure involviert sind und es um logistische Planungen und zeitkritische Aktionen innerhalb eines Angriffs geht. In diesem Zusammenhang profitieren Angreifer möglicherweise von Insider-Handlungen eines bewusst oder unbewusst agierenden Innentäters, sodass Angreifer mit entsprechenden Kapazitäten zur Rekrutierung, Kompromittierung oder Ausnutzung von Mitarbeitern des Ziels oft über die notwendigen technischen,

organisatorischen und finanziellen Ressourcen verfügen. Zuletzt sind auch Verschleierungstaktiken in Bezug auf die durchgeführten Angriffshandlungen ein relevanter Faktor für Angreifer, um durch den Einsatz von Anonymisierungstechniken, verschlüsselten Kommunikationskanälen und anderen Methoden zur Tarnung ihre Spuren zu verwischen und die Entdeckung zu vermeiden. Hinter den beobachteten IT-Sicherheitsvorfällen, die im Zusammenhang mit Midstream-Angriffen zu nennen sind, stehen oftmals gut organisierte und ausgestattete APT-Gruppierungen mit den entsprechenden Ressourcen, die aus kommerziellen, politischen oder anderen Interessen handeln und geschäftsmäßig agieren. Dabei sind die Komplexität der Angriffe und die Anforderungen an die Täter und Tatmittel typischerweise im direkten Vergleich zu Upstream-Angriffen geringer einzuschätzen, da Midstream-Angriffe in der Regel leichter für Angreifer durchzuführen sind.

Midstream-Angriffe in Bezug auf Hardware-Komponenten erfordern Wissen der Täter zur Verteilung und Auslieferung des Produkts, beispielsweise hinsichtlich er Logistik und der verwendeten Kanäle. Hierbei sind gegebenenfalls Fähigkeiten zur physischen Manipulation von Lieferungen erforderlich. Zugriffsmöglichkeiten ergeben sich für die Angreifer einerseits physisch durch den Zugriff auf Lieferwege oder Logistikzentren und andererseits logisch durch den Zugriff auf die an der Verteilung beteiligten Infrastruktur.

Beispiele

Ein typisches Beispiel eines Midstream-Angriffs ist die Manipulation legitimer Softwarereleases durch Angreifer, wobei beispielsweise die Downloadseite manipuliert wurde und die Angriffsziele die Schadsoftware bzw. kompromittierte Software selbst aktiv herunterladen. Hierfür gibt es zahlreiche Beispiele von IT-Sicherheitsvorfällen, die in der Vergangenheit beobachtet wurden. In diesem Zusammenhang ist insbesondere der IT-Sicherheitsvorfall NotPetya (siehe Abschnitt 3.1.4) zu nennen, der weltweit schwerwiegenden Auswirkungen hatte. Im Frühjahr 2017 erlangten Angreifer dabei Zugriff auf Systeme des Unternehmens Linkos Group und kompromittierten Updateserver, wobei sie eine Backdoor zur Verteilung der Schadsoftware NotPetya in offizielle Updates der Software M.E.Doc injizierten. Die schadhaften Updates wurden dann von den Angreifern auf den Updateservern von M.E.Doc für Kunden zum Download bereitgestellt. Die Angreifer kompromittierten mit Hilfe der installierten Backdoor alle betroffene Systemen, welche das schadsoftwarebehaftete Update heruntergeladen hatten, mit der Schadsoftware NotPetya. Ein ähnlicher IT-Sicherheitsvorfall ereignete sich im Juli 2021. Dabei wurden weltweit Updateserver eines Remote-Monitoring und -Management-Tools des amerikanischen IT-Dienstleisters Kaseya manipuliert (siehe Abschnitt 3.2.5). Die

Angreifer nutzten mehrere Sicherheitslücken und Zero-Day-Exploits aus, um die Server zu manipulieren und so ein schadsoftwarebehaftetes Update zu platzieren, welches entsprechend an die Systeme der Nutzer verteilt wurde. Von den Angriffen waren über 1000 Firmen betroffen, darunter auch Unternehmen, die selbst keinen direkten Bezug zu Kaseya haben, sondern deren IT-Dienstleister oder Zulieferer die Software nutzten. Ein Beispiel für die große Anzahl potenziell von einem Midstream-Angriff betroffener Systeme stellt der IT-Sicherheitsvorfall im Zusammenhang mit der Software CCleaner dar (siehe Abschnitt 3.1.10). Als Angreifer im Jahr 2017 Zugriff auf die IT-Systeme des Herstellers Piriform erlangten und die kostenlose Software mit einer kompromittierten Version ersetzten gelangte die mitgelieferte Schadsoftware auf Systeme von über 2 Millionen Nutzern.

5.3.3 Downstream-Angriffe

Beschreibung

Downstream-Angriffe sind auf die späteren Phasen des Lebenszyklus (Acquisiton, Deployment, Operation, Maintenance, Disposal) ausgerichtet. Angreifer nutzen diese Phasen dazu, Schwachstellen auszunutzen, die während der Beschaffung und Implementierung durch den Kunden, sowie während des Einsatzes, der Wartung und der Entsorgung des Produktes entstehen. Dies umfasst zunächst im Wesentlichen alle Prozesse im Zusammenhang der Integration, Installation und Inbetriebnahme von Komponenten und Systemen, beispielsweise im Rahmen von Neuanschaffungen oder Hard- und Softwareänderungen. In diesem Zusammenhang spielen Updates und Patches eine wesentliche Rolle. Dabei ist zu beachten, dass Updates und Patches selbst einem Lebenszyklus unterworfen sind und die entsprechenden Phasen wie beispielsweise Design, Development und Distribution durchlaufen. Updates und Patches können in diesen Phasen gezielt von Angreifern manipuliert werden oder Angreifer nutzen die Ausführung des Vorgangs, um weitere Angriffshandlungen durchzuführen. Zudem fällt die Ausnutzung von Schwachstellen in ungepatchten Systemen in dieses Muster. Ein weiterer wichtiger Aspekt im Zusammenhang mit Downstream-Angriffen stellen Remote-Zugänge und -Zugriffe dar, die von Angreifern ausgenutzt werden können. Zudem Umfassen Downstream-Angriffe alle Manipulationen und Angriffsschritte im Zusammenhang mit der Außerbetriebnahme, Entsorgung und Zerstörung von Komponenten und Systemen. Der Zugriff auf das Produkt durch die Angreifer und die eigentliche Manipulation findet beim Anwender statt.

Skalierbarkeit, Übertragbarkeit und potenzielle Auswirkungen

Die Skalierbarkeit derartiger Angriffe ist im Vergleich zu Upstream- oder Midstream-Angriffen allgemein geringer, da Angriffe oftmals gezielt auf spezifische Systeme, Schwachstellen oder Konfigurationen ausgerichtet sind und daher ohne Anpassungen oft bei nur einem einzelnen Angriffsziel (d. h. einer Anlage, Organisation oder Einrichtung) durchführbar sind. Die Übertragbarkeit hängt dabei von der gemeinsamen Nutzung von Systemen und Konfigurationen ab. Da Downstream-Angriffe primär auf die Phasen des Lebenszyklus abzielen, die einen größeren Bezug zu den letztlichen Anwendern haben, ergibt sich die Bedrohung primär für diese konkreten Ziele, wohingegen sich bei Upstream- und Midstream-Angriffen für Angreifer potenziell eine größere Anzahl möglicher Ziele ergibt. Die Auswirkungen von Downstream-Angriffen können erheblich sein, da sie direkt auf betriebliche Systeme abzielen können, was zu Betriebsstörungen, Datenverlust oder -Diebstahl führen kann. Obwohl Angreifern oftmals die Kompromittierung der Lieferkette als erster Schritt zur Erlangung von Zugriffsmöglichkeiten bei ihren Zielen dient, ist insbesondere im Rahmen von Downstream-Angriffen denkbar, dass der Fokus der Angreifer bei der direkten Manipulation betrieblicher oder sicherheits- und sicherungsrelevanter Systeme liegt. Da die Handlungen der Angreifer im Vergleich zu Upstream- und Midstream-Angriffen eher auf den Anwender bzw. den eigentlichen Einsatz der Systeme bezogen sind liegt es bei Downstream-Angriffen gegebenenfalls mehr im Einflussgebiet des Anwenders, Angriffe bzw. Angriffshandlungen im Zusammenhang mit der Lieferkette zu erkennen und anschließend weitere Sicherungsmaßnahmen zu ergreifen.

Anforderungen an Täter und Tatmittel

Generell erfordern Downstream-Angriffe fortgeschrittene technische Fähigkeiten der Angreifer in Bezug auf die jeweiligen, sich in Verwendung befindlichen Systeme und Komponenten. Dabei sind insbesondere Kenntnisse und Fähigkeiten in der Schadsoftware- und Exploit-Entwicklung relevant, um bekannte oder unbekannte Schwachstellen in Software und Systemen auszunutzen und für maßgeschneiderte Angriffe einzusetzen. Es ist dabei erforderlich, diese dabei gezielt auf die Zielumgebung zuzuschneiden, sodass die dort genutzten Systeme entsprechend für die Ausführung der Angriffsschritte ausgenutzt werden können. Generell sind somit zunächst nähere Kenntnisse der Angreifer über das Ziel und die dortigen Systeme und gegebenenfalls Sicherungsmaßnahmen essenziell bei der Durchführung von Downstream-Angriffen. Dies umfasst zudem in der Regel das Verständnis von Betriebs- und Wartungsprozessen, beispielsweise zur Auswahl

geeigneter Zeitpunkte der Angriffshandlungen und der geeigneten Werkzeuge. Dabei ermöglicht potenzielles Insider-Wissen, das die Angreifer beispielsweise durch wissentlich oder unwissentlich agierende Innentäter erlangt haben, ein gezielteres Vorgehen, beispielsweise hinsichtlich spezifischer Systemkonfigurationen oder Einstellungen. Da auch Downstream-Angriffe typischerweise mehrere aufeinander aufbauende und voneinander abhängige Angriffsschritte umfassen, ist eine koordinierte Vorgehensweise gegebenenfalls über mehrere Phasen und Akteure hinweg erforderlich. Dazu sind entsprechende finanzielle und organisatorische Ressourcen erforderlich, mit denen derartige Operationen finanziert werden. Obwohl Downstream-Angriffe in der Regel direkte Handlungen der Angreifer beim Angriffsziel beispielsweise in Form von Störungen betrieblicher Abläufe oder Informationsdiebstahl ermöglichen, sind auch in diesem Fall Verschleierungstechniken oftmals relevant für die Angreifer, um ihre Aktivitäten und Identitäten zu verschleiern und die Entdeckung und Verfolgung zu vermeiden.

In Bezug auf Hardware-Komponenten erfordern Downstream-Angriffe Wissen der Täter hauptsächlich zum operativen Betrieb und zur Wartung der Systeme, sowie zu Vorgehensweisen und Prozessen hinsichtlich der Außerbetriebnahme und Entsorgung. Die Zugriffe erfolgen dabei vor Ort bei den Anwendern bzw. bei Dienstleistern. Dazu sind entsprechende physische Zugriffsmöglichkeiten der Angreifer erforderlich.

Beispiele

Ein typisches Beispiel eines Downstream-Angriffs stellt die Kompromittierung durch legitime Fernwartungszugänge externer Unternehmen dar. Hierbei ist zunächst beispielshaft der IT-Angriff auf das Unternehmen Target zu nennen, bei dem Angreifer legitime Zugangsdaten eines externen Dienstleisters, die sie sich über vorbereitende Angriffsschritte verschafft hatten, ausnutzten, um Zugriff auf die Netzwerke von Target zu erhalten (siehe Abschnitt 3.1.6). Daraufhin konnten sie mit Hilfe von eingebrachter Schadsoftware sensible Zahlungsdaten von über 100 Millionen Kunden des Unternehmens abgreifen. Ein weiteres Beispiel stellen die Angriffe der APT-Gruppierung Dragonfly auf kritische Infrastrukturen dar, die im Zusammenhang mit kompromittierten VPN-Zugängen stehen (siehe Abschnitt 3.1.5). Dabei verschafften sich die Angreifer unter anderem über Credential Harvesting Zugriff auf die Netzwerke von Zwischenzielen in der Lieferkette. Ausgehend von der Kompromittierung eines Zwischenziels nutzte Dragonfly legitime VPN-Zugänge aus, um das eigentlich anvisierte Ziel zu kompromittieren und beispielsweise mit Hilfe von Schadsoftware Backdoors zu etablieren. In beiden Fällen nutzten Angreifer somit legitime Fernzugriffsmöglichkeiten zur Kompromittierung der

Zielnetzwerke aus, die im Rahmen der Zusammenarbeit mit externen Unternehmen von den Zielen selbst eingerichtet wurden.

5.3.4 Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten

Beschreibung

Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten setzen auf die Ausnutzung Schwachstellen, die sich aus der Einbeziehung von Softwarekomponenten oder Bibliotheken ergeben, die von externen Entwicklern oder Lieferanten bereitgestellt werden und außerhalb des direkten Einflussbereichs des Anwenders liegen. Dabei geht es beispielsweise um die Manipulation externer Softwarekomponenten, die vom eigentlichen Ziel des Angriffs verwendet werden, um einen Zugang zum Netzwerk und den Systemen des Opfers zu schaffen. Abhängigkeiten und externe Komponenten und Dienste können für alle Phasen des Lebenszyklus relevant sein und sowohl eigenständig für Angriffe genutzt werden wie auch zur Vorbereitung von Angriffen, beispielsweise im Rahmen eines Upstream-Angriffs. Der Zugriff auf das Produkt durch die Angreifer und die eigentliche Manipulation findet dabei typischerweise außerhalb des Einflussbereichs des Anwenders direkt auf die externen Komponenten und Abhängigkeiten statt.

Skalierbarkeit, Übertragbarkeit und potenzielle Auswirkungen

Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten sind hochgradig skalierbar, da eine Schwachstelle in einer weit verbreiteten Komponente viele Systeme betreffen kann, insbesondere wenn sie global genutzt wird und viele Anwendungsbereiche hat. Daraus ergibt sich ebenfalls eine hohe Übertragbarkeit, da dieselben Komponenten oft in unterschiedlichen Kontexten genutzt werden. Derartige Angriffe können entsprechend weitreichende Auswirkungen haben, da kompromittierte Drittanbieterkomponenten oder -Dienste in vielen unterschiedlichen Produkten und Systemen verwendet werden können, was zu einer Vielzahl gleichzeitig betroffener Systeme führen kann. Dadurch, dass externe Bibliotheken und Pakete typischerweise nicht auf einzelne Hersteller beschränkt sind und prinzipiell von jedem genutzt werden können, verstärkt sich im Vergleich zu den anderen Angriffsmustern die Problematik einer potenziellen Kompromittierung, die im Wesentlichen in der weiten Verbreitung begründet ist. Aber auch die potenziellen Auswirkungen von Kompromittierungen weniger breitflächig genutzter externer Komponenten können im Einzelfall schwerwiegende potenzielle

Auswirkungen haben. Die Detektion von Manipulationen bei derartigen Angriffen kann ähnlich zu Upstream-Angriffen und darüberhinausgehend sehr komplex sein, da häufig auch die Hersteller/Lieferanten nicht alle Abhängigkeiten und Zusammenhänge vollumfänglich im Detail durchblicken. Die Problematik potenzieller Auswirkungen bei Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten wird dadurch weiter erhöht.

Anforderungen an Täter und Tatmittel

Angreifer benötigen für Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten einschlägige Kenntnisse, insbesondere in Bezug auf die typische Architektur, Schwachstellen und die Einbindung und Integration in die jeweiligen Systeme. Dabei sind insbesondere Kenntnisse und Fähigkeiten in der Schadsoftware- und Exploit-Entwicklung relevant, um externe Komponenten entsprechend zu manipulieren, da der Zugriff in der Regel durch die Ausnutzung von Schwachstellen in Drittanbieter-Komponenten oder durch die Kompromittierung von externen Anbietern erfolgt. Für diese Art von Angriffen sind insbesondere Kenntnisse über eingebundene Komponenten und Abhängigkeiten innerhalb der Zielumgebung erforderlich, um die Angriffe entsprechend vorbereiten und durchführen zu können. Dabei ist in der Regel ein hohes Maß an Koordination erforderlich, da Angriffe in diesem Zusammenhang oftmals über mehrere Schritte und Stufen sowie gegebenenfalls über mehrere beteiligte Organisationen hinweg ausgeführt werden und die zeitliche Abstimmung typischerweise ein kritischer Faktor ist. Je nachdem welche externen Komponenten und Dienste betroffen und wie weit verbreitet diese sind, setzen Angreifer möglicherweise bewusst oder unbewusst agierende Innentäter ein oder versuchen Beteiligte zu kompromittieren, um Zugang zu kritischen Informationen oder Systemen zu erhalten. Dazu sind je nach genauen Umständen entsprechende finanzielle, materielle und zeitliche Ressourcen erforderlich, die entsprechend mit steigender Komplexität der Angriffe zunehmen. Auch bei Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten sind Verschleierungstechniken oftmals relevant für die Angreifer, um ihre Aktivitäten und Identitäten zu verschleiern und die Entdeckung und Verfolgung zu vermeiden.

Beispiele

Ein typisches Beispiel eines Angriffs im Zusammenhang mit Abhängigkeiten und externen Komponenten stellt die Kompromittierung von (frei verfügbaren) Bibliotheken dar. Ein bedeutendes Beispiel für einen derartigen Fall stellt der IT-Sicherheitsvorfall im

Zusammenhang mit Log4J dar, wobei es sich hierbei zunächst nicht um einen zielgerichteten Angriff, sondern um eine kritische Schwachstelle handelte, die für weitreichende Angriffe ausgenutzt werden konnte (siehe Abschnitt 3.2.4). Im Wesentlichen geht es dabei um eine Schwachstelle in einer weit verbreiteten Programmierbibliothek innerhalb der Programmiersprache Java, die erweiterte Funktionen bietet und deshalb vielfach eingebunden und weit verbreitet ist, sowohl im Open-Source-Bereich wie auch in kommerziellen Produkten. Die Ausnutzung der Schwachstelle ermöglichte Angreifern potenziell Zugriff auf unzählige verwundbare Systeme aus verschiedenen Bereichen von regulärer Büro-IT bis hin zu industriellen Steuerungssystemen. Ein weiteres Beispiel stellen Manipulationen frei verfügbarer Softwarepakete in öffentlich zugänglichen Archiven dar (siehe Abschnitt 3.2.7). In einem Fall modifizierten Angreifer legitime Pakete des NPM-Repositories mit der Absicht, dass diese von Anwendern heruntergeladen werden und Angreifern Zugriffe auf die betroffenen Systeme und weitere Angriffsschritte ermöglichen. In beiden Fällen geht es somit darum, dass Anwender externe Komponenten (in diesen Fällen Bibliotheken oder Software-Pakete) einbinden und durch die Kompromittierung dieser durch die Angreifer verwundbar werden.

5.4 Eignung und Wirksamkeit von Sicherungsmaßnahmen zur Verhinderung, Detektion und Mitigation von IT-Angriffen im Zusammenhang mit der Lieferkette

Eine zentrale Fragestellung, die im Rahmen des Vorhabens adressiert wurde, betrifft die Eignung und Wirksamkeit von Sicherungsmaßnahmen zur Verhinderung, Detektion und Mitigation von IT-Angriffen im Zusammenhang mit der Lieferkette. Dabei geht es um Sicherungsmaßnahmen, die vom Betreiber umgesetzt werden können und somit in seinem Einflussbereich liegen. Naturgemäß ist dies vor allem bei den späteren Phasen des Lebenszyklus eines Produkts der Fall, in denen es sich beim Anwender befindet. Die Sicherungsmaßnahmen, die bei den unterschiedlichen Zulieferern oder Beteiligten innerhalb der Lieferkette umgesetzt sind, liegen grundsätzlich nicht im direkten Einflussbereich eines Betreibers und werden somit für die weiteren Betrachtungen nicht berücksichtigt. Eine Ausnahme stellen hier Maßnahmen durch Zusicherungen dar, die der Betreiber durch entsprechende vertragliche Regelungen festschreiben und einfordern kann. Diese können beispielsweise Informationen über IT-Sicherheitsvorfälle oder etablierte Sicherungsmaßnahmen umfassen. Allgemein gibt es verschiedene Herangehensweisen und Ansätze, um im Rahmen von präventiven oder reaktiven Maßnahmen bzw. Maßnahmen zur Detektion, ein angemessenes Niveau der IT-Sicherheit in Bezug auf die Lieferkette zu gewährleisten. Dabei kommt es typischerweise nicht auf eine einzelne

isolierte Maßnahme oder Vorgehensweise an, sondern auf das Zusammenspiel mehrerer unterschiedlicher Sicherungsmaßnahmen. Die Auswertung unterschiedlicher IT-Sicherheitsvorfälle im Zusammenhang mit der Lieferkette (siehe Kapitel 3) hat gezeigt, dass in Bezug auf die unterschiedlichen IT-Sicherheitsvorfälle teilweise unterschiedliche Sicherungsmaßnahmen entscheidend sind. Im Wesentlichen lässt sich jedoch sagen, dass die jeweilige Realisierung umfangreicher Sicherungsmaßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette eine hohe Relevanz hat. Im Folgenden werden entsprechende Sicherungsmaßnahmen in Form der in Abschnitt 5.2 eingeführten Kategorien hinsichtlich der Eignung und Wirksamkeit in Bezug auf die in Abschnitt 5.1 vorgestellten generischen Angriffsmustern diskutiert.

5.4.1 Grundlegende Sicherungsmaßnahmen

Grundlegende Sicherungsmaßnahmen stellen allgemein das Fundament aller Bemühungen zur Sicherstellung der IT-Sicherheit dar, nicht nur in Bezug auf die Lieferkette, sondern hinsichtlich aller mit der IT-Sicherheit verbundenen Aspekte. In Bezug auf die Lieferkette sind solche Maßnahmen generell relevant, da eine angemessene Umsetzung derartige Angriffe erschweren oder verlangsamen können und den für die Angreifer erforderlichen Aufwand erhöhen. Dies trifft im Allgemeinen auf jedes der erläuterten Angriffsmuster zu.

Bei Upstream-Angriffen setzen die Angreifer auf bereits im Herstellungs- bzw. Entwicklungsprozess manipulierte und kompromittierte Systeme, die in der Regel für den Anwender nicht als solche zu erkennen sind. Möglicherweise kompromittierte Funktionen einer Software können somit beispielsweise für den Anwender nicht verdächtig erscheinen, sodass auch grundlegende Sicherungsmaßnahmen hier keine Detektions- oder Reaktionsmaßnahmen darstellen. Auch wirken die allgemeinen Sicherungsmaßnahmen nicht präventiv gegen Upstream-Angriffe, da die initiale Kompromittierung im Rahmen eines komplexen Angriffs, bei dem die Angreifer Techniken zur Detektionsevasion und Verschleierung einsetzen, nicht verhindert werden kann, wenn Manipulationen und Schadsoftware nicht erkennbar sind. Im Wesentlichen ergeben sich durch die Umsetzung grundlegender Sicherungsmaßnahmen für die Angreifer somit Hindernisse bei der Durchführung weiterer Angriffsschritte nach der initialen Kompromittierung, die das weitere Vorgehen erschweren oder temporär aufhalten können. In ähnlicher Weise kann mit Hilfe von grundlegenden Sicherungsmaßnahmen bei Midstream-Angriffen hauptsächlich lediglich das Vorgehen der Angreifer in Bezug auf weitere Angriffsschritte nach der initialen Kompromittierung verlangsamt oder erschwert werden. Auch bei Midstream-

Angriffen gibt es gegebenenfalls für die Anwender zunächst keine Anhaltspunkte für eine Kompromittierung des Produkts, da die erste Manipulation hier bereits vor dem Eintreffen beim Anwender stattgefunden hat. In Bezug auf Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten ergibt sich ein ähnliches Bild, da es hier im Prinzip um Manipulationen außerhalb des direkten Einflussbereichs des Anwenders geht und die initiale Kompromittierung in der Regel dort stattfindet. Somit kann mit Hilfe von grundlegenden Sicherungsmaßnahmen gegebenenfalls lediglich das Vorgehen der Angreifer in Bezug auf weitere Angriffsschritte verlangsamt oder erschwert werden, wobei es auch in diesem Fall für den Anwender zunächst möglicherweise keine Hinweise auf eine Kompromittierung gibt.

Bei Downstream-Angriffen ist der Einfluss umgesetzter grundlegender Sicherungsmaßnahmen im Vergleich zu Upstream- und Midstream-Angriffen und Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten größer, da die erste Einwirkung hier im Allgemeinen näher am Einflussbereich des Anwenders liegt. Ein wesentlicher Faktor sind hierbei beispielsweise Angriffe im Zusammenhang mit Fernwartungs- oder sonstigen externen Zugriffen. Durch eine angemessene Rechte- und Zugriffsverwaltung, zum Beispiel durch eine Multi-Faktor-Authentifizierung und der Sicherung und Beschränkung von physischen Zugangsmöglichkeiten, können unbefugte Zugriffsmöglichkeiten vorbeugend eingeschränkt werden. Zudem kann durch ein Managementsystem für mobile Datenträger und eine Überprüfung dieser auf Schadsoftware oder sonstige Kompromittierungen ein Angriff im Zusammenhang mit diesen Komponenten erschwert oder verhindert werden. Dies gilt auch für die Wiederverwendung bzw. Entsorgung von Komponenten, welche durch grundlegende Sicherungsmaßnahmen durch den Anwender in Bezug auf Downstream-Angriffe vor Angreifern geschützt werden kann. Präventive Sicherungsmaßnahmen sind somit bis zu einem gewissen Grad wirksam, auch wenn nicht alle Angriffsvektoren im Zusammenhang mit Downstream-Angriffen durch grundlegende Sicherungsmaßnahmen abgedeckt sind.

5.4.2 Reaktive Sicherungsmaßnahmen und Forensik

Reaktive Sicherungsmaßnahme und die Forensik beziehen sich primär auf die Aspekte Reaktion und, im Fall zeitlich ausgedehnter Angriffe, Detektion bezüglich IT-Angriffen im Zusammenhang mit der Lieferkette. Auch wenn derartige Sicherungsmaßnahmen in der Regel zunächst nicht zur Prävention geeignet sind und IT-Angriffe im Zusammenhang mit der Lieferkette nicht im Vorfeld verhindern oder erschweren, hat sich gezeigt, dass

sie dennoch eine hohe Relevanz in der Bewältigung und im Nachgang zur Aufarbeitung von IT-Sicherheitsvorfällen haben.

In Bezug auf Upstream- und Midstream-Angriffe kommen reaktiven Sicherungsmaßnahmen eine besondere Bedeutung zu, da derartige Angriffe typischerweise aufgrund der Tatsache, dass die ersten Angriffsschritte beim Hersteller bzw. beim Übergang vom Hersteller auf den Anwender erfolgen, für den Endnutzer nur sehr eingeschränkt bzw. nicht durch präventive Maßnahmen zu verhindern sind. Folglich sind reaktive Sicherungsmaßnahmen nach der Erkennung eines Angriffs zu dessen Eindämmung und Aufrechterhaltung bzw. Wiederherstellung des Betriebs essenziell. Dies gilt im Wesentlichen auch für Downstream-Angriffe, sowie für Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten. Dabei können außerdem durch forensische Maßnahmen erlangte Erkenntnisse bei der Rekonstruktion und Aufarbeitung von Angriffen helfen. Durch die Identifizierung der einzelnen Angriffsschritte können möglicherweise Schwachstellen im eigenen Cybersicherheitskonzept aufgedeckt werden, die zur Prävention zukünftiger Angriffe behoben werden können. Zudem ist häufig erst durch eine ausführliche Forensik feststellbar, welche Systeme im Detail kompromittiert wurden und wie die Angreifer vorgegangen sind, sodass sich unter anderem wesentliche Erkenntnisse für die Festlegung (weiterer) reaktiver Sicherungsmaßnahmen ergeben.

Der Aspekt der Wichtigkeit frühzeitig greifender reaktiver Sicherungsmaßnahmen ist insbesondere auch in Bezug auf Downstream-Angriffe relevant, um beispielsweise nach einem Angriff auf betriebliche oder sicherheits- bzw. sicherungsrelevante Systeme schnell zu reagieren, den Schaden zu begrenzen und die Funktionalität möglichst schnell wiederherzustellen. Da bei derartigen Angriffen typischerweise direkt Komponenten und Systeme im Einflussbereich der Anlage betroffen sind, können Angriffe möglicherweise frühzeitiger erkannt und entsprechende Maßnahmen eingeleitet werden. Die entsprechende Vorbereitung reaktiver Sicherungsmaßnahmen ist dabei essenziell. Dies gilt insbesondere auch für Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten, wobei hier angesichts der jeweiligen Abhängigkeiten und externen Komponenten und Dienstleistungen standardmäßig bereits Vorkehrungen gegen den Ausfall oder sonstige Beeinträchtigungen getroffen sein sollten.

5.4.3 Update- und Patchmanagement

Ein umfangreiches und ausgereiftes Update- und Patchmanagement ist in vielerlei Hinsicht essenziell zur Sicherstellung eines allgemein angemessenen Cyber-

Sicherheitsniveaus. Ungepatchte Schwachstellen sind typischerweise einer der häufigsten Angriffsvektoren für Cyberangriffe in allen Sektoren weltweit. Das Patchen von Schwachstellen stellt somit einen wichtigen Faktor zur Prävention von Cyberangriffen allgemein, wie auch speziell im Zusammenhang mit der Lieferkette, dar. Dabei ist jedoch zu beachten, dass der Update- oder Patch-Vorgang als solcher selbst Ziel oder Teil eines Cyberangriffs sein kann. Angreifer können solche Vorgänge beispielsweise ausnutzen, um Zugriff auf isolierte Systeme zu erlangen, die im Normalbetrieb nicht von außerhalb erreichbar sind. Da Patches und Updates einen eigenen Lebenszyklus inklusive der einzelnen Phasen wie Development und Distribution besitzen, können sie selbst angegriffen werden und kompromittiert sein und von Angreifern für weitere Angriffsschritte ausgenutzt werden. Durch Maßnahmen, wie beispielsweise die Prüfung der Integrität von Patches und Updates bzw. Software allgemein vor der Installation über Hash-Werte und die Verwendung geeigneter und eingehend geprüfter mobiler Datenträger und Servicegeräte, lässt sich die Sicherheit solcher Vorgänge entsprechend erhöhen, wobei auch dies bei einem ausreichend geschicktem Vorgehen der Angreifer keinen vollumfänglichen Schutz bietet. Dementsprechend gibt es in einigen Fällen auch legitime Entscheidungen gegen durch Durchführung von Updates und Patches, die entsprechend zu begründen und zu dokumentieren sind. In diesen Fällen ist das Ergreifen alternativer mitigativer Sicherungsmaßnahmen in Bezug auf die ungepatchten Schwachstellen essenziell.

Generell ist ein umfassendes Update- und Patchmanagement als präventive Maßnahme zur Verhinderung oder Erschwerung weiterer Angriffshandlungen im Rahmen eines Cyberangriffs im Zusammenhang mit der Lieferkette zu sehen. Dabei ist zu beachten, dass sich dabei für alle generischen Angriffsmuster Angriffe nicht gänzlich verhindern lassen, da die erste Kompromittierung typischerweise bereits außerhalb des Einflussgebiets der Anlage stattfinden kann: beispielsweise beim Hersteller im Fall von Upstream-Angriffen, beim Übergang zwischen Hersteller und Anwender bei Midstream-Angriffen, bei Fernwartungsdienstleistern bei Downstream-Angriffen oder bei externen Entwicklern bei Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten. Jedoch können weitere Angriffsschritte, die auf die Ausnutzung von Schwachstellen angewiesen sind, durch entsprechende Maßnahmen verhindert werden. Generell lässt sich dabei sagen, dass Upstream- und Midstream-Angriffe sowie Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten auch im Zusammenhang mit Updates und Patches typischerweise schwieriger für die Ziele der Angreifer abzuwehren sind, da Manipulationen durch eine kompromittierte Entwicklungsumgebung und Infrastruktur zur Verteilung schwieriger zu identifizieren sein können. Dies gilt im Wesentlichen auch für

einen möglichen Downstream-Angriff, der die Ausnutzung einer Schwachstelle beinhaltet. Unter Umständen können jedoch durch die Installation von Updates oder Patches Angriffe oder einzelne Angriffshandlungen verhindert werden.

5.4.4 Überprüfung von Code auf Schadsoftware

Maßnahme zur Überprüfung von Code auf Schadsoftware zielen darauf ab, durch Angreifer platzierte, illegitime Änderungen und Ergänzungen sowie anderweitige Manipulationen innerhalb einer Software zu erkennen, bevor der Code ausgeführt wird. Dadurch können Angriffshandlungen im Zusammenhang mit der Lieferkette präventiv erkannt und entsprechende Auswirkungen und weitere Angriffsschritte verhindert werden. Obwohl durch derartige Maßnahmen prinzipiell Manipulationen und Schadsoftwarekomponenten, die in legitimen Codeabschnitten hinzugefügt wurden, erkannt werden können, ist dies in der Praxis oftmals nur eingeschränkt möglich. Einerseits sind Softwareprodukte typischerweise sehr komplex und umfangreich, sodass sich ein entsprechend hoher Aufwand ergibt, auch bei Nutzung automatisierter Prozesse. Dazu ist zudem eine hohe technische Expertise bzw. genaue Kenntnis des Produkts erforderlich, um kompromittierte Elemente als solche zu identifizieren, die möglicherweise nur in Form kleinerer Abweichungen implementiert sind. Dies kann gegebenenfalls allein der Hersteller/Entwickler selbst durchführen, sodass der Anwender nicht die Möglichkeiten hat, dabei selbst effektiv tätig zu werden. Zudem sind bei proprietärer Software detaillierte Informationen über den Code im Gegensatz zu Open-Source-Software in der Regel nicht verfügbar. Gegebenenfalls können diesbezüglich bzw. generell im Zusammenhang mit der Überprüfung von Code auf Schadsoftware im Vorfeld spezielle vertragliche Vereinbarungen zwischen Hersteller/Entwickler und Anwender getroffen werden.

In Bezug auf die unterschiedlichen Angriffsmuster ist insbesondere bei Upstream-Angriffen sowie bei Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten eine Überprüfung von Code auf Schadsoftware für den Anwender aufgrund der oben genannten Gründe nur bedingt durchführbar, wobei es bei Letzteren zwischen proprietären (closed source) und Open-Source-Produkten zu unterscheiden gilt. Bei Midstream- und Downstream-Angriffen ist das ursprüngliche Produkt beim Hersteller selbst nicht kompromittiert, sodass die Chance zur Erkennung einer Kompromittierung durch Überprüfungen des Codes im Vergleich dazu gegebenenfalls unter entsprechenden Umständen höher sein kann. Jedoch sind auch hier die oben genannten Aspekte hinsichtlich der Komplexität und des Aufwands solcher Anstrengungen zu berücksichtigen. Insgesamt sind aus diesem Grund die Maßnahmen hinsichtlich der Überprüfung von Code auf

Schadsoftware für den Anwender im Vergleich zu den anderen in diesem Kapitel diskutierten Maßnahmen nur bedingt zur Prävention von Cyberangriffen im Zusammenhang mit der Lieferkette umsetzbar und geeignet.

5.4.5 Maßnahmen zur Echtzeitüberwachung und Detektion

Ein wesentlicher Aspekt bezüglich IT-Angriffen im Zusammenhang mit der Lieferkette ist die Tatsache, dass Angreifer dabei versuchen, Sicherungsmaßnahmen des eigentlichen Ziels zu umgehen, indem sie sich auf vermeintlich schwächere Zwischenziele innerhalb der Lieferkette konzentrieren. Dies gilt insbesondere (wenn auch nicht ausschließlich) für die präventiven Sicherungsmaßnahmen. Diese versuchen Angreifer zu umgehen, indem sie über die Lieferkette eine initiale Zugriffsmöglichkeit auf die Netzwerke und Systeme der Ziele etablieren, um weitere Angriffsschritte vorzubereiten. Aus diesem Grund kommen Maßnahmen zur Echtzeitüberwachung und Detektion eine besondere Bedeutung zu, um IT-Angriffe im Zusammenhang mit der Lieferkette möglichst frühzeitig zu erkennen, die Angriffe einzuschränken und weitere Maßnahmen einzuleiten. Im Idealfall wird dabei die Kompromittierung durch die Angreifer erkannt, bevor disruptive oder destruktive Auswirkungen auftreten oder Informationen gestohlen wurden. Um Angriffe zu erkennen, können verschiedene Maßnahmen und Technologien eingesetzt werden, die beispielsweise einzelne Verbindungsdaten überprüfen, ausgeführte Dateien und Programme überwachen oder den gesamten Netzwerkverkehr überwachen. Hierbei ist zu beachten, dass moderne Echtzeitüberwachungssysteme wie beispielsweise Security Information and Event Management (SIEM-)Systeme ein ausreichendes Maß an Vernetzung erfordern und gegebenenfalls weitreichende Zugriffsrechte besitzen, sodass sie selbst ein lukratives Ziel für Angreifer darstellen können. Zudem werden im kerntechnischen Bereich sicherheits- oder sicherungsrelevanten Komponenten typischerweise weitgehend isoliert und ohne direkte Verbindungen nach außerhalb eingesetzt, sodass eine umfassende Echtzeitüberwachung des gesamten Datenverkehrs unter derartigen Umständen möglicherweise nicht vollständig realisiert werden kann.

Maßnahmen zur Echtzeitüberwachung und Detektion sind grundsätzlich für alle IT-Angriffe im Zusammenhang mit der Lieferkette beziehungsweise alle Angriffsmuster relevant. Eine besonders hohe Bedeutung kommt derartigen Maßnahmen bei Upstream-Angriffen und Angriffen im Zusammenhang mit Abhängigkeiten und externen Komponenten zu, da in diesen Fällen die kompromittierenden Handlungen der Angreifer für den Anwender gegebenenfalls nur sehr schwer oder gar nicht zu erkennen sind. Dementsprechend ist es in diesem Zusammenhang essenziell, maliziöse Handlungen und

weitere Angriffsschritte der Angreifer im eigenen Netzwerk oder in Bezug auf einzelne Systeme und Komponenten schnellstmöglich zu detektieren, wenn eine Prävention oder Mitigation nicht möglich ist und die erste Kompromittierung nicht bemerkt wird. Hierbei ist hinsichtlich der Definition der Angriffsmuster zu beachten, dass Maßnahmen zur Echtzeitüberwachung typischerweise zwar grundsätzlich in den operativen Phasen im Lebenszyklus eingesetzt werden, dabei jedoch auch schon in früheren Phasen des Lebenszyklus vorbereitete und eingeleitete Angriffe detektieren können, beispielsweise durch weitere Angriffshandlungen der Angreifer oder unerwartetes Systemverhalten. Auch um Zusammenhang mit Midstream- und Downstream-Angriffen sind Maßnahmen zur Echtzeitüberwachung und Detektion ein wichtiges Werkzeug, um laufende IT-Angriffe zu detektieren, mitigieren und weitere Angriffshandlungen zu verhindern. In allen Fällen sind dabei sowohl Maßnahmen zur Echtzeitüberwachung wie auch regelmäßige Überprüfungen, beispielsweise in Form von Audits sinnvoll, wobei bei Echtzeitmaßnahmen die oben genannten Aspekte hinsichtlich der Konnektivität der entsprechenden Systeme zu berücksichtigen sind.

5.5 Abdeckung der Angriffsmuster und Sicherungsmaßnahmen durch betrachtetes Regelwerk

Aufbauend auf den definierten generischen Angriffsmustern (siehe Abschnitt 5.3) und den untersuchten Vorgehensweisen zur Sicherstellung der IT-Sicherheit in der Lieferkette (siehe Kapitel 4) wurde im Rahmen des Vorhabens analysiert, inwieweit die identifizierten relevanten Aspekte insbesondere in Bezug auf die Sicherungsmaßnahmen im Regelwerk adressiert werden und abgedeckt sind. Dabei liegt der Fokus auf dem deutschen Regelwerk. Zunächst ist dabei zu beachten, dass es innerhalb des betrachteten Regelwerks in Bezug auf IT-Angriffe im Zusammenhang mit der Lieferkette keine explizite Unterscheidung in Bezug auf den Lebenszyklus hinsichtlich einzelner Sicherungsmaßnahmen gibt, sondern der Lebenszyklus als Ganzes diskutiert wird. Dabei werden auch einzelne Phasen im Lebenszyklus wie beispielsweise die Entwicklung, der Einsatz oder die Entsorgung adressiert. Innerhalb des IT-Grundschutz Kompendiums des BSI gibt es zu diesen verschiedenen Aspekten beispielsweise einzelne Bausteine mit den jeweiligen Anforderungen (siehe Abschnitt 4.1.1). Somit werden einzelne Angriffsvektoren innerhalb der Angriffsmuster im IT-Grundschutz Kompendium explizit angesprochen wie beispielsweise die Fernwartung, die dem Angriffsmuster „Downstream-Angriffe“ zugeordnet ist oder die (Software-)Entwicklung, die unter die Definition der „Upstream-Angriffe“ fällt. Auch mögliche Probleme bei der Einbindung externer Komponenten und Dienstleistungen und entsprechende Sicherungsmaßnahmen werden im IT-

Grundschutz Kompendium explizit aufgegriffen. Somit werden Inhalte der generischen Angriffsmuster vom BSI jeweils adressiert, wobei hier keine Einzelbetrachtung aller möglichen Angriffsvektoren der einzelnen Angriffsmuster durchgeführt wird. Die für die einzelnen Phasen im Lebenszyklus wesentlichen Gefahren, relevante Angriffsmöglichkeiten, auf denen die generischen Angriffsmuster beruhen und entsprechende Sicherungsmaßnahmen lassen sich damit im IT-Grundschutz Kompendium wiederfinden. Hierbei ist zu beachten, dass der Fokus des BSI mit dieser Veröffentlichung wesentlich breiter angesetzt ist und die IT-Sicherheit im Zusammenhang mit der Lieferkette nur einen Teilbereich der zu betrachtenden Thematik hinsichtlich der Cybersicherheit darstellt. Generell gilt auch für die anderen betrachteten deutschen Regelwerke, dass der Themenbereich breiter gewählt ist und es bisher keine expliziten regulatorischen Veröffentlichungen alleinig zum Thema IT-Sicherheit in der Lieferkette gibt. Zusammen mit dem überwiegend leistungsbasierten Ansatz ist somit eine detaillierte Adressierung jedes einzelnen Angriffsvektors der generischen Angriffsmuster nicht der Anspruch des deutschen Regelwerks, welches abgesehen von einzelnen Bausteinen im IT-Grundschutz Kompendium die Sicherstellung der IT-Sicherheit in der Lieferkette im Wesentlichen durch definierte Ziele und Ergebnisse fordert. In großen Teilen lässt sich dies auch in Bezug auf die einzelnen Sicherungsmaßnahmen übertragen.

Hinsichtlich der unterschiedlichen Kategorien von Sicherungsmaßnahmen (siehe Abschnitt 5.2) gibt es im betrachteten Regelwerk wesentliche Unterschiede hinsichtlich der Anforderungen und Empfehlungen. Dabei ist zu beachten, dass sich die Maßnahmen direkt an die jeweiligen Betreiber bzw. Unternehmen richten, von diesen umzusetzen sind und sich in der Regel nicht explizit auf die Lieferkette erstrecken, wobei ggf. Anforderungen die Sicherstellung eines vergleichbaren Sicherungsniveaus fordern. Hierbei werden jedoch keine expliziten Vorgaben gemacht. Aus diesem Grund werden im Folgenden die betrachteten Kategorien von Sicherungsmaßnahmen hinsichtlich der Umsetzung vor Ort beim Betreiber bzw. Anwender diskutiert.

Grundlegende Sicherungsmaßnahmen stellen in nahezu allen betrachteten Regelwerken national und international das Fundament aller Bemühungen zur Sicherstellung der Cybersicherheit dar, allgemein und speziell im Zusammenhang mit der Lieferkette. Im deutschen Regelwerk sind in diesem Zusammenhang im kerntechnischen Bereich hauptsächlich die SEWD-Richtlinie IT sowie das IT-Grundschutz Kompendium des BSI zu nennen. In diesen Veröffentlichungen finden sich diverse Sicherungsmaßnahmen zur Etablierung eines grundlegenden Sicherungsniveaus, die hauptsächlich auf die Prävention setzen, wobei auch die Aspekte Detektion und Reaktion aufgegriffen werden. Die

grundlegenden präventiven Sicherungsmaßnahmen sind dabei nicht auf den Bereich IT-Sicherheit in der Lieferkette begrenzt, sondern finden übergeordnet und unabhängig von einzelnen Teilaspekten der Cybersicherheit breite Anwendungen. Im IT-Grundschutz-Kompendium gibt es beispielsweise in diesem Zusammenhang unterschiedliche Bausteine, die verschiedene Themengebiete mit entsprechenden Sicherungsmaßnahmen abdecken. Wie bereits oben diskutiert, wird dabei hauptsächlich ein leistungsbasierter Ansatz verfolgt, wobei im direkten Vergleich zu Regelwerken anderer Länder wie den USA, welche dedizierte Regelwerksdokumente zum Thema IT-Sicherheit in der Lieferkette veröffentlicht haben, die einzelnen Aspekte dieses Themenkomplexes nicht in dieser Detailtiefe adressiert werden. Insgesamt finden sich im einschlägigen deutschen Regelwerk somit diverse präventive, grundlegende Sicherungsmaßnahmen, die den Schutz kerntechnischer Anlagen vor Cyberangriffen, auch im Zusammenhang mit der Lieferkette, gewährleisten sollen.

Auch die Themen reaktive Sicherungsmaßnahmen und Forensik werden typischerweise im Regelwerk adressiert. In Deutschland finden sich Anforderungen zu entsprechenden Sicherungsmaßnahmen im einschlägigen Regelwerk, wobei hier der Fokus der reaktiven Maßnahmen auf den unmittelbaren Handlungen im Fall eines Cyberangriffs liegt. Das BSI ist dabei in solchen Fällen als die Cyber-Sicherheitsbehörde des Bundes der erste Ansprechpartner und sollte entsprechend informiert werden, sodass die weiteren Aktionen zur Eindämmung, Mitigation und Wiederherstellung koordiniert und effektiv eingeleitet und umgesetzt werden können. Auch die reaktiven Sicherungsmaßnahmen und Anforderungen bezüglich möglicher Forensik werden dabei typischerweise im deutschen Regelwerk für Cyberangriffe allgemein, nicht ausschließlich im Zusammenhang mit der Lieferkette, diskutiert. Dabei gibt es beispielsweise im IT-Grundschutz Kompendium einen Baustein zu Detektion und Reaktion, der im Rahmen des Security Incident Managements auch auf das Thema IT-Forensik eingeht.

Das Thema Update- und Patchmanagement wird ebenfalls in den unterschiedlichen Regelwerken aufgegriffen, wobei in diesem Zusammenhang der Fokus typischerweise bei dem damit einhergehenden Aspekt des Schwachstellenmanagements liegt. Im IT-Grundschutz Kompendium gibt es beispielsweise einen Baustein, der die Themengebiete Patch- und Änderungsmanagement beinhaltet. Dabei geht es zudem unter anderem um die Sicherstellung der Integrität und Authentizität von Softwarepaketen, sodass der Fokus hierbei auch auf der Sicherstellung der IT-Sicherheit in der Lieferkette liegt. Zudem sind die potenziellen Gefahren der automatisierten Verteilung von Patches explizit angesprochen, wobei unter anderem fehlerhafte Patches genannt werden, die

beispielsweise Sicherheitslücken enthalten. Weiterhin wird die Gefahr von Updates und Patches aus nicht vertrauenswürdigen Quellen, die gegebenenfalls mit schädlichem Code infiziert sind, konkret erwähnt. Insgesamt wird das Thema Update- und Patchmanagement somit hinsichtlich der allgemeinen Relevanz in Bezug auf die Sicherstellung der Cybersicherheit adressiert, wie auch durch konkrete Bezüge zur Lieferkette.

Das Thema Überprüfung von Code auf Schadsoftware wird in den betrachteten Regelwerken im Wesentlichen indirekt adressiert. Konkrete Anforderungen zur regelmäßigen Überprüfung von Code sind insbesondere für die Anwender nicht vorgesehen, was angesichts der bereits in den Abschnitten 5.2 und 5.4.4 diskutierten Komplexität und den entsprechenden technischen beziehungsweise logistischen Herausforderungen diesbezüglich hinsichtlich einer umsetzbaren Realisierung plausibel ist. Vielmehr gibt es unter anderem im IT-Grundschutz Kompendium Bausteine, die sich mit dem Thema Software-Entwicklung befassen und diverse Sicherungsmaßnahen in diesem Zusammenhang beinhalten, die eine sichere Software-Entwicklung garantieren sollen. Auch hier wird unter anderem explizit auf die notwendige Überprüfung externer Komponenten hingewiesen, sodass die IT-Sicherheit in der Lieferkette an dieser Stelle teilweise explizit adressiert wird.

Der Gruppe von Sicherungsmaßnahme in Zusammenhang mit der Detektion kommt bei IT-Angriffen auf beziehungsweise über die Lieferkette eine besondere Bedeutung zu, da sich wie bereits diskutiert solche IT-Angriffe typischerweise nicht vollständig durch präventive Sicherungsmaßnahmen verhindern lassen. Somit ist die Detektion von Angreiferhandlungen und laufender Angriffe, die nicht verhindert werden konnten, essenziell, um weiterführende Maßnahmen einleiten zu können und das Ausmaß zu begrenzen. Die Wichtigkeit von Maßnahmen zur Detektion hat sich vor allem mit der Zunahme von IT-Sicherheitsvorfällen im Zusammenhang mit der Lieferkette in den letzten Jahren gezeigt. Eine entsprechende Nachschärfung regulatorischer Anforderungen in dieser Hinsicht sind sowohl international wie auch national im deutschen Regelwerk zu beobachten. Hierbei sind vor allem das IT-Sicherheitsgesetz 2.0 mit der Forderung nach entsprechenden Echtzeitüberwachungssystemen (wenn auch nicht für kerntechnische Anlagen) wie auch das IT-Grundschutz Kompendium mit dem Baustein zu Detektion und Reaktion zu nennen. Speziell für den kerntechnischen Bereich wird das Thema auch in der Weiterleitungsnachricht 2021/01 „*IT-Angriffe auf kritische Infrastrukturen im Zusammenhang mit der Schadsoftware Triton/TriSIS*“ /GRS21r14/ der GRS mit entsprechenden Empfehlungen diskutiert. Bezüglich der generischen Angriffsmuster sind Maßnahmen zur Detektion für alle vier Muster relevant, wobei insbesondere bei den Angriffsmustern mit

Fokus auf die frühen Phasen im Lebenszyklus eine besondere Bedeutung vorliegt, da in diesen Fällen IT-Angriffe für Anlagen bzw. Anwender nur schwer zu verhindern beziehungsweise zu erkennen sind. Dementsprechend sind Maßnahmen zur Erkennung ungewöhnlicher Vorgänge und möglicher Angriffsspuren im eigenen System beziehungsweise Netzwerk essenziell. Dies gilt auch für Angriffe im Zusammenhang mit Abhängigkeiten und externen Komponenten.

Insgesamt handelt es sich bei der Fragestellung der Sicherstellung der IT-Sicherheit in der Lieferkette um ein hochdynamisches Themengebiet, das einerseits durch eine hohe Anzahl an IT-Sicherheitsvorfällen in diesem Bereich und andererseits durch entsprechend aktualisierte oder neu veröffentlichte Regelwerk gekennzeichnet ist. Insbesondere international sind in diesem Zusammenhang in den letzten Jahren verschiedene Regelwerke veröffentlicht worden oder diese befinden sich aktuell in der Vorbereitung. Das deutsche Regelwerk erstreckt sich in diesem Bereich mit einem überwiegend leistungsbasierten Ansatz auch auf das Thema IT-Sicherheit in der Lieferkette, auch wenn dies in vielen Fällen verglichen mit anderen nationalen oder internationalen Regelwerken nicht in dieser Ausführlichkeit dediziert adressiert wird. Dabei standen in der Vergangenheit im Wesentlichen der Aspekt der Prävention von IT-Angriffen, sowie Maßnahmen zur Reaktion im Fokus. Maßnahmen zur Detektion wurden dabei stets mitbetrachtet, jedoch stehen diese in den letzten Jahren vermehrt im Fokus. Generell ist der internationale Ansatz, das Thema IT-Sicherheit in der Lieferkette durch dedizierte Veröffentlichung prominent hervorzuheben und das Bewusstsein dafür zu stärken ein wesentlicher Baustein, die Cybersicherheit in diesem Bereich weiter zu verbessern. Dementsprechend ist auch im Bereich des deutschen Regelwerks zu erwarten, dass dieses Thema in Zukunft verstärkt adressiert wird und weiteren Einzug in die entsprechenden relevanten Veröffentlichungen erhält. Dies gilt sowohl für das bestehende Regelwerk, beispielsweise in Form zukünftiger Aktualisierungen, wie auch für mögliche neue dedizierte Regelungen in diesem Bereich (zum Beispiel durch neue Gesetze wie dem IT-Sicherheitsgesetz 2.0). Insbesondere angesichts der bereits beobachteten und mutmaßlich zunehmenden Angreiferaktivitäten in diesem Zusammenhang ist dies ein wichtiger Baustein der zukünftigen Strategie zur Abwehr und zum Umgang mit IT-Sicherheitsvorfällen und gezielten Cyberangriffen allgemein und speziell in diesem Bereich.

6 Zusammenfassung

Digitale Systeme zur Informationsverarbeitung sowie zur Steuerung von Prozessen und Systemen sind in der heutigen Zeit ein elementarer Bestandteil nahezu aller kommerziellen und industriellen und Systeme und Bereiche, einschließlich kritischer Infrastrukturen wie beispielsweise kerntechnische Anlagen und Einrichtungen. Auch in deutschen Anlagen werden neben informationsverarbeitenden Systemen vermehrt leittechnische Systeme bzw. rechnerbasierte und programmierbare Systeme zur Überwachung und Steuerung verfahrenstechnischer Prozesse eingesetzt. Die Sicherstellung der IT-Sicherheit derartiger Systeme bezüglich Störmaßnahmen und sonstigen Einwirkungen Dritter ist ein kritischer Baustein, der für den sicheren Betrieb solcher Anlagen essenziell ist. Dafür müssen mögliche Angriffspfade und Schwachstellen umfassend betrachtet werden, um potenzielle Auswirkungen zu verhindern und in diesem Zusammenhang notwendige Sicherungsmaßnahmen zu ergreifen. In den vergangenen Jahren sind vermehrt Cyberangriffe auf IT-Systeme sowie sicherheitskritische Einrichtungen beobachtet worden, die mit der Lieferkette dieser Systeme zusammenhängen. Derartige Angriffe können weitreichende Auswirkungen hinsichtlich der Anzahl potenzieller Opfer haben und ermöglichen Angreifern zudem gegebenenfalls Sicherungsmaßnahmen des anvisierten Ziels zu umgehen, indem vermeintlich schwächere Ziele in der Lieferkette kompromittiert und somit einfachere Zugriffsmöglichkeiten für Angriffshandlungen geschaffen werden. In diesem Vorhaben wurde die Frage der Sicherstellung der IT-Sicherheit im Zusammenhang mit der Lieferkette aufbauend auf einer Voruntersuchung zum Stand von Wissenschaft und Technik und in den letzten Jahren beobachteten IT-Sicherheitsvorfällen in diesem Bereich /GRS21r15/ untersucht.

Zunächst wurde anhand einer weitergehenden Untersuchung von IT-Sicherheitsvorfällen im Zusammenhang mit der Lieferkette das Potenzial derartiger IT-Angriffe analysiert. Neben IT-Sicherheitsvorfällen mit direktem Bezug zu kerntechnischen Anlagen und Einrichtungen wurden auch darüberhinausgehende relevante Fälle betrachtet, anhand derer entsprechend übertragbare Erkenntnisse gewonnen werden konnten. Die Auswertung der Gemeinsamkeiten, Unterschiede und Charakteristika der einzelnen, teilweise verschiedenartigen IT-Sicherheitsvorfälle (gezielte Angriffe auf Einzelziele, Kompromittierung von IT-Dienstleistern, ausgenutzte Schwachstellen usw.) ermöglichten die Erfassung eines möglichst vollständigen Gesamtbilds der IT-Bedrohungslage, Arten von Angriffsmöglichkeiten in diesem Zusammenhang und von Gemeinsamkeiten und generischen Aspekten. Dabei wurden zunächst für die verschiedenen Phasen des Lebenszyklus der einzelnen Systeme die Angriffsmöglichkeiten für Cyberangriffe im

Zusammenhang mit der Lieferkette betrachtet. Bezüglich der aus den betrachteten IT-Sicherheitsvorfällen abgeleiteten generischen Sicherungsmaßnahmen zur Sicherstellung der IT-Sicherheit in der Lieferkette wurden fünf übergeordnete Gruppen identifiziert, die dabei eine besondere Relevanz aufweisen. Neben allgemeinen, grundlegenden Sicherungsmaßnahmen sind dies reaktive und forensische Sicherungsmaßnahmen, das Update- und Patchmanagement, Codeüberprüfungen und insbesondere Maßnahmen zur Echtzeitüberwachung und Detektion.

In einem zweiten Schritt wurden nationale und internationale Vorgehensweisen zur Sicherstellung der IT-Sicherheit in der Lieferkette analysiert. Dazu wurden Regelwerke aus Deutschland, Großbritannien, Finnland und den Vereinigten Staaten sowie internationale Regelwerke der IAEA und entsprechende Normen betrachtet. Der Fokus lag dabei auf dem deutschen Regelwerk und dem Vergleich zu den anderen betrachteten Veröffentlichungen. Hierbei wurden als Grundlage das vom BSI herausgegebene IT-Grundschutz-Kompendium, für den nuklearen Kontext die dem BMUV zuzuordnende SEWD-Richtlinie IT und das Regelwerk des vom BMUV gebildeten Kerntechnischen Ausschusses, sowie das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) betrachtet. Im Wesentlichen ergeben sich dabei Unterschiede hinsichtlich eines leistungsbasierten und eines präskriptiven Ansatzes, wobei die Sicherstellung der IT-Sicherheit im Zusammenhang mit der Lieferkette im deutschen Regelwerk einerseits konkret angesprochen wird, oftmals aber auch im Rahmen allgemeinerer Anforderungen bzw. in Kombination mit anderen Themenschwerpunkten adressiert wird. In neueren Regelwerken beispielsweise in den Vereinigten Staaten wird das Thema teilweise dediziert aufgegriffen und durch spezifische Sicherungsmaßnahmen konkretisiert. Insgesamt ist die IT-Sicherheit im Zusammenhang mit der Lieferkette ein Thema, das sowohl in den deutschen wie auch in internationalen Regelwerken aufgegriffen wird wobei sich je nach nationalem Kontext Unterschiede in den Schwerpunkten sowie im Detaillierungsgrad ergeben.

Ausgehend von den untersuchten IT-Sicherheitsvorfällen im Zusammenhang mit der Lieferkette und dem analysierten Regelwerk wurden im Rahmen des Vorhabens generische Angriffsmuster erstellt und die Eignung und Wirksamkeit von Sicherungsmaßnahmen wurden in diesem Kontext analysiert. Die generischen Angriffsmuster orientieren sich dabei an den unterschiedlichen Phasen des Lebenszyklus und beinhalten Upstream-, Midstream und Downstream-Angriffe sowie Angriffe im Zusammenhang mit Abhängigkeiten, externen Komponenten und Diensten. Hierbei wurden jeweils die Skalierbarkeit, Übertragbarkeit und potenzielle Auswirkungen sowie Anforderungen an Täter

und Tatmittel untersucht. Bezüglich der Eignung und Wirksamkeit der Sicherungsmaßnahmen sind prinzipiell alle betrachteten übergeordneten Gruppen relevant für jedes der generischen Angriffsmuster, wobei sich entsprechend der unterschiedlichen Charakteristika der jeweiligen Angriffsmuster kleinere Unterschiede ergeben. Allgemein sind bei IT-Angriffen im Zusammenhang mit der Lieferkette insbesondere Maßnahmen zur Echtzeitüberwachung und Detektion von hoher Relevanz, da präventive Maßnahmen allein eine Kompromittierung nicht vollständig verhindern können und somit eine möglichst zeitnahe Aufdeckung entsprechender Angriffshandlungen essenziell ist, um den Angriff einzudämmen und weitere Maßnahmen einzuleiten. Hinsichtlich der Abdeckung der Angriffsmuster und Sicherungsmaßnahmen im Zusammenhang mit dem deutschen Regelwerk zeigt sich, dass die Sicherstellung der IT-Sicherheit in der Lieferkette einen wesentlichen Teilaspekt in Bezug auf die allgemeine Cybersicherheit darstellt, der hauptsächlich durch entsprechende Zielvorgaben adressiert ist. Durch die hohe Dynamik in diesem Bereich, insbesondere durch diesbezüglich zunehmende IT-Sicherheitsvorfälle, und damit einhergehende aktualisierte bzw. neu erstellte Regelwerke, die diesen Schwerpunkt besitzen, ist zu erwarten, dass das Thema auch zukünftig eine zentrale Rolle innerhalb jeder Strategie zur Sicherstellung der Cybersicherheit spielt. Dementsprechend sollten der sich ständig fortentwickelnde Stand von Wissenschaft und Technik sowie neue Entwicklungen in diesem Bereich kontinuierlich weiterverfolgt und analysiert werden.

Literaturverzeichnis

/3CX23w01/ 3CX: Update zum Sicherheitsvorfall: Samstag, 1. April 2023

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

/AKA22w01/ Akami Security Research, Doytshman, C., "Akamais Observations of Confluence Zero Day(CVE-2022-26134)", 28.06.2022, www.akami.com [abgerufen am 12.12.2023]

/ARS14w01/ Arstechnica, Active Malware Operation Let Attackers Sabotage US Energy Industry, D. Goodin, 30 June 2014, www.arstechnica.com [abgerufen am 14.07.2020]

/ATN21w01/ All Tech News, Codecov Supply Chain Attacke kann tausende treffen: Bericht, 21. April 2021, www.alltechde.com [abgerufen am 05.09.2022]

/BAR21w01/ BARIKAT, Microsoft Exchange Server Remote Code Execution Vulnerability-31206, www.guvenlikzafiyet.barikat.com, [abgerufen am 01.12.2021]

/BIT23r01/ BITMARCK: BITMARCK bestaetigt unbefugten Zugriff auf Infrastruktur, 03 February 2023

/BIT23r02/ BITMARCK: Informationen zum Cyberangriff, Stand 28 June 2023

/BLE18w01/ BleepingComputer, Cimpanu, C., "400K Malware Outbreak Caused by Backdoored Russian Torrenting Client", 14.03.2018, www.bleepingcomputer.com

/BLO21w03/ Bloomberg, Turton, W. et al., "Inside the Race to Fix aPotentially Disastrous Software Flaw", 14.12.2021 www.bloomberg.com

/BMU13n03/ 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), 13.06.2013

/BMU20n02/ BMU, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und bei Tätigkeiten der Sicherungskategorie III sowie der umsichtigen Betriebsführung gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT SK III), 25.08.2020

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

/BSI19i01/ Bundesamt für Sicherheit in der Informationstechnik, BSI-Cyber-Sicherheitswarnung, Angriffe über VPN-Zugänge von Zulieferern, CSW-Nr. 2019-208434-10k4, Version 1.0, 12.06.2019

/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

/BSI21i01/ Bundesamt für Sicherheit in der Informationstechik, BSI-Cyber-Sicherheitswarnung, Supply-Chain-Angriff über manipulierte SolarWinds OrionSoftware, CSW-Nr. 2020-533179-19k3, Version 1.9, 05.02.2021

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

/BSI21i04/ BSI, Mehrere Schwachstellen in MS Exchange, CSW-Nr. 2021-197772-18k2, Version 1.8, 12.03.2021

/BSI21i05/ BSI, Tageslagebericht vom 04.11.2021

/BSI21i12/ BSI, Cyber-Sicherheitswarnung 2021-234002-1332, 12.07.2021

/BSI21r05/ Bundesamt fuer Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, 2021

/BSI22i08/ BSI, Tageslagebericht vom 29.03.2022

/BSI23i13/ Bundesamt fuer Sicherheit in der Informationstechnik (BSI), Cyber-Sicherheitswarnung 2023-214183-11k7, "Cyberangriff auf adesso SE", 09.03.2023

/BSI23r22/ BSI, Schadhafte Version der 3CX Desktop App im Umlauf, Version 1.1, 05 April 2023

/BTB23w01/ B2B Cyber Security News, Alphv veroeffentlicht Daten von Ziegler, 25.04.2023, www.b2b-cyber-security.de/ [abgerufen am 28.09.2023]

/BUN21r01/ Deutscher Bundestag, Parlamentsnachrichten, Hackerangriff auf SolarWinds, Inneres und Heimat/Antwort - 01.02.2021 (hib 141/2021), www.bundestag.de [abgerufen am 20.04.2021]

/BUS17w01/ Business Insider, The 'Petya' global cyberattack may have just been cover for an attack in Ukraine, 30 June 2017, 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, www.businessinsider.com [abgerufen am 19.04.2021]

/CBS21w01/ CBS News, 60 Minutes, SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments, 14 February 2021, www.cbsnews.com [abgerufen am 08.03.2021]

/CHE22w01/ Checkmarx, A beautiful Factory for malicious Packages, March 28 2022, *https://checkmarx.com, [abgerufen am 15.11.2022]*

/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]

/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

/CIS20i01/ CISA, Emergency Directive 21-01, Mitigate SolarWinds Orion Code Compromise, 13 Dec 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]

/CIS21i10/ CISA Cybersecurity Advisory AA21-356A, "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities", 23.12.2021

/CIS21r02/ U. S. Department of Homeland Security, CISA, Malware Analysis Report (AR21-039A), MAR-10318845-1.v1 - SUNBURST, 08 February 2021

/CIS21w05/ Cisco Talos Intelligence Group, Microsoft Exchange vulnerabilities exploited once again for ransomware, this time with Babuk, www.blog.talosintelligence.com, [abgerufen am 13.06.2022]

/CIT17w01/ Cisco Talos, CCleanup: A Vast Number of Machines at Risk, 18. September 2017, www.blog.talosintelligence.com, [abgerufen am 13.08.2021]

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

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

/COD21w01/ Codecov, Bash Uploader Security Update, 15. April 2021, www.about.codecov.io/security-update [abgerufen am 05.09.2022]

/CSI14r01/ Cyber Security Infotech(P) Ltd: Rogue GOM Player Update That Installed Malware at a Japanese Nuclear Plant Analyzed, 2014

/CVE21w01/ CVE Details, Microsoft Exchange Server: Security Vulnerabilities Published In 2021, www.cvedetails.com, [abgerufen am 01.12.2021]

/CYA18w01/ Cyware Alerts - Hacker News, Operation Red Signature campaign found delivering 9002 RAT to South Korean organizations, August 22, 2018, www.cyware.com, [abgerufen am 09.02.2022]

/CYA19w01/ Cyware Alerts Hacker News, A Brief Look at the Citadel Banking Trojan, October 20, 2019, https://cyware.com, [abgerufen am 12.08.2021]

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

/DAR21w01/ Dark Reading, More SolarWinds Attack Details Emerge, K. Higgins, January 2019, www.darkreading.com [abgerufen am 04.03.2021]

/DAR21w02/ Dark Reading, FireEye's Mandia: 'Severity-Zero-Alert' Led to Discovery of SolarWinds Attack, K. Higgins, January 2021, www.darkreading.com [abgerufen am 04.03.2021]

/DEC22w01/ Decipher, Azure Developers Targeted by malicious NPM Packages, Mar 24 2022, www.duo.com/decipher/azure-developers-targeted-by-malicious-npm-packages [abgerufen am 15.11.2022]

/DEV21w01/ Dev Insider, Wie Hacker ihre Angriffe verschleiern, Der Codecov-Tool-Hack im Detail, 09.07.2021, www.dev-insider.de [abgerufen am 05.09.2022]

/DIN18n01/ DIN IEC 62443-4-1, IT-Sicherheit fuer industrielle Automatisierungssysteme, Teil 4-1: Anforderungen an den Lebenszyklus fuer eine sichere Produktentwicklung, 2018

/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

/DIN20n05/ DIN EN IEC 62443-2-4, IT-Sicherheit fuer industrielle Automatisierungssysteme, Teil 2-4: Anforderungen an das IT-Sicherheitsprogramm von Dienstleistern fuer industrielle Automatisierungssysteme, 2020

/DIV21w02/ DIVD CSIRT, Breedijk, F., "KASEYA VSA LIMITED DISCLOSURE", 07.07.2021, www.csirt.divd.nl [abgerufen am 12.12.2023]

/DIV21w03/ DIVD CSIRT, Gevers, V., "KASEYA CASE UPDATE 2", 04.07.2021, www.csirt.divd.nl [abgerufen am 12.12.2023]

/DOD20r01/ Office of the Undersecretary of Defence, Acquisition and Sustainment, Cybersecurity Maturity Model Certification (CMMC), 18. Maerz 2020

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

/DSW14r01/ Dell Secure Works Counter Threat Unit TM Threat Intelligence, Keith Jar-vis and Jason Milletary, Inside a Targeted Point-of-Sale Data Breach, Threat ID: 773, 24 January 2014

/ENI22w01/ Enigmasoftware, "Magecart", www.enigmasoftware.de

/ENI23r01/ European Union Agency for Cybersecurity (ENISA), "Good Practices for Supply Chain Cybersecurity", 13. Juni 2023

/ENS20w01/ EnigmaSoft: Backdoor.Win32.Miancha, Informationen, 2020

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

/EWO20w01/ Ewon, „Kompetenzzentrum für Remote Solutions das sind wir“, www.e-won.biz/de [abgerufen am 15.07.2020]

/FAY18r01/ Fayi S.Y.A.: “What Petya/NotPetya Ransomware Is and What Its Remidiations Are” Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738, 2018

/FAZ21w04/ FAZ, "Bundesfinanzhof schaltet Website nach Hackerangriff ab", 17.12.2021, www.faz.net [abgerufen am 12.12.2023]

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

/FSE15w01/ F-Secure Labs, Havex Hunts for ICS/SCADA Systems, www.archive.f-secure.com [abgerufen am 15.07.2020]

/GRS10r01/ Gesellschaft für Anlagen- und Reaktorsicherheit, Weiterleitungsnachricht WLN 2010/07, "Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCS7", 01.10.2010

/GRS16r01/ Gesellschaft für Anlagen- und Reaktorsicherheit, Weiterleitungsnachricht WLN 2016/08, „Schadsoftwarefunde im Kernkraftwerk Gundremmingen, Block B“, 18.08.2016

/GRS21r14/ Gesellschaft für Anlagen- und Reaktorsicherheit, Weiterleitungsnachricht WLN 2021/01, „IT-Angriffe auf kritische Infrastrukturen im Zusammenhang mit der Schadsoftware Triton/TriSIS“, 23.02.2021

/GRS21r15/ Gesellschaft für Anlagen- und Reaktorsicherheit, GRS-Bericht 638 "IT-Sicherheit in der Lieferkette", Mai 2021

/GRS21r16/ Gesellschaft für Anlagen- und Reaktorsicherheit, GRS-Bericht 647, "IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand Mai 2021", August 2021

/GRS23r02/ Gesellschaft für Anlagen- und Reaktorsicherheit, GRS-Bericht 718, "IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand September 2022", November 2022

/GRS24r01/ Gesellschaft für Anlagen- und Reaktorsicherheit, GRS-Bericht zur IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen, Veröffentlichung voraussichtlich 2024

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

/HEI18r01/ Heise Online, „Hacker stellen Daten zu französischen Atomanlagen ins Netz“, 02.11.2018, www.heise.de [abgerufen am 20.12.2023]

/HEI21w14/ Heise online, Sicherheitsforscher bricht ueber Open-Source-Repositories bei PayPal & Co. ein, 10.02.2021, www.heise.de/news/Sicherheitsforscher-bricht-ueber-Open-Source-Repositories-bei-PayPal-Co-ein-5051635.html [abgerufen am 10.11.2022]

/HEI21w15/ Heise Online, Schmidt, J., "Kaseya VSA: Wie die Lieferketten-Angriffe abliefen und was sie fuer uns bedeuten", 06.07.2021, www.heise.de [abergufen am 12.12.2023]

/HEI21w16/ Heise Online, "Hacker-Angriff ueber IT-Dienstleister Kaseya trifft Hunderte Unternehmen", 05.07.2021, www.heise.de [abgerufen am 12.12.2021]

/HEI22w24/ Heise Online, Scherschel, F. A., "Log4Shell: Eine Bestandsaufnahme", 29.01.2022, www.heise.de [abgerufen am 12.12.2023]

/HEI23w14/ Heise Online: BITMARCK bestaetigt unbefugten Zugriff auf Infrastruktur, 03 February 2023

/HEI23w15/ Heise Online, Schmidt, J. et al., "Cyberattacke auf IT-Dienstleister Adesso: Systeme kompromittiert, Daten kopiert", 01.02.2023, www.heise.de [abgerufen am 12.12.2023]

/HUM14w01/ Hummingbird, "PHP/Webshell-Diagnoseprobleme und Sicherheitsprobleme, die auf dem GOM Player Bulletin Board entdeckt wurden", www.hummingbird.tistory.com [abgerufen am 26.01.2024]

/IAE11n02/ International Atomic Energy Agency (IAEA), IAEA Nuclear Security Series, Computer Security at Nuclear Facilities, NSS 17, 2011

/IAE18n02/ International Atomic Energy Agency (IAEA), IAEA Nuclear Security Series, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, NSS 33-T, 2018

/IAE21n01/ International Atomic Energy Agency (IAEA), IAEA Nuclear Security Series, Implementation Guide, Computer Security for Nuclear Security , NSS 42-G, 2021

/IAE21n03/ International Atomic Energy Agency (IAEA), Computer Security Techniques for Nuclear Facilities NSS 17-T, September 2021

/IAE22n01/ International Atomic Energy Agency (IAEA), Non-serial Publication IAEA-TDL-011, "Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain", Dezember 2022

/IAE22r01/ International Atomic Energy Agency (IAEA), Non-serial Publication IAEA-TDL-011, "Computer Security Approaches to Reduce Cyber Risks in the Nuclear Supply Chain", Dezember 2022

/IBI21w01/ InfraBIM open 2021, “Digital Assets and Cybersecurity: ScredIN from Ingerop”, www.infrabimopen.com, [abgerufen am 04.08.2021]

/IEC15n01/ IEC 62443-2-3, IT-Sicherheit fuer industrielle Automatisierungssysteme, Teil 2-3: Patch management in the IACS environment, 2015

/IIT17w01/ Inside IT, Hans Jörg Maron, CCleaner-Angreifer wollten Tech-Konzerne beklauen, 21. September 2017, www.inside-it.ch/de/, [abgerufen am 13.08.2021]

/IIT21w01/ Inside-IT, Codecov-Breach: So schlimm wie Solarwinds?, 21. April 2021, www.inside-it.ch [abgerufen am 05.09.2021]

/IJR19r01/ R Lakshmi Prasanna Sai, T. Pavan Kumar, “Reverse Engineering the Behaviour of NotPetya Ransomware”, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-7, Issue-6S, March 2019

/ING19r01/ Ingérop, Press Release, Ingerop unveils the successful IN³ Projects and commits to supporting innovative Ideas developed by its Staff, Paris, 20. November 2019

/INS18r01/ Idaho National Laboratory, Kevin E. Hemsley, Dr. Ronald E. Fischer: History of Industrial Control System Cyber Incidents, 2018

/INS23w01/ Anz, P., Inside IT, "Adesso Deutschland verschwieg Cyberangriff lange", 20.04.2023, www.inside-it.ch [abgerufen am 13.10.2023]

/IRW15w01/ Iran Watch, Wisconsin Project on Nuclear Arms Control, Kalaye Electric Company, 15 May 2015, http://www.iranwatch.org [abgerufen am 06.10.2021]

/ISO17n02/ DIN EN ISO/IEC27001, Informationstechnik Sicherheitsverfahren InformationssicherheitsmanagementsystemeAnforderungen(ISO/IEC 27001:2013 einschließlich Cor1:2014 und Cor2:2015), Deutsche FassungENISO/IEC27001:2017, Juni 2017

/ISO17n03/ DIN EN ISO/IEC27002, Informationstechnik - Sicherheitsverfahren - LeitfadenfürInformationssicherheitsmaßnahmen(ISO/IEC27002:2013 einschließlich Cor1:2014 und Cor 2:2015), Deutsche Fassung EN ISO/IEC 27002:2017, Juni 2017

/ITW17w01/ IT World Canada, Solomon, H., "Canadian cyber firm confirms it was the victim described in RSA investigation", 23.02.2017, www.itworldcanada.com

/ITW19w01/ IT Welt, Strom, D., Krokoszinski, J., Was ist Magecart? So stiehlt die Hackergruppe Kreditkartendaten, 07.06.2019, www.itwelt.at

/JAE14r01/ Japan Atomic Energy Agency: „Die Möglichkeit eines Informationsverlustes aufgrund einer Computervirusinfektion“, 2014

/JAT14r01/ Japan Today: “Monju power plant facility PC infected with virus”, Japan, 07.01.2014, www.japantoday.com [abgerufen am 20.12.2023]

/JFR22w01/ JFrog, Malware Civil War Malicious npm Packages Targeting Malware Authors, February 22 2022, www.jfrog.com/blog/malware-civil-war-malicious-npm-packages-targeting-malware-authors [abgerufen am 10.11.2022]

/JFR22w02/ JFrog, Large-scale npm attack targets Azure developers with malicious packages, March 23 2022, www.jfrog.com [abgerufen am 15.11.2022]

/KAS16r01/ Kaspersky Sicherheitsbericht: „Petya ransomware eats your hard drives“, 2016

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

/KAS21w04/ Kaseya, "Updates Regarding VSA Security Incident", Juli 21, www.kaseya.com [abgerufen am 12.12.2023]

/KRE17w01/ KrebsonSecurity, "How to Bury a Major Breach Notification", 21.02.2017, www.krebsonsecurity.com

/LAN19r01/ Paul Lanois: “How to prepare for data breaches? Lessons learned from recent incidents”, Journal of Data Protection & Privacy, Volume 2, Number 3, 2019

/LRL17t01/ LogRythmLabs, The Security Intelligence Company, NotPetya Technical Analysis, July 2017

/MAL21w02/ Malwarebytes Labs, Pieter Arntz, Patch now! Microsoft Exchange is being attacked via ProxyShell, 23. August 2021, www.blog.malwarebytes.com, [abgerufen am 01.12.2021]

/MAN23r02/ Mandiant: 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible, 20 April 2023

/MEN22w01/ MEND, WhiteSource Threat Report Reveals Massive Uptick In Cyberattacks Related To JavaScript npm, 2022, www.mend.io/newsroom/ [abgerufen am 11.11.2022]

/MIC20w04/ Microsoft On the Issues, Brad Smith, A moment of reckoning: the need for a strong and global cybersecurity response, 17 December 2020, https.blogs.microsoft.com [abgerufen am 19.04.2021]

/MIC21w09/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-26855, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w10/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-26857, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w11/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-26858, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w12/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-27065, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w13/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Umgehung von Sicherheitsfunktionen, CVE-2021-31207, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w14/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Rechteerweiterungen, CVE-2021-34523, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w15/ Microsoft, Sicherheitsauffälligkeit in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-34473, www.msrc.microsoft.com [abgerufen am 30.11.2021]

/MIC21w16/ Microsoft, Sicherheitsauffälligkeiten in Microsoft Exchange Server bezüglich Remotecodeausführung, CVE-2021-31206, https://msrc.microsoft.com [abgerufen am 30.11.2021]

/MIT21w02/ MITRE ATT&CK, NotPetya, 23. April 2021, www.attack.mitre.org/software/S0368/, [abgerufen am 10.08.2021]

/MSS17r01/ Microsoft Security: Windows Defender ATP thwarts Operation WilySupply software supply chain cyberattack

/MSS18r02/ Microsoft Security: Poisoned peer-to-peer app kicked off Dofoil coin miner outbreak, 2018

/NCS18i01/ National Cyber Security Centre, Advisory: Hostile state actors compromising UK organisations with a focus on engineering and industrial control companies, April 5, 2018

/NET14w01/ NETRESEC, Full disclosure of Havex Trojans, E. Hjelmvik, www.netresec.com, 27 October 2014 [abgerufen am 15.07.2020]

/NIS15r01/ National Institute of Standards and Technology (NIST), Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations", April 2015

/NIS22r01/ National Institute of Standards and Technology (NIST), Special Publication 800-161r1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations" Rev. 1, Mai 2022

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

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

/NYT18w02/ Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says, March 15, 2018, www.nytimes.com [abgerufen am 5.11.2020]

/NYT20w01/ The New York Times, Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid, October 23, 2020, www.nytimes.com [abgerufen am 3.11.2020]

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

/ONR19r01/ Office for Nuclear Regulation (ONR), NS-TAST-GD-077 Revision 6, "Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services", Juli 2019

/ONR20r01/ Office for Nuclear Regulation (ONR), CNS-TAST-GD-7.1 Revision 1, "EFFECTIVE CYBER AND INFORMATION RISK MANAGEMENT", Maerz 2023

/ONR22r01/ Office for Nuclear Regulation (ONR), CNS-INSP-GD-7.0 Revision 1, "CYBER SECURITY AND INFORMATION ASSURANCE", Januar 2022

/ONR22r02/ Office for Nuclear Regulation (ONR), CNS-INSP-GD-4.0 Revision 1, "NUCLEAR SUPPLY CHAIN MANAGEMENT", Januar 2022

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

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

/RIS18r01/ RiskIQ, Flashpoint, Klijnsma, Y. et al., "Inside Magecart: Profiling the Groups Behind the Front Page Credit Card Breaches and the Criminal Underworld that Harbors Them", 2018

/SAN20w01/ SANS Institute, What You Need to Know About the SolarWinds Supply-Chain Attack, 15 December 2020, www.sans.org [abgerufen am 14.04.2021]

/SEC14r01/ Security Insider: Angriffsmuster der SCAD und ICS-Malware Havex, 2014

/SEC14w02/ Securelist, Kaspersky, Stuxnet: Zero Victims, 11 November 2014, www.securelist.com [abgerufen am 06.10.2021]

/SEC18w01/ Security Affairs, Pierluigi Paganini, Operation Red Signature South Korean Firms victims of a supply chain attack, August 23, 2018, www.securityaffairs.co, [abgerufen am 05.08.2021]

/SEC20w03/ Security Week, SolarWinds Removes Customer List From Site as It Releases Second Hotfix, 16 December 2020 [abgerufen am 17.05.2021]

/SEC22w12/ Security Week, 1,300 Malicious Packages Found in Popular npm JavaScript Package Manager, February 02 2022, www.securityweek.com/ [abgerufen am 10.11.2022]

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

/SEN23r01/ SentinelOneBlog: SmoothOperator, Ongoing Campagin Trojanizes 3CX Desktop App in Supply Chain Attack, 29 March 2023

/SOL21i01/ SolarWinds, Security Advisory, 29 Jan 2021, www.solarwinds.com [abgerufen am 04.03.2021]

/SOP14r01/ Softpedia, “Malware Stole Data from Computer at Japanese Nuclear Power Plant”, 09.01.2014, www.news.softpedia.com [abgerufen am 20.12.2023]

/SOP21w01/ Sophos News, Loman, M. et al., "Independence Day: REvil uses supply chain exploit to attack hundreds of businesses", 04.07.2021, www.news.sophos.com [abgerufen am 12.12.2023]

/SOP22w01/ Sophos News, Wisniewski, C., "Log4Shell: No Mass Abuse, But No Respite, What Happened?", 24.01.2022, www.news.sophos.com [abgerufen am 12.12.2023]

/SPI21w02/ Spiegel, Beuth, P., "Wie loescht man ein brennendes Internet?", 13.12.2021, www.spiegel.de [abgerufen am 12.12.2023]

/SPI21w03/ Spiegel, "Belgisches Militaer von Angriff ueber Sicherheitsluecke Log4j betroffen", 21.12.2021, www.spiegel.de [abgerufen am 12.12.2023]

/STR18r01/ Securonix Threat Research: British Airways Breach: Magecaart Formgrabbing Supply Chain Attack Detection, Oleg Kolesnikov and Harshvardhan Parashar, 2018

/STU21r01/ Radiation and Nuclear Safety Authority (STUK), GUIDE YVL A.12, "INFORMATION SECURITY MANAGEMENT OF A NUCLEAR FACILITY", 12.02.2021

/SUE21w01/ Sueddeutsche Zeitung, "Schwedische Supermarktkette Coop muss 800 Filialen schliessen", 03.07.2021, www.sueddeutsche.de [abgerufen am 12.12.2023]

/SUE23w01/ Sueddeutsche Zeitung, Muth, M., "Wie man nicht auf einen Cyberangriff reagiert", 19.04.2023, www.sueddeutsche.de, [abgerufen am 12.12.2023]

/SYM14r02/ Symantic Enterprise, Dragonfly: Western Energy Companies Under Sabotage Threat, 2014

/SYM17r02/ Symantic Enterprise: Dragonfly: Western energy sector targeted by sophisticated attack group, 2017

/TOR18w01/ Torrentfreak, Van der Sar, E., "Microsoft: Poisoned Torrent Client Triggered Coin Miner Outbreak", 15.03.2018, www.torrentfreak.com

/TRM18w01/ Trend Micro, Operation Red Signature Targets South Korean Companies, August 21, 2018, www.trendmicro.com, [abgerufen am 09.02.2022]

/TRN21w01/ Tremplin Numerique, Codecov gehackt! Was jetzt zu tun ist, wenn Sie Codecov verwenden, 27.04.2021, www.tremplin-numerique.org [abgerufen am 05.09.2022]

/TVE19w01/ The Verge, Sean Hollister, “Asus just patched the ShadowHammer malware that was masquerading as a security update”, 26. März 2019, www.theverge.com, [abgerufen am 09.08.2021]

/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]

/VER16r01/ Meldung eines deutschen Kernkraftwerkes: Virenfund auf IT-Systemen, Deutschland 2016

/VIC19w01/ Vice, Kim Zetter, Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers, 25. März 2019, www.vice.com, [abgerufen am 12.08.2021]

/VOL21w01/ Volexity, Operation ExchangeMarauder: ActiveExploitation of Multiple Zero-Day Microsoft ExchangeVulnerabilities, 02.03.2021, www.volexity.com [abgerufen am 13.06.2022]

/WAP18r01/ Washington Post: Hacker linked to Target data breach gets 14 years in prison

/WIR17r01/ Wired, Andy Greenberg: “The untold Story of NotPetya, the Most Devastating Cyberattack in History”, 2017, www.wired.com [abgerufen am 20.12.2023

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

/WSN21w01/ Web Set Net, Berichten zufolge wurden Hunderte von Netzwerken bei einem Angriff auf die Codecov-Lieferkette gehackt, 20. April 2021, www.websetnet.net/de [abgerufen am 05.09.2022]

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

/ZFK18r01/ Zeitung für kommunale Wirtschaft: „Hacker klauen KRITIS-Daten“, 2018

/ZDN15r01/ ZDNET: Anatomy of the Target data breach: Missed opportunities and lessons learned, 2015

/ZDN21w04/ ZDNet, Everything you need to know about the Microsoft Exchange Server hack, 19.04.2021, www.zdnet.com [abgerufen am 13.06.2022]

/ZDN22w04/ ZDNET, Hundreds more packages found inmalicious npm 'factory', March 28 2022, www.zdnet.com/article/hundreds-more-malicious-packages-found-in-npm-factory [abgerufen am 10.11.2022]

/ZDN22w05/ ZDNET, Angriff auf Azure Entwickler, Boesartige npm-Pakete zielen auf Azure-Entwickler, um persoenliche Daten zu stehlen. Dabei sind Typosquatting und automatische Toolsdie Waffen der Wahl, 24. Maerz 2022, www.zdnet.de [abgerufen am 10.11.2022]

Abbildungsverzeichnis

Abb. 4.1 IT-Grundschutz-Bausteine. /BSI21r05/ 68

Abb. 4.2 Sichtbarkeit, Verständnis und Kontrolle der Lieferkette aus der Sicht eines Unternehmens. /NIS22r01/ 80

Abb. 4.3 C-SCRM im Multilevel Risk Management. /NIS22r01/ 81

Abb. 4.4 CMMC-Ebenen. /DOD20r01/ 86

Abb. 4.5 Übersicht über den Aufbau der Normenreihe 62443. /DIN18n01/ 114

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 978-3-910548-69-5