Untersuchung der Angriffsmöglichkeiten auf IT-Systeme in Kernkraftwerken über Kommunikationssysteme/ -einrichtungen/ -protokolle

GRS - 846

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Untersuchung der Angriffsmöglichkeiten auf IT-Systeme in Kernkraftwerken über Kommunikationssysteme/ -einrichtungen/ -protokolle

Abschlussbericht

Alexander Schug
Oliver Rest

August 2026

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) unter dem Förderkennzeichen 4723R01580 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 BMUKN übereinstimmen.

GRS - 846
ISBN 978-3-911727-39-6

Deskriptoren

Angriffsmöglichkeiten, IT-Sicherheit, kerntechnische Anlagen, Netzwerke, Schwachstellen

Kurzfassung

Seit mehr als 20 Jahren etabliert sich in deutschen kerntechnischen Anlagen für sicherheits- und sicherungsrelevante Aufgaben der Einsatz von Informationstechnik. Neben informationsverarbeitenden Bürosystemen handelt es sich auch um einzelne oder vernetzte leittechnische Systeme und weitere Systeme, die sicherheits- oder sicherungsrelevante Aufgaben übernehmen. Um ihre Aufgaben auszuführen, sind eine Vielzahl dieser Systeme auf eine limitierte oder umfassende Vernetzung und digitale Kommunikation angewiesen, zum einen zwischen den einzelnen Komponenten der Systeme und zum anderen mit anderen Systemen bis hin zur Außenwelt.

Seit vielen Jahren nimmt die Zahl der erkannten Schwachstellen von kommunikationsrelevanter Soft- und Hardware zu, sodass auch eine Betroffenheit von kerntechnisch relevanten Komponenten und Systemen bereits in Bezug auf bekannte, aber auch zukünftige Schwachstellen erwartbar ist. Um die Auswirkungen einer solchen Betroffenheit spezifischer zu erfassen, wurden die sich aus Schwachstellen ergebenden Angriffsmöglichkeiten im Kontext der in kerntechnischen Anlagen eingesetzten Komponenten ermittelt. 280 Schwachstellen mit Relevanz zur Netzwerkkommunikation wurden im Rahmen dieses Ermittlungsverfahrens selektiert. Mögliche Angriffstechniken, welche sich aus diesen Schwachstellen ergeben, wurden eruiert, herausgearbeitet sowie in Bezug zu typischen, generischen IT-Komponenten kerntechnischer Anlagen gesetzt.

Abstract

For more than 20 years, the use of information technology has been established in German nuclear facilities for safety- and security-related tasks. In addition to information-processing office systems, this also includes individual or networked industrial control systems and other systems that perform safety- or security-related tasks. In order to perform their tasks, many of these systems rely on limited or comprehensive networking and digital communication, both between the individual components of the systems and with other systems, including the outside world.

For many years now, the number of identified vulnerabilities in communication-related software and hardware has been increasing, so that nuclear-related components and systems can also be expected to be affected by known and future vulnerabilities. To assess the effects of such an impact more specifically, the attack possibilities resulting from vulnerabilities were determined in the context of the components used in nuclear facilities. 280 vulnerabilities relevant to network communication have been selected as part of this investigation. Possible attack techniques resulting from these vulnerabilities were identified, elaborated and discussed in relation to typical, generic IT components of nuclear facilities.

Inhaltsverzeichnis

1 Einleitung

Eine zentrale Aufgabe der GRS ist die Gewinnung wissenschaftlicher Erkenntnisse im Bereich der Sicherheit und der Sicherung einschließlich der Informationssicherheit von kerntechnischen Anlagen sowie der Entwicklung von Grundlagen auf diesen Gebieten für wissenschaftliche Beiträge zur Fortentwicklung der Sicherheits- und Sicherungsstandards deutscher und internationaler kerntechnischer Anlagen. National und international werden die Regelwerke in Bezug auf die Sicherheit, Sicherung und Informationssicherheit fortwährend mit dem technischen Fortschritt weiterentwickelt und entsprechend eine Verbesserung der Sicherheit, Sicherung sowie Informationssicherheit erreicht. Hierzu sind dauerhaft qualitativ hochwertige, effiziente und zielgerichtete Forschungsarbeiten notwendig, um das kontinuierliche Erreichen des nach Stand der Wissenschaft & Technik (W&T) anforderungsgemäßen sicherheits-, sicherungs- und informationssicherheitstechnischen Niveaus kerntechnischer Anlagen zu ermöglichen. Somit ist ein Ziel der GRS, zur fortwährenden Weiterentwicklung der Sicherheit, Sicherung und Informationssicherheit kerntechnischer Anlagen neben der Erkennung und Darstellung des Standes von Wissenschaft & Technik auch zu dessen Fortschreibung beizutragen.

Seit mehr als 20 Jahren etabliert sich in deutschen kerntechnischen Anlagen für sicherheits- und sicherungsrelevante Aufgaben der Einsatz von Informationstechnik. Neben informationsverarbeitenden Bürosystemen handelt es sich auch um einzelne oder vernetzte leittechnische Systeme und weitere Systeme, die sicherheits- oder sicherungsrelevante Aufgaben übernehmen. In kerntechnischen Anlagen im Ausland ist dieser Etablierungsprozess noch deutlich stärker wahrzunehmen als in Deutschland, dennoch besitzten auch heutige deutsche kerntechnische Anlagen und Einrichtungen typischerweise hunderte verschiedener informationstechnischer Systeme.

Die meisten informationstechnischen Systeme bieten Möglichkeiten zur limitierten oder umfassenden Vernetzung, um ihre Funktionsweisen zu erweitern oder überhaupt erst umfassende Funktionen zu ermöglichen. Um diese Vernetzungen zu realisieren, werden die informationstechnischen Systeme entsprechend mit Soft- und Hardware ausgestattet, welche den Systemen eine direkte Kommunikation untereinander ermöglicht. Eine solche Kommunikation findet über Netzwerkprotokolle basierend auf entsprechenden entwickelten Standards zur digitalen Kommunikation statt. Diese Kommunikation ermöglicht jedoch insbesondere bei einer fehlerhaften Implementierung oder bei bisher nicht erkannten Schwachstellen der Kommunikationsstandards, dass Dritte auf die Kommunikation einwirken.

Da die digitale Kommunikation zum Teil das Tor in die digitale Außenwelt des Internets ist, stehen Schwachstellen und Angriffsmöglichkeiten über die Kommunikation seit einigen Jahren in einem besonderen Fokus von Angreifern. Mit umfassenden Untersuchungen wie Amnesia:33 oder INFRA:HALT wurden hierbei mittlerweile allein von Forescout mit /FOR20r02/, /FOR21r01/, /FOR21r02/ und /FOR21r03/ über dutzende Schwachstellen aufgedeckt, die Millionen oder potenziell Milliarden von digitalen Systemen betreffen.

Grundsätzlich ist eine Übertragbarkeit von entsprechenden kommunikationstechnisch relevanten Schwachstellen auf die in kerntechnischen Anlagen und Einrichtungen eingesetzte digitale Infrastruktur nicht nur nicht auszuschließen, sondern bei der hohen Anzahl an bekannt gewordenen Schwachstellen und betroffenen Systemen realistisch wahrscheinlich. Die Auswirkungen solcher Schwachstellen hängen jedoch insbesondere von der Art und Weise der Nutzung vernetzter digitaler Systeme in kerntechnischen Anlagen und Einrichtungen und deren Grad und Art der Vernetzung ab, wodurch eine direkte Übertragbarkeit der erkannten netzwerktechnischen Schwachstellen und deren Auswirkungen, die z. B. bei industriellen Anlagen und Systemen beobachtet werden, auf kerntechnische Anlagen und Systeme, nur eingeschränkt möglich ist.

Um ein umfassendes Bild möglicher Schwachstellen und deren Auswirkungen auf digitale Systeme in kerntechnischen Anlagen und Einrichtungen zu erhalten, ist daher eine grundsätzliche Untersuchung zu netzwerktechnischen Schwachstellen digitaler Systeme in Bezug auf generische, in kerntechnischen Anlagen typischerweise eingesetzte IT-Komponenten sinnvoll.

In dem vorliegenden Eigenforschungsvorhaben wurden daher anhand bisheriger berichteter netzwerktechnischer Schwachstellen deren Wirkmechaniken aufgezeigt. Anhand von generischen IT-Komponenten kerntechnischer Anlagen und Einrichtungen wurde eine Übersicht erstellt und dargelegt, welche potenziellen Wirkmechaniken auf die entsprechenden übergeordneten IT-Systeme und Prozesse der kerntechnischen Anlagen stattfinden.

2 Stand von Wissenschaft & Technik

Eine elementare Funktion von digitalen Systemen ist die Möglichkeit zur Kommunikation mit weiteren digitalen Netzwerken in einfachen und komplexen Netzwerken. Erst durch diese Kommunikation sind die meisten Systeme in der Lage ihre vorgesehene Funktionsweise auszuführen. So können z. B. Brandmeldesysteme nur dann ordnungsgemäß funktionieren, wenn die entsprechenden Sensoren und manuellen oder automatischen Brandmelder ihre Auslösung an ein entsprechendes Melde- oder Alarmsystem weitergeben. Während früher solche Systeme zumeist analog aufgebaut wurden, bestehen mehr und mehr für kerntechnische Anlagen relevante Systeme aus digitalen Komponenten, die gemeinsam ein digitales System bilden. Eine Brandmeldeanlage besteht daher zumeist aus digitalen Meldern und Sensoren, die ihre Signale an Server weiterleiten, welche anschließend die Signale verarbeiten und dann an Bedienplätze, Alarmsysteme und angeschlossene weitere Systeme weitergeben. Umgekehrt können über die Bedienplätze die Server angesteuert werden und hierrüber wiederum die Konfiguration und Parametrierung der angeschlossenen digitalen Melder und Sensoren bearbeitet werden.

Um eine digitale Kommunikation umzusetzen, sind neben denen physischen Verbindungen der Kommunikationspartner verschiedene Protokolle notwendig um eine geordnete, sichere und wiederkehrende Kommunikationsmöglichkeit zwischen allen Kommunikationspartnern zu gewährleisten. Hierfür wurden im Laufe der technischen Entwicklungen unterschiedliche Kommunikationsprotokolle entwickelt, welche wiederum auf Kommunikationsstandards basieren. Da diese Kommunikationsprotokolle vielfach nur Teile der Aufgaben der digitalen Kommunikation übernehmen, werden im Rahmen der digitalen Kommunikation mehrere Protokolle gleichzeitig verwendet, die unterschiedliche Aufgaben wie beispielsweise die Adressierung der Nachrichten übernehmen.

Um das Zusammenwirken unterschiedlicher Standards zu ermöglichen, wurde 1984 erstmals das ISO-OSI Referenzmodell /KÜV03b01/ entwickelt, welches insgesamt sieben Schichtebenen für die digitale Kommunikation einführt, die als Ebenen der digitalen Kommunikation, deren sichere Versendung, Adressierung, Transport und deren Inhalt sicherstellen. Die Ebenen werden in Abb. 2.1 vollständig dargestellt.

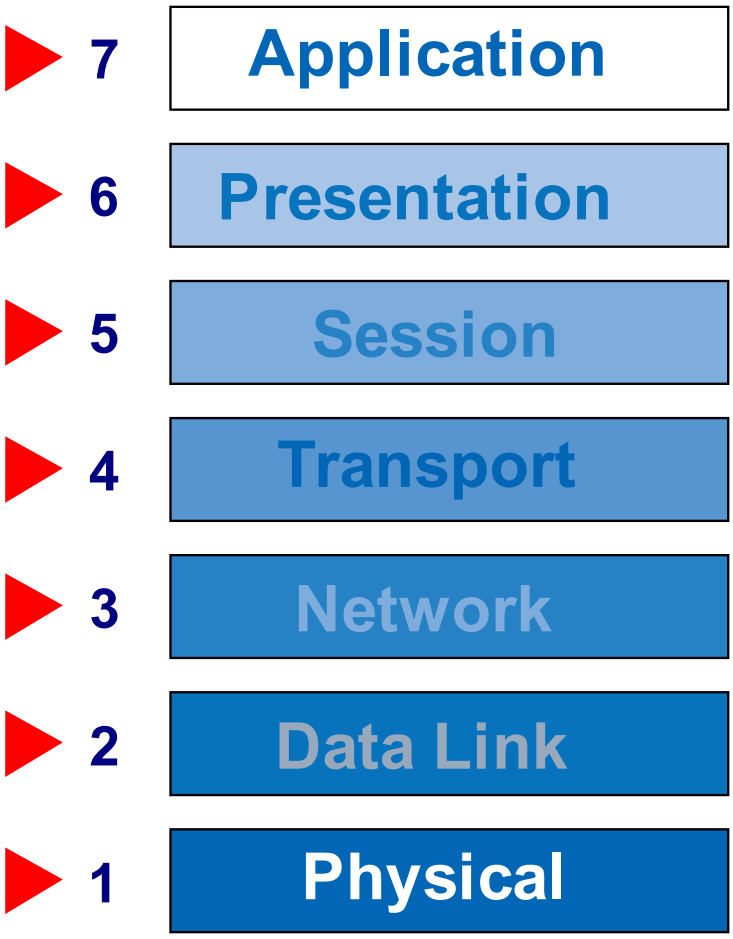

Abb. 2.1 Die sieben Schichten des ISO-OSI Referenzmodells, beginnend auf der physikalischen Ebene bis hin zur Applikationsebene.

Die erste Ebene beschreibt die physikalische Ebene, also den Aufbau von Kabeln, Steckverbindungen und die Netzwerkarchitektur, z. B. als BUS oder Ringnetzwerk. Die zweite Ebene beschreibt die Art und Weise wie Daten verpackt werden und wie Fehler im Netzwerkverkehr erkannt und im Rahmen der Verarbeitung behoben werden. Ethernet ist z. B. als Data Link der Ebene 2 des ISO/OSI Referenzmodells zugeordnet. Die Ebene 3 beschreibt die Adressierung von Kommunikationsnachrichten innerhalb eines Netzwerkes und das durchzuführende Routing zwischen den Kommunikationsteilnehmern. So ist das Internet Protocol (IP) z. B. innerhalb der Ebene 3 angesiedelt und dient der Adressierung von Kommunikationsteilnehmern mit IP-Adressen. Ebene 4 beschreibt den Datentransport, insbesondere in welcher Form Daten innerhalb des Netzwerks ausgetauscht werden und inwieweit der korrekte Datentransport sichergestellt wird. Das Transport Layer Protocol (TCP)dient im Rahmen der modernen Internetkommunikation als Transportprotokoll und wird damit der Ebene 4 zugeordnet.

Die Ebenen 5, 6 und 7 bilden gemeinsam als Ebenen der Sitzung, Präsentation und Applikation eine Applikationsebene, welche entsprechend spezifisch für die verwendeten Anwendungen sind. So ist z. B. https diesen Ebenen zuzuordnen.

Um eine Kommunikation von IT-Systemen zu ermöglichen, sind diese neben der physikalischen Hardware zur Kommunikation mit der entsprechenden Software zur Verarbeitung der Datenkommunikation auszustatten. Zur Verarbeitung von Ethernetkommunikation mittels TCP/IP werden daher z. B. sogenannte TCP/IP Protocol Stacks eingesetzt, also Protokolltürme, welche aufeinander aufbauen. Solche Stacks können von Anbietern kommunizierender digitaler Systeme selbst entwickelt werden, sie werden aber auch kommerziell sowie als freie open source Software angeboten. Insbesondere kommerzielle und freie Software zur Verarbeitung von Netzwerkkommunikation kann hierbei in vielen Unterschiedlichen Systemen und damit bei Millionen oder gar Milliarden unterschiedlichen Anwendung Gebrauch finden.

Kommunikationsstandards bzw. Kommunikationsprotokolle sowie die hierfür genutzte Software können Schwachstellen enthalten, welche für unterschiedliche Formen von Cyberangriffen genutzt werden können. Durch die hohe Verbreitung individueller netzwerkprotokollverarbeitender Software führen Schwachstellen solcher Software umgehend zu einer hohen Anzahl betroffener Systeme, welche gleichzeitig noch mit Netzwerken, häufig dem allgemeinen Internet, verbunden sind und damit Schwachstellen mit Zugriffsmöglichkeiten für Angreifer kombinieren.

Große Aufmerksamkeit erhielten solche Schwachstellen unter anderem durch die Veröffentlichungen des Unternehmens Forescout. So wurde im Jahr 2020 mit Amnesia:33 /FOR20r02/ durch Forescout bekannt, dass sich in sieben weit verbreiteten TCP/IP Stacks 33 bis dahin nicht bekannte Schwachstellen befanden, wovon mindestens vier Schwachstellen Angreifern die Ausführung beliebigen Codes auf den betroffenen Systemen ermöglichen. Forescout veröffentlichte anschließend mit /FOR21r01 bis /FOR21r03/ weitere Untersuchung von TCP/IP Stacks und deren Schwachstellen, sodass innerhalb weniger Jahre mehr als 100 neue netzwerktechnische Schwachstellen nur für TCP/IP verarbeitende Software bekannt wurden.

In kerntechnischen Anlagen und Einrichtungen werden national und international IT-Systeme verwendet, deren IT-Komponenten untereinander wie auch die IT-Systeme selbst, miteinander oder zum Teil mit der Außenwelt vernetzt sind. Entsprechend ist es

vorstellbar, dass durch netzwerktechnische Schwachstellen auch eine Gefahr für Cyberangriffe auf die IT-Systeme kerntechnischer Anlagen und Einrichtungen ausgeht.

3 AP 1: Erfassung von relevanten Schwachstellen der Kommunikation digitaler IT-Systeme

In kerntechnischen Anlagen und Einrichtungen werden eine Vielzahl von unterschiedlichen IT-Komponenten in unterschiedlichsten IT-Systemen mit sicherheits-, sicherungs- und betrieblicher Relevanz eingesetzt. Diese IT-Komponenten bilden typischerweise durch eine Vernetzung basierend auf Kommunikationsstandards ein komplexeres IT-System. Viele IT-Systeme wiederum kommunizieren untereinander. So gibt eine Brandmeldeanlage ihre Alarmmeldungen z. B. an weitere IT-Systeme mit Meldefunktionen weiter, sodass eine installierte Videoeinrichtung automatisch auf den entsprechenden Brandmelder aufschaltet. Da heutige IT-Systeme vielfach keine analoge Kommunikation mehr unterstützten, sind für die Kommunikationsaufgaben in kerntechnischen Anlagen und Einrichtungen mehr und mehr digitale Kommunikationsformen basierend auf modernen digitalen Kommunikationsstandards im Einsatz.

Sowohl die Kommunikationsstandards selbst wie auch die individuelle, die Kommunikation ausführende Soft- und Hardware können dabei von Schwachstellen betroffen sein. Im Arbeitspaket 1 (AP 1) des vorliegenden Vorhabens wurde daher eine Übersicht über die relevanten Standards der digitalen Kommunikation erstellt und zugehörig eine Übersicht über bekannte Schwachstellen digitaler Kommunikation der letzten Jahrzehnte entwickelt.

3.1 Typische genutzte Kommunikationsstandards in kerntechnischen Einrichtungen

In kerntechnischen Anlagen und Einrichtungen werden typischerweise eine Vielzahl unterschiedlicher Kommunikationsstandards verwendet, um die Netzwerkkommunikation digitaler Systeme zu realisieren. Die Verwendung der Standards hängt hierbei von den Anforderungen und Aufgaben der Systeme, dem Alter der Systeme sowie der gewünschten bzw. benötigten Vernetzung der Systeme ab. Im Folgenden werden typischerweise verwendete Kommunikationsstandards kurz vorgestellt.

3.1.1 RS 232

Die RS 232 Schnittstelle ist eine der ältesten Schnittstellen für die Datenübertragung von IT-Systemen. Ursprünglich in den frühen 1960er Jahren entwickelt und standardisiert,

wird diese bis heute in IT-Systemen eingesetzt. Der Standard für die RS 232 Schnittstelle beschreibt die elektrischen Signalcharakteristika, die mechanischen Spezifikationen der Steckverbindung sowie weitere Eigenschaften, jedoch nicht die Bitrate. Als asynchrone serielle Schnittstelle werden die Daten mittels variablen Spannungsintervallen in Paketform übertragen. Die Pakete bestehen aus sogenannten kodierten Zeichen, wobei RS 232 nicht vorgibt, welche Zeichenkodierung genutzt wird.

Am häufigsten wird ASCII verwendet, der weitverbreitetste Zeichencode nach ISO 646. Als physische Steckverbindung wird die RS 232 Schnittstelle dem ersten Level des ISO/OSI-Referenzmodells zugeordnet.

Um mit der Schnittstelle Kommunikation zu ermöglichen, müssen Protokolle eingesetzt werden, die die weiteren Ebenen des ISO/OSI-Referenzmodells umsetzen. Datenübertragungsprotokolle wie Modbus sind in der Lage die RS 232 Schnittstelle zu nutzen, um die entsprechenden Datenübertragungsfunktionen physisch zu realisieren. Darüber hinaus werden vielfach auch eigens entwickelte Protokolle von den Entwicklern von IT-Systemen für die systemspezifische Kommunikation über RS 232 Schnittstellen angewendet.

Die Schnittstelle wird noch heute vielfach als serielle Schnittstelle für einzelne IT-Systeme verwendet, z. B. für Konfigurationen, Steuerung und Parametrierung von industriellen Steuerungssystemen. Darüber hinaus wird RS 232 in einer Vielzahl von IT-Systemen eingesetzt, bei denen aus verschiedenen Gründen auf eine modernere Schnittstelle, wie Ethernet oder USB, verzichtet wird. Als reine serielle Schnittstelle sind entsprechende Protokolle zu nutzen, um mittels der Schnittstelle Daten zu übertragen. Schwachstellen solcher Protokolle ergeben sich aus den entsprechenden Programmierungen der Protokolle, nicht aus der Beschaffenheit der RS 232-Schnittstelle selbst.

3.1.2 Ethernet

Ethernet beschreibt eine Gruppe von Netzwerktechnologien, welche 1974 entwickelt wurde und 1983 erstmalig im Standard IEEE 802.3 festgeschrieben wurde. Ursprünglich wurde Ethernet ähnlich wie BUS-Systeme aufgebaut und entwickelt. Ein von allen IT-Systemen geteiltes Kabel leitet die in Form von Datenblöcken verteilte Kommunikation zu den jeweiligen Empfängern. Für die Kommunikationsverwaltung innerhalb des einzelnen Kabels dient der Carrier Sense Multiple Access/Collision Detection Algorithmus, welcher steuert, dass von den gleichberechtigten angeschlossenen IT-Systemen immer nur

eines zur gleichen Zeit kommuniziert. Angeschlossene IT-Systeme erhalten grundsätzlich sämtliche Kommunikation, verwerfen jedoch die nicht an sie selbst adressierte Kommunikation. Die Kommunikation wird über eindeutig adressierte Datenpakete realisiert, anhand welcher jedes angeschlossene IT-System erkennt, dass es adressiert wurde. Gesendet werden die Daten ausschließlich von den IT-Systemen, wenn diese erkennen, dass aktuell kein anderes IT-System über das Kabel kommuniziert.

Aufgrund der initialen Gestaltung von Ethernet auf Basis eines einzelnen Kabels, war die Ethernet Technologie zu Beginn ihrer Entwicklung eingeschränkt. Es wurden lokale Netzwerke aufgebaut, welche über das Ethernet Kabel miteinander kommunizierten, jedoch wurde die Länge der Kabel sowie die Anzahl der kommunizierenden IT-Systeme durch die Datenübertragungsraten des Kabels eingeschränkt. Je länger das Kabel und je mehr IT-Systeme an der Kommunikation teilnehmen, desto kleiner wurden die erzielten Datenübertragungen. Darüber hinaus wurde jedes Datenpaket jedem Teilnehmer zugestellt, als sogenannte Broadcast (Rundruf) Nachrichten. Die Sicherheit der Kommunikation war hierdurch eingeschränkt und konnte nur durch Verschlüsselungsmethoden verbessert werden.

Mit der Zeit wurde Ethernet fortwährend weiterentwickelt. Die Einschränkungen des BUS-Kabels wurden mittels der Einführung von Switchen überwunden. Hierbei wird der Netzwerkverkehr segmentiert, wobei die einzelnen IT-Systeme an einen oder mehrere Switche angeschlossenen werden und damit die Kommunikation auf die angeschlossenen IT-Systeme des Switches begrenzt wird. Werden die heute etablierten „Twisted-Pair“-Kabel oder Glasfaserkabel genutzt, kann die Broadcast Kommunikation vollständig eingestellt werden, es werden sogenannte Vollduplex-Modi eingesetzt, bei welchen ausschließlich zwei im Netzwerk verbundene Geräte miteinander kommunizieren, die Switches senden dann die entsprechenden Daten direkt zu den einzelnen IT-Systemen anstatt zu allen an einem Switch angeschlossenen IT-System. Die Sicherheit wurde hierbei erhöht, jedoch ist insbesondere die Adressierung im Rahmen der Kommunikation über Ethernet eine Schwachstelle. Den angeschlossenen IT-Systemen wird eine MAC-Adresse als eindeutige Identifikationsmöglichkeit zugeordnet. Diese Adressen lassen sich jedoch auch mittels Spoofing, also das künstlichen Beanspruchen Adresse durch Angreifer, kopieren, was zu falschen Identifikationen und damit falscher Zustellung von Datenpaketen führen kann.

Ethernet ist nach dem ISO/OSI-Referenz Modell ein Level 2 Kommunikationsstandard und regelt die physische Datenübertragung. Jedes von Ethernet übertragene Datenpaket besteht hierbei aus einer Präambel, einem Startblock zur Synchronisation, der Zieladresse, der Absenderadresse, einem Prioritätsblock, einem Typfeld für das nächsthöhere Schichtprotokoll nach ISO/OSI-Referenzmodell (also z. B. IP), den Nutzerdaten, einem Füllfeld, falls die Nutzerdaten nicht die notwendige Größe haben, sowie einer Prüfsumme. Während zu Beginn für die Datenübertragung Koaxialkabel eingesetzt wurden, ist mittlerweile das TIA-568A/B Kabel mit dem RJ-45 Stecker bestehend aus acht parallelen, gebündelten Leitungen weit verbreitet.

Hiermit werde Kabellängen von bis zu 100 Metern, sowie Datenübertragungen mit bis zu 40 Gigabit erreicht. Ethernet-Glasfaserleitungen können im Single Mode, also nur einer Datenübertragungsrichtung, Längen von bis zu 80 km erreichen.

Ethernet ist heute für kabelbasierte Datenverbindungen weit verbreitet und wird sowohl in IT-Netzen von Konsumenten und Unternehmen wie auch in leittechnischen Netzen eingesetzt. Hierbei werden verschiedene höhergruppierte Protokolle für die Datenkommunikation eingesetzt, z. B. IP, TCP oder PROFINET. In der Leittechnik wird mittels dieser Protokolle eine Echtzeitdatenübertragung über Ethernet sichergestellt.

3.1.2.1 TCP/IP

Beim Transmission Control Protocol (TCP) und dem Internet-Protocol (IP) handelt sich um eine aufeinander aufbauende Gruppe von Netzwerkprotokollen, die in den frühen Anfängen des Internets von der amerikanischen DARPA Anfang der 1970er Jahre entwickelt wurden. Für große umfassende Netzwerke wie dem Vorgänger des Internets, dem Arpanet, waren Kommunikationsprotokolle notwendig, die zielgenau Daten über weite Entfernungen und komplexe Netzwerke transportieren konnten. Solche Protokolle standen zu dieser Zeit nicht zur Verfügung und wurden daher mit der Entwicklung großer Netzwerke über große Distanzen hinweg entwickelt. IP übernimmt im Datenverkehr des Internets, aber typischerweise auch lokalen Netzwerken die Adressierung der unterschiedlichen verbundenen IT-Systeme. Jedem einzelnen IT-System in einem Netzwerk, kann eine eindeutige IP-Adresse zugewiesen werden, anhand welcher dieses spezielle IT-System identifiziert werden kann und Daten zu diesem übertragen werden können. TCP dient der Realisierung der Ende-zu-Ende Datenübertragung der entsprechend über

IP adressierten IT-Systeme. Ohne Anwendung von IP können keine TCP basierten Verbindungen aufgebaut werden. Die physikalischen Datenverbindungen werden dann über entsprechende Arten von Datenverbindungen wie Ethernet realisiert.

Durch TCP und IP lassen sich umfassende Netzwerke aufbauen, wie das Internet, großen File-Sharing Netzwerke oder große lokale Netzwerke. Neben TCP werden bei spezifischen Aufgaben wie Echtzeitkommunikation auch weitere Protokolle auf der Transportebene wie UDP oder RTP eingesetzt, welche ebenfalls IP für die Adressierung nutzen.

3.1.2.2 Industrial Ethernet

Industrial Ethernet ist ein Überbegriff für unterschiedliche Kommunikationsstandards, welche auf Ethernet basieren und an die besonderen Herausforderungen von industriellen Anwendungen angepasst wurden. Hierzu zählt insbesondere die echtzeitgesicherte Kommunikation mit Übertragungszeiträumen von 100 µs, weiterhin auch die Absicherung der physischen Kommunikationskomponenten wie Stecker und Anschlüsse in Bezug auf Staub, Vibrationen, Temperaturen oder Feuchtigkeit.

3.1.2.3 BUS over Ethernet

Bus over Ethernet (BoE) bezeichnet die Integration klassischer Feldbussysteme in Ethernet-basierte Netzwerke, um die Vorteile moderner IT-Infrastrukturen in der industriellen Kommunikation zu nutzen. Dabei werden herkömmliche serielle Busprotokolle wie CAN, Modbus oder Profibus (siehe die nachfolgenden Unterkapitel) über Ethernet-TCP/IP übertragen, entweder durch Tunnelung oder durch Protokollkonvertierung. Dies ermöglicht eine höhere Datenrate, größere Reichweiten und eine verbesserte Interoperabilität zwischen Geräten unterschiedlicher Hersteller. BoE trägt zur Konvergenz von IT und OT (Operational Technology) bei und unterstützt die Umsetzung von Industrie-4.0-Konzepten, indem es eine flexible, skalierbare und zukunftssichere Kommunikationsarchitektur schafft.

3.1.2.4 PROFINET

PROFINET, entwickelt von der industriellen Interessengemeinschaft Profibus Nutzerorganisation e.V., ist ein industrielles Ethernet-Standardprotokoll, das für die Echtzeitkommunikation in Automatisierungsnetzwerken entwickelt wurde. Es basiert auf TCP/IP und

Ethernet und ermöglicht die Integration von Steuerungssystemen, Sensoren und Aktoren in eine einheitliche Kommunikationsinfrastruktur. PROFINET unterscheidet sich von klassischen Feldbussystemen durch seine hohe Datenübertragungsrate, flexible Topologie und die Fähigkeit zur Echtzeitkommunikation. Es unterstützt verschiedene Kommunikationsmodelle, darunter PROFINET IO für die zyklische Datenübertragung und PROFINET CBA für komponentenbasierte Automatisierung, wodurch sowohl deterministische als auch nicht-deterministische Datenflüsse effizient gehandhabt werden können.

Ein wesentliches Merkmal von PROFINET ist die Unterstützung von Real-Time (RT) und Isochronous Real-Time (IRT) Kommunikation. RT ermöglicht schnelle Datenübertragung mit geringer Latenz, während IRT für hochpräzise, synchronisierte Prozesse in Motion-Control-Anwendungen eingesetzt wird. Darüber hinaus bietet PROFINET umfassende Diagnosefunktionen, einfache Geräteintegration über GSDML-Dateien und eine hohe Skalierbarkeit für komplexe Automatisierungssysteme. Durch die Kompatibilität mit bestehenden Ethernet-Strukturen und die Unterstützung von Safety- und Security-Erweiterungen trägt PROFINET maßgeblich zur Umsetzung von Industrie-4.0-Konzepten und zur Digitalisierung industrieller Prozesse bei.

3.1.3 Modbus

Modbus ist ein Übertragungsprotokoll, welches in dieser Form erstmalig 1979 etabliert wurde und seitdem kontinuierlich von der Modbus-Organisation verwaltet und weiterentwickelt wird. Modbus unterscheidet sich hierbei zum einen in Modbus RTU sowie Modbus IP.

Modbus RTU nutzt die seriellen Schnittstellen RS 232 sowie RS 485 und wird als Modbus Remote Terminal Unit (RTU) vermarket. Bei der Schnittstelle RS 232 werden Modbus Verbindungen als Punkt zu Punkt Verbindungen etabliert, wobei ein Anschluss als Mastersystem die Führung der Kommunikation (zumeist ein Controller oder Computer) übernimmt und das andere System als Slave entsprechend angesteuert wird (zumeist ein Feldgerät). Die Kommunikation über Modbus wird hierbei in der Art aufgebaut, dass das Master-System wiederholt Lese- und Schreibanfragen an die angeschlossenen Systeme schickt und darüber jedes Einzelsystem individuell ansteuert.

RS 232 und RS 485 Schnittstellen und damit Modbus RTU unterstützen ausschließlich die Kommunikation mittels Binärcode, wobei jeweils ein Byte in der Kommunikation für

die Adressierung und die Funktion und zwei Byte für die Redundanzprüfung aufgewendet werden.

Demgegenüber steht das seit 2007 verwendete Modbus TCP auf Basis der Ethernet Schnittstelle. Hierbei wird die Ethernet-Schnittstelle verwendet und basierend auf dem Transmission Control Protocol (TCP) sowie dem Internet Protocol (IP) die Netzwerkarchitektur des Modbus TCP Netzwerks aufgebaut. Dadurch wird anstatt eines Masters die Verwendung mehrerer steuernder Zentralgeräte ermöglicht. Diese steuern Clients an, welche die Feldgeräte ansteuern. Modbus TCP über Ethernet erreicht deutlich höhere Übertragungsraten als Modbus RTU und ermöglicht die Nutzung klassischer Ethernet-basierter Hardware sowie die Adressfindung für die Kommunikation.

Im ISO/OSI Referenzmodell ist Modbus auf der höchsten, der siebten Schicht als Applikation eingeordnet. Abhängig ist Modbus RTU allein von den Schichten der physischen Verbindung über die RS 232 bzw. RS 485 Schnittstelle sowie dem Datenlink, welcher als Ebene zwei des Referenzmodells durch die serielle Master Slave Kommunikation dargestellt wird. Modbus TCP nutzt für die physikalische Ebene sowie die Datenverbindungsebene Ethernet entsprechend ISO 8802-3 sowie für die Netzwerkebene das IP. Mittels Modbus TCP, einer Form des TCP-Protokolls, wird der Datentransport im Ethernet-Netzwerk ausgeführt.

Modbus ist in der Automatisierungstechnologie weit verbreitet und gilt als einfaches Kommunikationsprotokoll zur Vernetzung von Feldgeräten und anderen Systemen auf der Automationsebene. Während Modbus RTU insbesondere bei älteren industriellen Steuerungssystemen weit verbreitet ist, wird Modbus TCP bei neueren Systemen integriert und verwendet. Modbus gilt als kostengünstig für die Integration in entsprechende Systeme, sodass dieses Protokoll weiterhin in hoher Zahl verwendet wird.

Aufgrund des Alters, aber auch weil Modbus als Kommunikationsprotokoll zu den Feldgeräten insbesondere Wert auf Verlässlichkeit und Verfügbarkeit legt, fehlen Modbus RCU und auch älteren Versionen von Modbus TCP viele etablierte Sicherungsmaßnahmen. Dabei sind die fehlenden Sicherungsmaßnahmen keine Schwachstellen im herkömmlichen Sinne, bieten jedoch auch für IT-Angreifer Funktionalitäten, die im Einwirkungsfall genutzt werden können. Darüber hinaus werden immer wieder Schwachstellen in IT-Systemen bekannt, welche auf fehlerhafter Programmierung der Modbus-Integrität der Systeme basieren. Bei der Integration von Modbus-Funktionalitäten können Fehler auftreten, welche sich dann als Schwachstellen im Endsystem wiederfinden.

Darüber hinaus ist vielfach eine Übertragung von einem Protokoll zu einem anderen vorgesehen.

Sogenannte Protokollgateways dienen der Übersetzung von einem Protokoll in ein anderes, wobei insbesondere herstellerspezifische Kommunikationsprotokolle in allgemein verwendbare Protokolle übertragen werden. Verschiedenste Modbus Protokollgateways sind in den vergangenen Jahren durch Schwachstellen aufgefallen.

3.1.4 CAN-Bus

Der CAN-Bus ist ein serielles Kommunikationsprotokoll, das ursprünglich für die Automobilindustrie entwickelt wurde, um die Kommunikation zwischen elektronischen Steuergeräten (ECUs) zu ermöglichen. Es zeichnet sich durch eine hohe Fehlertoleranz, Echtzeitfähigkeit und ein dezentrales Kommunikationsmodell aus. Die Datenübertragung erfolgt über ein Mehrmaster-System, bei dem alle Teilnehmer gleichberechtigt sind und Nachrichten prioritätsbasiert senden können. Durch die Verwendung eines nichtadressierten Nachrichtenformats mit Identifyern wird eine flexible und effiziente Kommunikation ermöglicht, die besonders für sicherheitskritische Anwendungen geeignet ist.

Technisch basiert der CAN-Bus auf einem differenziellen Zweidrahtsystem, das eine robuste Datenübertragung auch in elektromagnetisch belasteten Umgebungen erlaubt. Die maximale Datenrate beträgt bis zu 1 Mbit/s (bei klassischem CAN), wobei moderne Erweiterungen wie CAN FD (Flexible Data Rate) höhere Datenmengen und dynamische Datenlängen unterstützen. CAN findet heute nicht nur im Fahrzeugbau Anwendung, sondern auch in der Industrieautomatisierung, Medizintechnik und Luftfahrt. Die einfache Implementierung, geringe Kosten und hohe Zuverlässigkeit machen den CAN-Bus zu einem weit verbreiteten Standard für eingebettete Systeme und verteilte Steuerungsarchitekturen.

3.1.5 PROFIBUS

Process Field Bus (PROFIBUS) ist ein weit verbreitetes Feldbusprotokoll zur seriellen Datenübertragung in der industriellen Automatisierung. Es wurde in den 1980er Jahren entwickelt und ermöglicht die Kommunikation zwischen Steuerungen, Sensoren und Aktoren über ein einheitliches Bussystem. PROFIBUS basiert auf dem Master-Slave-Prinzip und unterstützt sowohl zyklische als auch azyklische Datenübertragung. Die bekanntesten Varianten sind PROFIBUS-DP (Decentralized Peripherals) für die schnelle

Kommunikation mit dezentralen Geräten und PROFIBUS-PA (Process Automation) für den Einsatz in prozessnahen Anwendungen mit besonderem Fokus auf Sicherheit und Energieeffizienz.

Technisch nutzt PROFIBUS eine RS-485- oder MBP-physikalische Schnittstelle und erreicht Datenraten von bis zu 12 Mbit/s (bei DP). Die Kommunikation erfolgt deterministisch, was eine präzise Steuerung zeitkritischer Prozesse ermöglicht. PROFIBUS bietet umfangreiche Diagnosefunktionen, automatische Geräteerkennung und eine hohe Störfestigkeit, wodurch sich das Protokoll besonders für raue industrielle Umgebungen eignet.

Die Anwendungsfelder von PROFIBUS sind vielfältig und reichen von der Fertigungsautomatisierung über die Prozessindustrie bis hin zur Gebäudeautomation. In der diskreten Fertigung wird PROFIBUS-DP häufig zur Anbindung von Sensoren, Ventilen und Antrieben eingesetzt, während PROFIBUS-PA in chemischen und pharmazeutischen Anlagen sowie in der Energieerzeugung verwendet wird, wo explosionsgeschützte und zuverlässige Kommunikation erforderlich ist. Trotz der zunehmenden Verbreitung von Ethernet-basierten Protokollen wie PROFINET bleibt PROFIBUS aufgrund seiner Robustheit und breiten Geräteunterstützung ein relevanter Standard in bestehenden und hybriden Automatisierungslösungen.

3.1.6 OPC

OPC ist ein herstellerunabhängiger Kommunikationsstandard, der den Datenaustausch zwischen verschiedenen Automatisierungssystemen und Softwareanwendungen ermöglicht. Ursprünglich als Schnittstelle für die Anbindung von Prozessdaten an Visualisierungs- und Leitsysteme entwickelt, basiert OPC auf einer Client-Server-Architektur und verwendet standardisierte Schnittstellen zur Übertragung von Echtzeitdaten, Alarmen und historischen Informationen.

Die Anwendungsfelder von OPC sind vielfältig und reichen von der Fertigungs- und Prozessautomatisierung über die Energie- und Gebäudetechnik bis hin zur Medizintechnik und Logistik. OPC wird insbesondere dort eingesetzt, wo Daten aus unterschiedlichen Quellen konsolidiert und in übergeordnete Systeme wie SCADA, MES oder ERP integriert werden müssen. Durch die Fähigkeit zur semantischen Beschreibung von Daten und zur sicheren Kommunikation über Firewalls und Netzgrenzen hinweg spielt OPC UA

eine zentrale Rolle in der Umsetzung von interoperablen und vernetzten Produktionssystemen.

Die breite Unterstützung durch Industrieunternehmen und die kontinuierliche Weiterentwicklung machen OPC zu einem Schlüsselstandard für die digitale Transformation in der industriellen Kommunikation.

3.1.6.1 OPC-UA

Die Weiterentwicklung von OPC (mittlerweile häufig als OPC Classic bezeichnet) zu OPC Unified Architecture (OPC UA) hat den Standard plattformunabhängig, skalierbar und sicher gemacht, wodurch er sich für moderne Industrie-4.0-Anwendungen eignet. OPC UA nutzt ein serviceorientiertes Architekturmodell (SOA) und unterstützt sowohl binäre als auch webbasierte Protokolle, was eine flexible Integration in IT- und OT-Systeme erlaubt.

3.1.7 IO-Link

IO-Link ist ein weltweit standardisiertes Punkt-zu-Punkt-Kommunikationsprotokoll (IEC 61131-9), das für die Anbindung intelligenter Sensoren und Aktoren an Automatisierungssysteme entwickelt wurde. Im Gegensatz zu klassischen digitalen Ein-/Ausgangssignalen ermöglicht IO-Link die bidirektionale Kommunikation über eine standardisierte, ungeschirmte Dreidrahtleitung. Dadurch können nicht nur Prozessdaten, sondern auch Diagnose- und Parameterdaten übertragen werden. IO-Link arbeitet auf der untersten Ebene der Automatisierungspyramide und stellt eine wichtige Schnittstelle zwischen der Feld- und Steuerungsebene dar. Die einfache Integration, automatische Geräteerkennung und die Möglichkeit zur zentralen Parametrierung tragen zur Reduzierung von Inbetriebnahmezeiten und Wartungsaufwand bei.

Die Anwendungsfelder von IO-Link sind vielfältig und reichen von der diskreten Fertigung über die Verpackungsindustrie bis hin zur Prozessautomatisierung. Besonders in modularen Maschinenkonzepten und flexiblen Produktionssystemen bietet IO-Link Vorteile. Die kontinuierliche Überwachung von Sensorzuständen und die Übertragung von Zustandsdaten ermöglichen eine vorausschauende Wartung (Predictive Maintenance) und verbessern die Anlagenverfügbarkeit. In Kombination mit IO-Link-Mastern und Gateways lässt sich die Technologie nahtlos in übergeordnete Systeme wie SPS, SCADA oder MES integrieren und unterstützt damit die Umsetzung von Industrie-4.0-Strategien.

3.2 Bekanntgewordene kommunikationsrelevante Schwachstellen

Schwachstellen von IT-Systemen, Software, Standards oder anderen datentechnisch relevanten Objekten treten in einer Vielzahl von Formen und Varianten auf und werden für unterschiedlichste Systeme, Software, Betriebssysteme, Geräte und Protokolle jedes Jahr bekannt. Seit 25 Jahren hat sich in diesem Zusammenhang das Common Vulnerabilities and Exposures (CVE) System zur einheitlichen Dokumentation und Klassifizierung öffentlich bekannt gewordener Schwachstellen etabliert /CVE25w01/. Jede bekannte Schwachstelle erhält ein individuelles Kürzel, bestehend aus dem Namen CVE, der Jahreszahl der Entdeckung und einer fortlaufenden Nummer, mit der alle dokumentierten Schwachstellen eines Jahres fortlaufend durchnummeriert werden.

Im Rahmen der zugehörigen CVE-Datenbasis werden somit sämtliche seit 25 Jahren gemeldeten Schwachstellen eindeutig identifiziert und gelistet. Zu den Listungen zugeordnet werden das Publikationsdatum, eine kurze Beschreibung der Schwachstelle, der betroffene Anbieter, das betroffene Produkt, die betroffenen Versionen des Produkts, eine Kreditierung der Melder/Entdecker der Schwachstelle, Referenzen wie Herstellermeldungen sowie einer Schwachstellenbewertung entsprechend des Common Vulnerability Scoring System (CVSS) verwendet. Das CVSS ermöglicht eine schnelle Übersicht über den gesamten potenziellen Impakt einer Schwachstelle, in dem es aus verschiedenen Faktoren einen Schweregrad der Schwachstellen von 1 (sehr leicht) bis 10 (kritisch) erzeugt. Als Faktoren werden unterschiedliche Aspekte einbezogen, z. B. die grundsätzlichen sich ergebenden Möglichkeiten der Schwachstelle wie die Remote Code Execution (RCE) oder Denial of Service (DoS), eine Bewertung der für die Ausnutzung notwendiger komplexer oder einfacher Angriffsschritte, der Beteiligung von Nutzern an der Ausnutzung sowie z. B. die benötigte Authentifizierungsstufe bei Ausnutzung der Schwachstelle. Der sich somit ergebende Score ermöglicht eine einfache, schnelle und vergleichbare Bewertung der Schwere der Schwachstelle.

Die Anzahl gemeldeter Schwachstellen über das CVE-System steigt seit Jahren kontinuierlich an. Im Jahr 2014 musste die Nomenklatur angepasst werden, sodass 5-stellige fortlaufende Nummern an Schwachstellen vergeben werden konnten. Im Jahr 2024 wurden erstmalig mehr als 40.000 Schwachstellen, ein Anstieg von 37 % zu 2023 gemeldet.

Grundsätzlich sind Schwachstellen, welche direkt kommunikationstechnische Standards betreffen, zumeist historisch bedingt. Die ist einerseits dadurch begründet, dass Funktionalitäten sich als missbrauchsfähig herausgestellt haben, und andererseits weil im

Rahmen der Entwicklung von Standards heute etablierte Sicherungsmaßnahmen nicht bedacht oder nicht verfügbar waren. So sind unverschlüsselte Nachrichten, welche über TCP übersendet werden, durch Packet Sniffing sehr einfach auszulesen. Dies ergibt sich aus der grundlegenden Funktionalität von TCP, in deren Rahmen Nachrichtenpakete übertragen werden. Die meisten Kommunikationsprotokolle, insbesondere solche, welche historisch gewachsen sind für das Internet oder für industriellen Nutzen, wurden nicht unter den Gesichtspunkten der Cybersicherheit entwickelt, sondern unter den Gesichtspunkten der Funktionalität und Praktikabilität.

Kommunikationsprotokolle bzw. Kommunikationsstandards müssen durch Software auf jedem kommunizierenden System einzeln umgesetzt werden. Wurden ausnutzbare Schwachstellen in Kommunikationsprotokollen erkannt, können daher Maßnahmen bzw. Lösungen etabliert werden, welche die Schwachstellen absichern: verschlüsselte Nachrichten können nicht im Rahmen von Packet Sniffing ausgelesen werden; vorgeschriebene Authentifizierungsmechanismen von kommunizierenden Partnern ermöglichen es unerwünschte Kommunikationsteilnehmer und Spoofing zu unterbinden.

Schwachstellen, welche die digitale Kommunikation betreffen, sind zumeist Schwachstellen in den entwickelten Softwarelösungen zur Abwicklung der Kommunikation, wie z. B. TCP/IP Stacks, mit welchen die Protokolle TCP und IP abgewickelt werden. Hierbei kann es sich z. B. um die nicht korrekte Implementierung etablierter Praktiken zur Absicherung der Kommunikation über die betroffenen Standards handeln, oder grundlegende programmiertechnische Fehler, welche von Angreifern ausgenutzt werden. Dokumentierte Schwachstellen mit Relevanz für die zugehörigen kommunikationstechnischen Standards betreffen daher in den meisten Fällen nicht sämtliche diesen Standard nutzende Systeme, sondern die spezifischen Softwarelösungen, mit welchen die Standards tatsächlich umgesetzt werden. Je nach Verbreitungsgrad dieser umsetzenden Softwarelösungen können die Schwachstellen wie bei Amnesia:33 potenziell Milliarden Systeme betreffen oder nur wenige einzelne.

Um Schwachstellen mit Relevanz für die digitale Kommunikation und damit das vorliegende Vorhaben zu erkennen, wurde daher im Rahmen des Vorhabens auf die Suchfunktionen der CVE-Datenbank bzw. weiterer auf der CVE-Datenbank aufbauender Datenbanken ebenso zurückgegriffen wie auch auf allgemein mit großer Aufmerksamkeit bekannt gewordene kommunikationsrelevante Schwachstellen wie AMNESIA:33.

So ergab sich für das vorliegende Vorhaben eine Datenbasis von knapp 300 Schwachstellen die digitale Kommunikation betreffend, welche eine Relevanz aufzeigen und zur Bearbeitung in Arbeitspaket 1 herangezogen wurden (siehe Tab. 3.1).

Tab. 3.1 Übersicht genutzter Schwachstellen in Bezug zur digitalen Kommunikation

Kommunikationsstandard	**Anzahl im Vorhaben bestimmter relevanter Schwachstellen**	**Kritische Schwachstellen**
TCP/IP	96	14
Profinet	39	0
Modbus	81	18
Modbus TCP	22	2
Industrial Ethernet	15	0
OPC UA	1	0
IEC 60870-5-104	3	0
Unspezifisch Ethernet	22	4
Insgesamt	280	38

3.3 Zusammenfassung AP 1

Im Rahmen der Arbeiten zum Arbeitspaket 1 wurde eine Übersicht der wichtigsten und bekanntesten digitalen Kommunikationsstandards dargelegt, welche grundsätzliche Relevanz für das vorliegende Vorhaben besitzen. Unter Anwendung dieser Standards wurden im nächsten Schritt die CVE-Datenbank auf Schwachstellen mit Relevanz für die digitale Kommunikation ausgewertet, wobei insgesamt knapp 300 Ereignisse ausgewertet wurden. Mit den Arbeiten zum Arbeitspaket 1 wurde somit eine umfassende Datenbasis erstellt, welche die Grundlage der Auswertung von Angriffsmöglichkeiten auf digitale Kommunikation, in den nachfolgenden Arbeitspaketen bildet.

4 AP 2 Auswertung der sich aus Kommunikationsschwachstellen ergebenden Angriffsmöglichkeiten

Die gesammelten Schwachstellen in AP 1 beschreiben grundsätzliche Schwachstellen in der Programmierung oder in der anderweitigen digitalen Kommunikation. Für Angriffe über oder auf die digitale Kommunikation können diese Schwachstellen ausgenutzt werden. Hierbei können die in den Blick genommenen Schwachstellen sich in unterschiedlichen Wirkmechaniken unterscheiden, auf deren Basis die Ausnutzung der Schwachstellen möglich ist. So kann ein Programmierfehler dazu führen, dass ein Programm sich in eine unendlich wiederholende Berechnungsschleife begibt, wodurch das Programm in der Konsequenz immer mehr Rechenressourcen benötigt und schließlich das Gesamtsystem überlastet. In der digitalen Kommunikation kommen z. B. sehr oft Schwachstellen vor, bei denen bestimmte Parameter nicht ausreichend verifiziert werden. Während die meisten Kommunikationsstandards Länge und/oder Form übersendeter Datenpakete fest definieren, können Schwachstellen dazu führen, dass die die Kommunikation verarbeitenden Programme, die eingehende Länge und Form der Datenpakete nicht prüfen. In der Konsequenz können Angreifer mit manipulierten Datenpaketen nicht vorgesehener Länge oder Form unvorhergesehene Aktionen in den betroffenen Programmen und damit den betroffenen kommunizierenden Systemen verursachen.

4.1 Common Weakness Enumeration für Klassifizierung von Schwachstellen

Seit 2006 wurde von Freiwilligen ein System zur Kategorisierung und systematischen Beschreibung von Schwachstellen entwickelt, welches als Common Weakness Enumeration (CWE) System bekannt ist. Mittels CWE werden Schwachstellen typisiert und damit eindeutig in ihrer Wirkweise beschrieben. Mittlerweile sind mehr als 900 verschiedene CWE-Nummern für die Typisierung von Schwachstellen vergeben worden und das CWE-Projekt wird finanziell von US-Regierungsbehörden maßgeblich finanziert.

Typischerweise werden allen erkannten und gemeldeten Schwachstellen eine entsprechende CWE-Nummer für die Typisierung der Schwachstelle zugeordnet, entweder durch die Melder der Schwachstelle oder durch die Meldeplattform. Älteren CVE-Nummern können durch die Schwachstellenbeschreibungen CWE-Nummern und damit Schwachstellentypen zugeordnet werden. Die Typisierung von Schwachstellen ermöglicht darüber hinaus eine schnelle Übersicht über die sich aus der Schwachstelle

potenziell ergebenden Angriffsmöglichkeiten bei Ausnutzung der Schwachstellen. Je nach Schwachstellentyp können sich unterschiedliche Angriffsmöglichkeiten mit jeweils unterschiedlichen Auswirkungen auf das betroffene Gesamtsystem ergeben.

4.2 Angriffsmöglichkeiten durch Schwachstellen in der Kommunikation

Die im Arbeitspaket 1 erkannten Schwachstellen lassen sich nach den entsprechenden zugehörigen CWE-Nummern und damit Typen von Schwachstellen kategorisieren. Mittels der CWE-Nummern wiederum ergeben sich anschließend die hieraus möglicherweise zugehörigen resultierenden Angriffsmöglichkeiten. Die im Rahmen des Vorhabens wesentlichen CWEs werden im Folgenden kurz zusammengefasst.

4.2.1 Improper Input Validation

Beschreibung

Länge des IP-Felds (Header und Daten-Länge) kann durch Senden eines IP-Pakets über das Netzwerk ein Integer Overflow herbeigeführt werden, der Verfügbarkeit, Vertraulichkeit und Integrität beeinflussen kann.

Die Schwachstelle *Improper Input Validation* (CWE-20) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, die im Zusammenhang mit einer unzureichenden Prüfung von Eingaben oder Daten stehen. Dabei werden Eingaben oder Daten erfasst, aber nicht, nicht vollständig oder fehlerhaft validiert, sodass nicht sichergestellt ist, dass sie die entsprechenden Eigenschaften besitzen, die für eine sichere und korrekte Verarbeitung erforderlich sind. Die Ursache dieser Schwachstelle liegt typischerweise in der unzureichenden Implementierung sicherheitsarchitektonischer Anforderungen.

Während erste digitale Kommunikationsstandards oft noch mit der Erwartung sich konform verhaltender Teilnehmer entwickelt wurden, werden in modernen Systemen zur Sicherung der Kommunikation und Systeme alle Eingaben automatisiert auf potenzielle Gefahren für die jeweilige Software geprüft, um sicherzustellen, dass die Eingaben für die Verarbeitung innerhalb des Codes oder für die Kommunikation mit anderen Komponenten sicher sind und nicht zu unerwünschten Ergebnissen führen.

Ist dies nicht der Fall, können Angreifer dies ausnutzen und Eingaben erzeugen, die von der Software nicht beabsichtigt und erwartet sind, sodass es zu unbeabsichtigten Funktionen kommen kann, wie beispielsweise der illegitimen Nutzung einer Ressource oder einer illegitimen Ausführung von beliebigem Code. Von der Schwachstelle betroffen sein können sowohl Rohdateneingaben (z. B. Strings, Zahlen) wie auch Metadateneingaben (z. B. Informationen über Daten wie deren Größe oder Header). Dabei kann die unzureichende Validierung verschiedenste Parameter betreffen wie Größen- oder Längenparameter, Indizes, logische Elemente, kryptografische Signaturen oder sonstige Eingaben.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer können durch nicht validierte, unerwartete Eingaben nicht dafür vorgesehene Speicherelemente und somit Dateien oder Verzeichnisse auslesen und haben ggf. Zugriff auf vertrauliche Informationen.
- Denial of Service: Angreifer können durch die Übermittlung nicht validierter, unerwarteter Eingaben Systeme zum Absturz bringen, neu starten, beenden oder einen übermäßigen Verbrauch von Ressourcen wie Arbeitsspeicher und Prozessorleistung herbeiführen.
- Modify Memory & Remote Code Execution: Durch die Übermittlung nicht validierter, unerwarteter Eingaben können Angreifer nicht dafür vorgesehene Bereiche des Speichers ändern und nicht autorisierten Code oder Befehle ausführen.

Bekanntgewordene Schwachstellen

- CVE-2020-11901: Aufgrund nicht adäquater Input-Validierung kann durch Beantwortung einer DNS-Anfrage eines Geräts auf eine bestimmte Weise beliebiger Code ausgeführt werden.
- CVE-2021-31401: Aufgrund nicht adäquater Input-Validierung im Zusammenhang mit dem TCP-Header bezüglich der Länge des IP-Felds (Header und Daten-Länge) kann durch Senden eines IP-Pakets über das Netzwerk ein Integer Overflow herbeigeführt werden, der Verfügbarkeit, Vertraulichkeit und Integrität beeinflussen kann.
- CVE-2020-17439: Durch eine unzureichende Prüfung eingehender und ausgehender DNS-Anfragen kann ein DNS-Cache-Poisoning herbeigeführt werden, bei dem

manipulierte DNS-Einträge im Cache des DNS-Resolvers eingegeben werden, sodass Server falsche Antworten auf Anfragen geben und Datenverkehr gezielt auf Systeme der Angreifer umgeleitet werden kann (ermöglicht beispielsweise Man-in-the-Middle-Angriffe).

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs *Improper Input Validation* sind in den meisten Fällen keine Authentifizierungsmechanismen erforderlich. Dabei müssen Angreifer entsprechende Eingaben in Form von Roh- oder Metadaten an Systeme senden, welche keine ausreichende Überprüfung der Eingaben durchführen. Um einen solchen Angriff auszuführen, muss der Angreifer somit lediglich in der Lage sein, eine Kommunikationsverbindung zum betroffenen System aufzubauen. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.2 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Beschreibung

Unter der CWE-Nummer CWE-120 werden allgemein solche Schwachstellen bzw. auf diesen basierenden Angriffstechniken verstanden, welche im Zusammenhang oftmals nicht anforderungsgerechter Überprüfung von Ein- und Ausgabeparametern und somit der Überschreitung der Kapazität eines Zielpuffers stehen.

Grundsätzlich gibt es innerhalb der gängigen Programmiersprachen feste Speicherbereiche (Buffer) für Daten, die eine bestimmte Länge aufweisen. Wenn Daten, die in einen bestimmten Bereich geschrieben werden sollen, eine größere Länge als der Speicherbereich besitzen, werden benachbarte Speicherbereiche innerhalb des Arbeitsspeicher-

prozesses überschrieben, sodass dort vorhandene, ggf. wichtige Informationen überschrieben werden. Dies kann ein Angreifer gezielt ausnutzen, indem er Eingaben derartig präpariert, dass sie nicht nur die vorgesehenen Speicherbereiche füllen, sondern auch angrenzende Speicherbereiche überschreiben und dadurch ggf. Programme abstürzen lassen oder dass auch eigener Code ausgeführt wird. Insgesamt ergeben sich dadurch mögliche schadhafte Auswirkungen auf die Verfügbarkeit, Vertraulichkeit und Integrität von Systemen und Informationen.

Buffer-Overflows können eine Vielzahl von Folgen für das betroffene System aufweisen, wenn keine oder nicht ausreichende Maßnahmen zur Überprüfung von Eingangsparametern in Bezug auf deren Länge getroffen werden. Grundsätzlich sind bei Manipulation solcher Schwachstellen eine Vielzahl von Konsequenzen bekannt geworden:

- Denial of Service: Buffer-Overflows führen vielfach zu Programm- und Systemabstürzen, z. B. wenn durch illegitim geschriebene Daten außerhalb des vorgesehenen Speicherbereichs, andere relevante Daten, die zur ordnungsgemäßen Ausführung relevanter Programme wichtig sind, überschrieben werden.
- Integrität: Angreifer können durch Buffer-Overflows in andere Speicherbereiche als ursprünglich für die legitime Ausführung vorgesehen schreiben und somit die Integrität des Systems beeinflussen.
- Arbitrary Code Execution: Angreifer können durch die Übermittlung eigenen Codes und der Forcierung der Speicherung dieses Codes in nicht dafür vorgesehene Bereiche, eine Ausführung erzwingen und somit unter bestimmten Umständen beliebigen Code ausführen.

Bekanntgewordene Schwachstellen

- CVE-2020-7559: Durch eine unzureichende/fehlende Implementierung der Überprüfung der Inputlänge beim Kopieren kommt es zu einem Buffer-Overflow, wodurch Angreifer einen Absturz des betroffenen PLCs herbeiführen können.
- CVE-2020-24336: Durch eine unzureichende Prüfung der Adresslänge kann es beim Kopieren von Daten beliebiger Länge zu einem Buffer-Overflow kommen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über die Schwachstellen des Typs Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') sind grundsätzlich keine Authentifizierungsmechanismen notwendig. Die Schwachstellen dieses Typs resultieren auf einer unzureichenden Prüfung von Inputparametern. Je nach Schwachstelle sind vielfach keine vorhergehenden Angriffsschritte zur Ausführung eines Angriffes notwendig. Im Kontext von Schwachstellen von Netzwerkprotokollen sind hierbei lediglich direkte Zugriffe über dauerhafte oder temporäre Netzwerkverbindungen notwendig.

4.2.3 Out-of-bounds Read

Beschreibung

Die Schwachstelle *Out-of-bounds Read* (CWE-125) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, die im Zusammenhang mit dem Auslesen von Daten außerhalb des vorgesehenen Speichers stehen. Dabei können Angreifer durch Ausnutzung dieser Schwachstelle im Wesentlichen unberechtigt Informationen aus nicht vorgesehenen Speicherbereichen lesen oder Abstürze verursachen. Ein Absturz kann dabei unter anderem auftreten, wenn variable Datenmengen eingelesen werden und dabei ein Sentinel-Wert (spezieller Wert im Kontext eines Algorithmus, der sein Vorhandensein als Beendigungsbedingung verwendet, typischerweise in einer Schleife oder einem rekursiven Algorithmus) erwartet wird, der außerhalb des dafür vorgesehenen Bereichs liegt. Dabei werden gegebenenfalls zu viele Daten eingelesen, was zu einem Segmentierungsfehler (segmentation fault) oder Pufferüberlauf (buffer overflow) führen kann. Die Ursache dieser Schwachstelle liegt typischerweise in der unzureichenden Implementierung sicherheitsarchitektonischer Anforderungen. Maßnahmen zur Mitigation derartiger Schwachstellen sind beispielsweise die Implementierung einer angemessenen Inputvalidierung, sodass Eingaben, die potenziell Out-of-bounds Read Schwachstellen ausnutzen könnten, unterbinden.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer somit eine Verletzung der Verfügbarkeit und Vertraulichkeit bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Durch das Auslesen unerlaubter Speicherbereiche können Angreifer illegitim Informationen erhalten wie beispielsweise Speicheradressen, die für weitere Angriffsschritte relevante Informationen enthalten.

- Denial of Service: Durch den Zugriff auf nicht dafür vorgesehene Speicherbereiche können Angreifer Abstürze und somit Denial of Service Zustände herbeiführen.

Bekanntgewordene Schwachstellen

- CVE-2020-35683: Im Zusammenhang mit ICMP-Paketen (Internet Control Message Protocol) wird die Payload-Größe nicht geprüft, sondern aus dem IP-Header extrahiert. Wenn die tatsächliche Payload-Größe kleiner als die im Header angegebene Größe ist, kann eine Checksummenfunktion außerhalb vordefinierter Grenzen operieren, was zu Denial of Service führen kann.
- CVE-2020-13987: Im Zusammenhang mit einer unzureichenden Prüfung der Längenparameter im Paket-Header kann es bei bestimmten Umständen während der Prüfsummenberechnung zum unzulässigen Auslesen des Speichers und einem Denial of Service Zustand kommen.
- CVE-2020-24334: Durch eine unzureichende Prüfung von DNS-Antworten hinsichtlich der Übereinstimmung der Anzahl der im DNS-Paket-Header angegebenen mit den im DNS-Paket verfügbaren Antwortdaten, kann es zu einem Zugriff außerhalb des vorgesehenen Bereichs und einem Denial of Service Zustand kommen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs *Out of bounds Read* sind in den meisten Fällen keine Authentifizierungsmechanismen erforderlich. Dabei müssen Angreifer entsprechende Netzwerkpakete an das Ziel schicken, welche durch Ausnutzung der Schwachstelle einen Out of bounds Read provozieren. Um einen solchen Angriff auszuführen, muss der Angreifer somit lediglich in der Lage sein, eine Kommunikationsverbindung zum betroffenen System aufzubauen. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.4 Improper Handling of Length Parameter Inconsistency

Beschreibung

Unter der CWE-Nummer CWE-130 werden eine Bandbreite von Schwachstellen bzw. auf diesen basierende Angriffstechniken beschrieben, welche auf einer fehlerhaften Verarbeitung von Parameterlängen basieren. Typischerweise werden bei der Bearbeitung von Parametern im Rahmen der digitalen Kommunikation auch die erwarteten bzw. festgeschriebenen Längen dieser Parameter festgelegt. Im Rahmen einer schwachstellenfreien Programmierung legt das ausführende Programm die Länge der akzeptierten Parameter grundsätzlich fest. Längere Parameter werden grundsätzlich nicht akzeptiert, daher nicht bearbeitet, die Anfrage mit einem Parameter inkorrekter Länge führt zu einer Fehlerrückmeldung an den Absender der Anfrage.

Wird die Abfrage der Parameterlänger fehlerhaft oder gar nicht implementiert oder aber eine Parameterlängenbegrenzung fehlt, kommt es zumeist zu einer Schwachstelle, welche als inkorrekte Bearbeitung von Parameterlängeninkonsistenz (Improper Handling of Lenght Parameter Inconsistency), also einer Schwachstelle des Typs CWE-130 führt. Das angefragte Programm liest den spezifischen Parameter unabhängig von dessen Länge aus bzw. schreibt diesen unabhängig von dessen Länge in den Arbeitsspeicher des ausführenden Systems. Bei einem Parameter mit einer Länge, welche die vorgesehene Parameterlänge überschreitet, führt dies zum Auslesen bzw. Überschreiben des an den für den Parameter reservierten Speicherplatz des Arbeitsspeichers. Hierdurch kommt es zu einem Auslesen programmfremder Informationen oder zu einem Einspeichern von im Parameter enthaltenen Informationen in den Speicherbereich anderer Programme.

In der Konsequenz werden entweder dem Absender der Parameter, also dem Kommunikationspartner des Programms mit fehlerhafter Parameterbearbeitung, Informationen von anderen Programmen aus angrenzenden Speicherblöcken des Arbeitsspeichers ausgespielt oder aber die im Parameter enthaltenden Daten werden in angrenzenden Speicherblöcken eingespeichert und dann wiederum von anderen Programmen ausgelesen. Typische Konsequenzen hierdurch sind:

- Information disclosure: Der Absender des Parameters erhält durch das ausführende Programm Informationen aus angrenzenden Speicherblöcken, welche er nicht erhalten sollte.

- Denial of Service: Das den überlangen Parameter bearbeitende Programm bricht seine Lese- oder Schreiboperation ab und geht in einen Zustand über, mit dem die Programmfunktionen nicht mehr oder nicht mehr korrekt ausgeführt werden können.
- Remote Code Execution: Das Auslesen von angrenzenden Speicherblöcken oder das Einspeichern spezifischer Befehle in angrenzende Speicherblöcke durch den Absender des überlangen Parameters führen dazu, dass der Absender die Möglichkeit zur Ausführung beliebigen Codes auf dem betroffenen System erhält.

Bekanntgewordene Schwachstellen

- CVE-2009-2299: http Anfragen an die Hyperguard Web Application Firewall des Apache HTTP Server führen bei http Anfragen ab einer bestimmten Größe zu einem Denial of Service Zustand, da der Systemspeicher überlasten wird.
- CVE-2020-11896: Der TCP/IP Stack Treck verarbeitet bei der Nutzung von IPv4 Tunneling (eine Funktion, um die Kommunikation zwischen IPv4 und IPv6 zu ermöglichen) IPv4 Pakete mit untypischer Größe und Form auf eine Weise, dass dem Angreifer eine dauerhafte Möglichkeit zur Ausführung beliebigen Codes möglich ist. Varianten der Schwachstelle ermöglichen die Auslösung eines Denial of Service Zustandes, welcher bis zur Stromabschaltung des Gerätes anhält.
- CVE-2020-11898: Bestimmte IPv4 bzw. ICMPv4 (Internet Control Message Protocol) Nachrichten mit überlangen Längenparameter führen dazu, dass Angreifer Zugriff auf sensible im Arbeitsspeicher gespeicherte Informationen erhalten.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über dies Schwachstellen des Typs Improper Handling of Length Parameter Inconsistency sind in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Angreifer müssen hierzu entsprechende auf die Schwachstellen angepasste Parameter innerhalb der verarbeiteten Kommunikationsprotokolle versenden. Um einen solchen Angriff auszuführen, muss der Angreifer daher lediglich in der Lage sein, Kommunikationsanfragen oder zu verarbeitende Datenpakete an das betroffene System zu senden. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.5 Integer Underflow and Integer Overflow

Beschreibung

Unter den CWE-Nummern CWE-190 und 191 werden allgemein solche Schwachstellen bzw. auf diesen basierenden Angriffstechniken verstanden, welche aufgrund der grundsätzlichen Eigenschaften von Integer-Zahlen als ganzen Zahlen verstanden.

Integer-Zahlen sind ganze Zahlen und werden vielfach in Programmiersprachen angewendet, um Objekte in ganzen Zahlen auszudrücken und zu verarbeiten, z. B. bei Prozessen, bei denen ausschließlich ganze Zahlen (also solche ohne Komma und Brüche) verarbeitet werden. Dies können z. B. Zahlen als distinktiv zählbare Objekte wie Gegenstände in einem Spielsystem, Nummern in Datenmengen oder die Länge eines Objektes in Bit sein. Integerzahlen werden in einer vorher fest definierten Bit-Größe gespeichert, Int32 beschreibt z. B. Zahlen von 0 bis 4.294.967.295, wenn der negative Bereich nicht betrachtet wird oder aber von -2.147.483.648 bis 2.147.483647. Mit Integerzahlen können sämtliche Rechenoperationen durchgeführt werden, solange die Ergebnisse ganze Zahlen ergeben. Bei Divisionen von Integer-Zahlen, welche einen Bruch ergeben, werden Nachkommareste z. B. verworfen.

Integer Overflow und Integer Underflow sind zwei spezifische Fälle, in denen Rechenoperationen von Integer-Zahlen zu nicht plausiblen Ergebnissen führen. Integer Overflow beschreibt ein Verhalten, bei welchem durch Addition oder Multiplikation zweier Integer-Zahlen eine Integer-Zahl erzeugt wird, die größer ist als der ihr zugewiesene Speicherplatz. Eine 8 Bit große Integer-Zahl z. B. besitzt eine minimale Größe von -128 und maximale Größe von 127, wenn negative Zahlen mitbetrachtet werden. Wird 127 + 1 addiert, wird das System anstatt 128, eine Zahl außerhalb des erlaubten Zahlenbereiches „umspringen“ und als Ergebnis -128 anzeigen.

Integer Underflow beschreit einen ähnlichen Prozess bei der Subtraktion. Zwei Integer-Zahlen werden miteinander subtrahiert, das Ergebnis liegt außerhalb des vorgesehenen

Bereiches. Werden z. B. bei einer 8 Bit Integer-Zahl ohne Betrachtung des negativen Bereiches die Zahlen 10 und 11 miteinander subtrahiert, wäre das theoretische Ergebnisse -1. Der Zahlenbereich ist jedoch von 0 bis 255 definiert, sodass das ausgegebene Ergebnis anschließend als 255 wiedergegeben wird.

Integer-Overflow und Integer-Underflow können eine Vielzahl von Folgen für das betroffene System aufweisen, wenn keine oder nicht ausreichende Maßnahmen zur Erkennung von Rechenoperationen, die zur Über- oder Unterschreitung der gesetzten Zahlenbereiche führen, getroffen werden. Grundsätzlich sind bei Manipulation solcher Schwachstellen eine Vielzahl von Konsequenzen bekannt geworden:

- Denial of Service: Integer Overflow und Integer Underflow führen vielfach zu Programm- und Systemabstürzen, z. B. wenn bei der Zuordnung von Speicherbereichen zu kleine oder zu große Speicherbereiche zugewiesen werden.
- Integrität: Durch Integer Overflow bzw. Underflow erfolgt die Speicherung und Verarbeitung fehlerhafter Daten, wodurch wiederum weitergehende Konsequenzen erfolgen können.
- Access Control: Zum einen können Integer Overflow und Integer Underflow zu fehlerhafter Speicherallokation führen, sodass Angreifer beliebige Codes ausführen können, zum anderen können z. B. bei Anmeldeoptionen Integer Overflow bzw. Underflow Möglichkeiten für Angreifer eröffnen.

Bekanntgewordene Schwachstellen

- CVE-2024-38063: Sendet ein Angreifer übergroße IPv6 Pakete an ein Windows System, kann der Angreifer die Fähigkeit zur Ausführung beliebigen Codes erhalten.
- CVE-2020-17443: Erhält der picoTCP TCP/IP Stack einen ICMPv6 echo Request, wird nicht geprüft, ob dieser Request die minimale Größe besitzt. Die Bearbeitung solcher Requests führt zu einer Speicherkorrumpierung.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über die Schwachstellen des Typs Integer Overflow bzw. Integer Underflow sind grundsätzlich keine Authentifizierungsmechanismen notwendig. Symptomatisch für Schwachstellen dieses Typs ist, dass sie sich zumeist aus der direkten Verarbeitung von Daten bzw. Zahlen ergeben und hierdurch vielfach ohne Authentifizierung ausgeführt werden können. Je nach Schwachstelle sind vielfach

keine vorhergehenden Angriffsschritte zur Ausführung eines Angriffes notwendig. Im Kontext von Schwachstellen von Netzwerkprotokollen sind hierbei lediglich direkte Zugriffe über dauerhafte oder temporäre Netzwerkverbindungen notwendig.

4.2.6 Exposure of Sensitive Information to an Unauthorized Actor

Beschreibung

Die Schwachstelle *Exposure of Sensitive Information to an Unauthorized Actor* (CWE-200) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, die im Zusammenhang mit einer Bereitstellung von sensitiven Informationen an nicht autorisierte Angreifer stehen. Dabei werden sämtliche Arten von Informationen, Passwörter, persönliche Daten, Geschäftsgeheimnisse oder ähnliches, betrachtet. Die Schwachstelle kann einzeln auftreten, z. B. durch direkte Übersendung von sensitiven Informationen an eine unautorisierte Person oder durch eine weitere vorhergehende Schwachstelle, die den Zugriff auf diese Schwachstelle ermöglicht.

Abweichend von der Konsequenz „Information Exposure“ bzw. „Information Disclosure“, welche bei einer Vielzahl unterschiedlicher Schwachstellentypen auftreten, tritt „Exposure of Sensitive Information to an Unauthorized Actor“ bei solchen Softwareverhalten auf, bei welchem direkt Informationen verwaltet, verarbeitet, gespeichert, übersendet oder gelöscht werden. Im Falle der Schwachstelle CVE-2017-7575 der speicherprogrammierbaren Steuerung Modicon M221 des Herstellers Schneider Electric, gibt das Gerät ein Passwort für den Geräteschutz an beliebige über Modbus verbundene Angreifer aus, welche eine Anfrage des Typs

```
\x00\x01\x00\x00\x00\x05\x01\x5a\x00\x03\x00
```

senden. Die Schwachstelle ermöglicht Angreifern damit direkten Zugriff auf eine kritische Information, welche von den Angreifern weitergehend verwendet werden kann. Weitere typische Beispiele sind z. B. die Implantierung von Account- und Passwortabfragen, welche Hinweise auf fehlerhaft eingegeben Account- oder Passwörter geben, die Herausgabe von Fehlermeldungen, welche Angreifern Speicherorte und Dateipfade aufzeigen oder fehlerhafte Datenbankabfragen, welche den nicht autorisierten Abfragenden Informationen zur Verfügung stellen, welche nur autorisierte Personen erhalten sollten.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer ausschließlich eine Verletzung der Vertraulichkeit von gespeicherten Daten der betroffenen Systeme. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer erhalten Zugriff auf sensitive Informationen, ohne die hierfür notwendige Autorisierung zu besitzen.

Werden im Rahmen von „Exposure of Sensitive Information to an Unauthorized Actor" Zugangsdaten wie Accountdaten oder Passwörter in Erfahrung gebracht, besteht eine anschließende Möglichkeit zur Verletzung der Verfügbarkeit und Integrität mit den folgenden Konsequenzen:

- Denial of Service
- Remote Code Execution

Bekanntgewordene Schwachstellen

- CVE-2017-7575: Eine einzelne Anfrage über Modbus führt zur Herausgabe des Application-Protection Passwords des Schneider Electric Modicon SPS.
- CVE-2020-11903: Spezifische DHCP-Antworten des Treck TCP/IP Stack ermöglichen Angreifern lesenden Zugriff auf bestimmte Speicherbereiche und damit die dort abgespeicherten, sensitiven Informationen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs *„Exposure of Sensitive Information to an Unauthorized Actor"* sind grundsätzlich keine bzw. niederschwellige Authentifizierungsmechanismen erforderlich. Dies bedeutet, dass Angreifer entweder ohne jedwede Authentifizierung oder aber Authentifizierungsstufen überspringend (z. B. Normale Benutzer können auf Daten von Administratorkonten zugreifen) die Schwachstellen ausnutzen können. Hierzu muss lediglich eine dauerhafte oder temporäre datentechnische Kommunikationsverbindung zwischen den Angreifenden und den betroffenen Systemen vorliegen.

Abhängig von der Art der Schwachstelle, ist für die Ausnutzung von „*Exposure of Sensitive Information to an Unauthorized Actor"* teilweise die Ausnutzung weiterer Schwachstellen wie „*Improper Input Validation"* notwendig, welche dann wiederum die Möglichkeit zur spezifischen Informationsgewinnung ermöglichen.

4.2.7 Improper Access Control

Beschreibung

Die Schwachstelle *Improper Access Control* (CWE-284) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, welche die unzureichende Implementierung und Durchführung von Zugriffskontrollen betreffen, sodass unautorisierte Akteure illegitime Zugriffsmöglichkeiten erlangen.

Die Zugriffskontrolle umfasst allgemein im Wesentlichen Mechanismen zur Authentifizierung (Identitätskontrolle eines Akteurs), Autorisierung (Sicherstellung des Besitzes der für einen Zugriff erforderlichen Berechtigungen) und zur Rechenschaftspflicht (Nachverfolgung durchgeführter Aktivitäten). Die ausbleibende oder unzureichende Ausführung dieser Kontrollen und Mechanismen gefährdet die Sicherheit von Systemen, Programmen und Daten, indem Angreifern ermöglicht wird nicht autorisierte Handlungen durchzuführen. Dies können je nach genauen Umständen unterschiedliche Handlungen sein wie die Erhöhung von eigenen Zugriffsrechten, der illegitime Zugriff auf vertrauliche Informationen sowie das illegitime Ausführen von Aktionen.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer können durch unzureichende Zugriffskontrollen. Zugriff auf vertrauliche Informationen erlangen.
- Denial of Service: Angreifer können durch unzureichende Zugriffskontrollen unautorisierte Befehle ausführen und so beispielsweise Systeme zum Absturz bringen, neu starten, beenden oder einen übermäßigen Verbrauch von Ressourcen wie Arbeitsspeicher und Prozessorleistung herbeiführen.
- Modify Memory & Remote Code Execution: Durch die unautorisierte Übermittlung von illegitimen Befehlen können Angreifer für sie nicht vorgesehene/änderbare Bereiche des Speichers ändern und nicht autorisierten Code oder Befehle ausführen.

Bekanntgewordene Schwachstellen

- CVE-2020-11911: Aufgrund der fehlerhaften Verarbeitung von speziell präparierten WebRTC-Paketen (für Echtzeitkommunikation wie Videoanrufe) können Angreifer,

sofern sie eine Verbindung über WebRTC zum Opfer hergestellt haben, durch Senden entsprechend manipulierter Pakete Heap-Buffer-Overflows verursachen, sodass das Programm abstürzt oder Angreifer die Kontrolle übernehmen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs *Improper Access Control* sind in den meisten Fällen keine Authentifizierungsmechanismen erforderlich. Da dieser Typ von Schwachstellen Sicherungsmaßnahmen zur Zugriffskontrolle betrifft, ermöglicht die Ausnutzung potenzieller Angreifer im Wesentlichen illegitime Aktionen, unautorisierte Handlungen und Angriffsschritte auszuführen. Dies kann unter Umständen per Fernzugriff durch Übermittlung entsprechender Daten an Netzwerke/Systeme erfolgen, wobei durch die mangelnde Zugriffskontrolle schadhafte Handlungen ermöglicht werden. Um einen solchen Angriff auszuführen, muss der Angreifer somit lediglich in der Lage sein, eine Kommunikationsverbindung zum betroffenen System aufzubauen. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.8 Improper Authentication

Beschreibung

Die Schwachstelle *Improper Authentication* (CWE-287) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, welche die unzureichende Implementierung von Authentifizierungsmechanismen betreffen, sodass Angreifer ohne hinreichende Authentifizierung Zugriffsmöglichkeiten erlangen und ihre Identität dabei verschleiern können.

Mechanismen zur Authentifizierung sind im Bereich der Cybersicherheit elementar, da durch diese sichergestellt wird, dass nur ein vorher definierter Personenkreis Zugriff auf bestimmte Daten oder Systeme erhält. Durch die Authentifizierung weist ein Anwender

nach, zu dem berechtigten Personenkreis zu gehören. Wenn Authentifizierungsmechanismen umgangen werden, können je nach genauen Umständen dazu führen, dass nicht für den Zugriff auf Daten oder Systeme vorgesehene Personen Zugriffsmöglichkeiten erlangen. Zudem werden Angreifer dadurch unterschiedliche Handlungen ermöglicht wie beispielsweise der illegitime Zugriff auf vertrauliche Informationen sowie das illegitime Ausführen von weiteren Aktionen.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer können durch unzureichende Authentifizierungsmechanismen Zugriff auf vertrauliche Informationen erlangen.
- Denial of Service: Angreifer können durch unzureichende Authentifizierungsmmechanismen illegitim Zugriff erlangen, Befehle ausführen und so beispielsweise Systeme zum Absturz bringen, neu starten, beenden oder einen übermäßigen Verbrauch von Ressourcen wie Arbeitsspeicher und Prozessorleistung herbeiführen.
- Integrität: Angreifer können, nachdem sie unautorisiert Zugriff erlangt haben, Daten manipulieren und verändern, sodass diese kompromittiert werden.

Bekanntgewordene Schwachstellen

- CVE-2016-7112: Angreifer mit Netzwerkzugriff auf die Webschnittstelle eines betroffenen Geräts können bei Ausnutzung der Schwachstelle die Authentifizierung umgehen und bestimmte administrative Aktionen ausführen.
- CVE-2018-14805: Die Ausnutzung der Schwachstelle kann unbefugten Zugriff auf das System ermöglichen, wenn LDAP so eingestellt ist, dass anonyme Authentifizierung zulässig ist, und bestimmte Kondition in relevanten Dateien in diesem Zusammenhang erfüllt sind.
- CVE-2022-29865: Die Ausnutzung dieser Schwachstelle ermöglicht es einem Angreifer aus der Ferne, die Authentifizierungsprüfung mithilfe gefälschter Anmeldedaten zu umgehen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs

Improper Authentication sind in den meisten Fällen keine Authentifizierungsmechanismen erforderlich. Die Ausnutzung von derartigen Schwachstellen erfordert in der Regel keinen tiefergehenden technischen Hintergrund, sondern lediglich den Zugriff potenzieller Angreifer auf die betroffenen Programme/Funktionen/Komponenten, die keine Authentifizierung verlangen. Somit können potenzielle Angreifer mit Zugriff (ggf. logisch, über entsprechende Netzwerkverbindungen) illegitime Befehle an das System senden. Je nachdem, inwiefern ggf. vorhandene weitere Sicherungsmaßnahmen beispielsweise zur Härtung realisiert sind, stehen potenziellen Angreifern entsprechend weitere Angriffsschritte offen. Da die Schwachstelle mangelhafte Authentifizierungen für kritische Funktionen betrifft, sind mögliche Auswirkungen relativ weitläufig und nicht eingeschränkt; dabei aber im Wesentlichen abhängig von den genauen Umständen des Systems.

4.2.9 Authentication Bypass by Spoofing und Capture Replay

Beschreibung

Die Schwachstellen CWE-290 und -294 *(Authentication Bypass by Spoofing und Authentication Bypass by Capture-replay)* betreffen unzureichend implementierte Realisierungen von Mechanismen zur Authentifizierung von Anwendern durch verschiedene Techniken.

Angreifer können durch die Ausnutzung derartiger Schwachstellen die Authentifizierung und damit den Nachweis ihrer Zugriffsberechtigung umgehen, sodass sie illegitim Zugriffe erlangen oder Funktionen ausführen können. Dies ist beispielsweise der Fall, wenn eine von dieser Art Schwachstelle betroffene Anwendung die Identität eines Benutzers nicht ausreichend überprüft, bevor sie Zugriff gewährt. Die Angreifer erlangen dabei je nach Umständen Zugriffsrechte ähnlich zu denen legitimer Benutzer, jedoch ohne den Authentifizierungsprozess angemessen zu durchlaufen. Die oben genannten CWEs betreffen dabei zwei unterschiedliche Täuschungsmethoden, mit denen der Authentication Bypass durchgeführt wird.

Das Spoofing umfasst verschiedene Methoden zur Verschleierung der eigenen Identität. Dabei geht es im Wesentlichen darum, eine vertrauenswürdige Identität (die der Angreifer entsprechend vorgibt) vorzutäuschen. Dabei gibt es mittlerweile verschiedene Spoofing-Arten, die je nach Bedarf eingesetzt werden können. Das Telefon-Spoofing setzt beispielsweise auf gefälschte Telefonnummern und entsprechende Anrufe, bei denen

sich Angreifer als andere Personen ausgeben. Andere Spoofing-Arten umfassen beispielsweise E-Mail Spoofing durch die Manipulation von E-Mail-Headern und IP/DNS-Spoofing mit gefälschten IP-Adressen, über die beispielsweise schadsoftwarebehaftete Datenpakete verschickt werden.

Beim Capture-Replay geht es im Wesentlichen darum, dass Angreifer den Netzwerkverkehr überwachen und durch die Übermittlung gleicher oder leicht abgewandelter, abgefangener Nachrichten eine fremde Identität vortäuscht. Dabei profitiert der Angreifer von legitimen, ggf. signierten Nachrichten und kann durch den Replay-Angriff den Anschein einer ebenfalls legitimen Nachricht erwecken.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Wenn Angreifer illegitim und nicht authentifiziert auf sensible Daten zugreifen, können sie diese Informationen stehlen.
- Denial of Service: Durch unkontrollierte und unautorisierte Zugriffsvorgänge können (kritische) Funktionen überlastet oder deaktiviert werden, sodass die Verfügbarkeit von Diensten und Funktionen gestört wird.
- Integrität: Angreifer können, nachdem sie unautorisiert Zugriff erlangt haben, Daten manipulieren und verändern, sodass diese kompromittiert werden.

Bekanntgewordene Schwachstellen

- CVE-2021-22779: Angreifer können bei Ausnutzung dieser Schwachstelle unautorisiert Modbus-Funktionen auf einem betroffenen Controller ausführen, indem die Authentifizierung mit Hilfe eines Replay-Angriffs umgangen wird.
- CVE-2022-45789: Indem Angreifer durch Ausnutzung dieser Schwachstelle unautorisiert Zugriff auf einen betroffenen Controller erlangen, können sie die Kommunikation zwischen der Engineering Software und dem korrespondierenden Controller manipulieren.

Ausnutzung der Schwachstellen

Die Ausnutzung von derartigen Schwachstellen erfordert in der Regel keinen tiefergehenden technischen Hintergrund, sondern lediglich den Zugriff potenzieller Angreifer auf

die betroffenen Programme/Funktionen/Komponenten, die keine Authentifizierung verlangen. Somit können potenzielle Angreifer mit Zugriff (ggf. logisch, über entsprechende Netzwerkverbindungen) illegitime Befehle an das System senden. Je nachdem, inwiefern ggf. vorhandene weitere Sicherungsmaßnahmen beispielsweise zur Härtung realisiert sind, stehen potenziellen Angreifern entsprechend weitere Angriffsschritte offen. Da die Schwachstelle mangelhafte Authentifizierungen für kritische Funktionen betrifft, sind mögliche Auswirkungen relativ weitläufig und nicht eingeschränkt; dabei aber im Wesentlichen abhängig von den genauen Umständen des Systems.

4.2.10 Missing Authentication for Critical Function

Beschreibung

Die Schwachstelle *„Missing Authentication for Critical Function“* (CWE-306) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, die im Zusammenhang mit ausbleibenden Authentifizierungen für Funktionen stehen, welche eine nachweisbare Benutzeridentität erfordern oder eine erhebliche Menge an Ressourcen verbrauchen. Eine Anwendung führt somit beispielsweise keine Authentifizierung für sicherheitskritische Funktionen durch, wodurch Angreifer unter Umständen ohne vorherige Identitätsprüfung auf sensible Systemfunktionen, Daten manipulieren oder unbefugt Aktionen ausführen können. Zudem ist beispielsweise bei Ausnutzung dieser Schwachstelle durch Angreifer ein Zugriff auf Ressourcenintensive Prozesse möglich, wodurch die Systemleistung entsprechend beeinträchtigt werden kann.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Wenn Angreifer illegitim und nicht authentifiziert auf sensible Daten zugreifen, können sie diese Informationen stehlen.
- Denial of Service: Durch unkontrollierte und unautorisierte Zugriffsvorgänge können (kritische) Funktionen überlastet oder deaktiviert werden, sodass die Verfügbarkeit von Diensten und Funktionen gestört wird.
- Integrität: Angreifer können, nachdem sie unautorisiert Zugriff erlangt haben, Daten manipulieren und verändern, sodass diese kompromittiert werden.

Bekanntgewordene Schwachstellen

- CVE-2018-4838: Unter Ausnutzung dieser Schwachstelle können nicht authentifizierte Angreifer Firmware Updates oder Downgrades durchführen und so beispielsweise ältere Versionen mit bekannten Schwachstellen ausnutzen, um weitere Angriffshandlungen vorzubereiten.
- CVE-2018-4840: Diese Schwachstelle ermöglicht es nicht authentifizierten Angreifern manipulierte Gerätekonfigurationen an betroffene Geräte zu übermitteln und dabei Zugriffspasswörter zu überschreiben oder die Funktionalität des betroffenen Geräts zu beeinträchtigen.

Ausnutzung der Schwachstellen

Die Ausnutzung von derartigen Schwachstellen erfordert in der Regel keinen tiefergehenden technischen Hintergrund, sondern lediglich den Zugriff potenzieller Angreifer auf die betroffenen Programme/Funktionen/Komponenten, die keine Authentifizierung verlangen. Somit können potenzielle Angreifer mit Zugriff (ggf. logisch, über entsprechende Netzwerkverbindungen) illegitime Befehle an das System senden. Je nachdem, inwiefern ggf. vorhandene weitere Sicherungsmaßnahmen beispielsweise zur Härtung realisiert sind, stehen potenziellen Angreifern entsprechend weitere Angriffsschritte offen. Da die Schwachstelle mangelhafte Authentifizierungen für kritische Funktionen betrifft, sind mögliche Auswirkungen relativ weitläufig und nicht eingeschränkt; dabei aber im Wesentlichen abhängig von den genauen Umständen des Systems.

4.2.11 Use of Insufficiently Random Values

Beschreibung

Unter der CWE-Nummer CWE-330 werden allgemein solche Schwachstellen bzw. auf diesen basierenden Angriffstechniken verstanden, welche darauf basieren, dass zufällige Zahlen auf datentechnischen Systemen grundsätzlich nicht rein zufällig generiert werden können.

Eine Vielzahl von Programmen wie Verschlüsselungen, Identifikationsmerkmale, Seeds oder Hashwerte benötigen im Rahmen ihrer Generierung zufallsbasierte Zahlen oder zufällige Folgen von Buchstaben und Zahlen. Rein zufällige Zahlen bzw. Zeichenfolgen sind jedoch technisch nicht ausschließlich mit Software realisierbar, da für die Erzeugung

grundsätzlich ein Algorithmus angewendet werden muss, jedoch bisher kein reiner Zufallsalgorithmus bekannt ist. Die so erzeugten Zufallszahlen und Zeichenfolgen werden daher im informationstechnischen Sinn „pseudo-zufällig“ genannt. Zu ihrer Erzeugung werden daher komplexe und lange Startwerten mit einer Größe von 128 Bit bis 2.048 Bit verwendet. Je größer der Startwert zur Generierung der Zufallszahlen bzw. Zufallszeichenfolgen, desto komplexer die sich hieraus ergebenden Zufallszahlen bzw. Zufallszeichenfolgen. Wahre Zufallsalgorithmen basieren auf der Wahrnehmung von physikalischen Messungen tatsächlich zufälliger Phänomene wie dem Hintergrundrauschen von Sensoren.

Grundsätzlich gibt es eine Vielzahl von Möglichkeiten, wie Schwachstellen der Zufallsgenerierung dazu führen, dass Angreifer generierte Zufallszahlen bzw. Zufallszeichenfolgen vorhersagen können. Dies führt dazu, dass Angreifer z. B. kryptografische Schlüssel vorhersagen können und damit automatisch generieren können. Andere Möglichkeiten bestehen z. B. für Angreifer zur Vorhersehung einer individuellen ID für Benutzer, welche von den Angreifern dann für weitere Einwirkungen auf die betroffenen Systeme verwendet werden können. Zu diesen Schwachstellen der Erzeugung und Nutzung von Zufallszahlen gehören hierbei folgende kategorischen Unterschwachstellen:

- Die Nutzung unzureichender Zufälligkeit (englisch: Entropy), also einen Algorithmus, welcher in der Ausgabe einen geringen Grad der Zufälligkeit erreicht, sodass erkennbare Muster in den erzeugten Werten vorliegen.
- Die Nutzung einer geringen Bandbreite von Zufallszahlen/Zeichen, z. B. die Vorgabe Zahlen zwischen 1-10 zu generieren.
- Inkorrekte Nutzung von Startwerte (Englisch: Seeds) in der Zufallszahlengenerierung, sodass diese von Angreifern ermittelt werden können.
- Nutzung von kryptographisch schwachen Startwerten, also Seeds mit einer geringen Bit-Anzahl, wie 128bit oder weniger.
- Die Generierung von grundsätzlich vorhersehbaren Nummern oder IDs, z. B. durch den Einsatz eines bekannten Zufallsalgorithmus mit bekannten Startwerten.
- Die Nutzung konstanter Werte in Fällen, in denen variable Werte eingesetzt werden sollten. Hierzu zählen z. B. hart festgeschriebene Passwörter.

- Generierung schwacher Initialisierungsvektoren, welche z. B. bei kryptografischen Verfahren eingesetzt werden. Sind diese vorhersehbar, können diese bei Angegriffen und für die Aushebelung kryptographischer Verfahren angewendet werden.
- Nutzung vorhersehbarer oder bekannter Algorithmen zur Erzeugung von Zufallszahlen.

Unabhängig welches Unterschwachstelle der Schwachstelle einer nicht ausreichenden Zufälligkeit von Zufallszahlen und Zufallszeichenfolgen vorliegt, können diese grundsätzlich durch Angreifer manipuliert werden, wenn Angreifer in der Lage sind die eigentlich zufälligen Zahlen bzw. Zeichenfolgen vorherzusehen. Typische Konsequenzen hierdurch sind:

- Confidentiality: Zufallszahlen werden insbesondere bei Verschlüsselungen und anderen Identifizierungsmerkmalen eingesetzt. Sind diese Vorhersehbar, können Angreifer z. B. die Entschlüsselung verschlüsselter Dateien durchführen oder auf Informationen zugreifen, die eine Identifikation benötigen.
- Access Control: Werden bei Authentifizierungsmerkmalen bzw. Identifikationsmerkmalen keine ausreichend zufälligen Daten verwendet, können Angreifer diese Ermitteln und für Zugriffe auf gesicherte Bereiche verwenden.

Bekanntgewordene Schwachstellen

- CVE-2021-35685: Vorhersehbare Zufallswerte der Start-Sequenznummer eines TCP basierten Verbindung führen dazu, dass Angreifer durch Spoofing sich als das betroffene System ausgeben können.
- CVE-2021-31228: Bei der Handhabung von DNS-Requests wird eine nicht ausreichende Zufälligkeit angewendet, da diese auf der Tageszeit basieren. Angreifer können manipulierte DNS-Pakete versenden, welche zu einem Denial-of-Service führen.
- CVE-2020-25926: Der betroffene TCP/IP Stack nutzt einen Algorithmus mit nicht ausreichender Zufälligkeit, wodurch Angreifer in der Lage sind besondere DNS-Pakete zu entwickeln, mit welchen die Angreifer dann den DNS-Cache des betroffenen Systems füllen können, in dessen Konsequenz es zu einem Denial-of-Service kommt.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über dies Schwachstellen des Typs „Use of Insufficiently Random Values“ und seiner Untertypen sind grundsätzlich keine Authentifizierungsmechanismen notwendig. Die Schwachstellen dieses Typs und deren Untertypen weisen sich dadurch aus, dass diese Authentifizierung- und kryptographische Verfahren schwächen und daher in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Je nach Schwachstelle und Ausgestaltung dieser sind einfache oder hochkomplexe Angriffsschritte wie der Vorausberechnung von nicht ausreichend zufälligen Werten durch die Angreifer notwendig, um einen erfolgreichen Angriff auf Systeme mit entsprechenden Schwachstellen ausführen. Im Kontext von Schwachstellen von Netzwerkprotokollen sind hierbei direkte Zugriffe über dauerhafte oder temporäre Netzwerkverbindungen notwendig, in Fällen, die z. B. ausschließlich kryptografische Schlüssel betreffen, sind Zugriffe auf die verschlüsselten Dateien notwendig.

4.2.12 Insufficient Entropy

Beschreibung

Unter der CWE-Nummer CWE-331 werden Schwachstellen bzw. auf diesen basierenden Angriffstechniken beschrieben, welche auf eine unzureichende Implementierung realer Zufallswerte hinauslaufen.

Eine unzureichende Entropie bedeutet in diesem Zusammenhang, dass Zufallswerte wie beispielsweise Schlüssel oder Session-IDs nicht unvorhersehbar sind und dadurch Werte in Mustern/Clustern auftreten, da gewisse Werte häufiger auftreten als andere. Wenn dieses Problem in sicherheitskritischen Funktionen auftritt, kann ein Angreifer potenziell relevante Werte erraten oder vorhersagen und beispielsweise illegitim Zugriff auf Ressourcen erlangen. Das grundlegende Problem ist dabei, dass rechnerbasierte Systeme als deterministische Maschinen nicht ohne weiteres in der Lage sind, echte Zufallszahlen zu generieren, die keinem (logischen) Muster folgen. Dazu werden Pseudorandom Number Generators verwendet, die entsprechend ausreichend dimensioniert und initialisiert sein müssen. Wenn dies nicht der Fall ist, können Angreifer beispielsweise durch Beobachtung der erhaltenen Zufallswerte Rückschlüsse auf die vermutlich weiteren generierten Werte schließen und damit beispielsweise Brute-Force Angriffe auf sensible Inhalte vorbereiten.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer können durch unzureichende Entropie Zugriff auf vertrauliche Informationen erlangen, indem vorhersehbare Zufallswerte beispielsweise die Dechiffrierung verschlüsselter Kommunikation ermöglicht.
- Denial of Service: Angreifer können durch unzureichende Entropie vorhersehbare Sequenznummern und Tokens missbrauchen und so beispielsweise Systeme zum Absturz bringen, neu starten, beenden oder einen übermäßigen Verbrauch von Ressourcen wie Arbeitsspeicher und Prozessorleistung herbeiführen.
- Bypass/Account-Übernahme und falsche Signaturen: Je nach Einsatz der unzureichenden Entropie können Integritätsverletzungen beispielsweise durch gefälschte Signaturen herbeiführen. Zudem ermöglichen erratbare Session-IDs oder Tokens Benutzerkonten zu übernehmen und sich als legitime Nutzer auszugeben.

Bekanntgewordene Schwachstellen

- CVE-2020-25926: Eine unzureichende Entropie in der DNS-Transaktions-ID ermöglicht DNS-Poisoning bzw. DNS-Cache-Poisoning, bei der gefälschte IP-Adressen-Einträge im Cache des DNS-Servers eingeschleust werden.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über dies Schwachstellen des Typs *Insufficient Entropy* sind in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Angreifer müssen hierzu entsprechende auf die Schwachstellen angepasste Befehle oder von dem angegriffenen System zu verarbeitende Nachrichten senden. Um einen solchen Angriff auszuführen, muss der Angreifer daher lediglich in der Lage sein, Kommunikationsanfragen oder zu verarbeitende Datenpakete an das betroffene System zu senden. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden. Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende

Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

Wesentlich für die Ausnutzung derartiger Schwachstellen ist typischerweise zudem die Beobachtung oder das Abfangen von Zufallswerten, sodass Aussagen über zukünftige Zufallswerte getroffen werden können.

4.2.13 Uncontrolled Ressource Consumption

Beschreibung

Unter der CWE-Nummer CWE-400 werden Schwachstellen bzw. auf diesen basierenden Angriffstechniken beschrieben, welche auf eine Ressourcenerschöpfung und dadurch eine herbeigeführte bedingte Einschränkung von Funktionen hinauslaufen.

Das System kontrolliert die Zuteilung notwendiger Ressourcen für bestimmte Prozesse und Aufgaben im Normalfall derartig, dass jederzeit die notwendigen Ressourcen zur Erfüllung von Aufgaben bereitgehalten werden. Dies gilt insbesondere für kritische Aufgaben. Durch einen unkontrollierten Verbrauch bzw. die Blockade relevanter Ressourcen sind diese entsprechend gebunden, sodass einer oder mehrere Prozesse und Aufgaben bis hin zum System selbst nicht mehr verfügbar sind. Bei den Ressourcen kann es sich beispielsweise um Arbeitsspeicher, Dateisystemspeicher, Netzwerkbandbreite oder Rechenkapazitäten von CPU oder GPU handeln. Es gibt mehrere Möglichkeiten, wie eine solche Erschöpfung von Ressourcen zustande kommen kann, zum Beispiel eine fehlende oder fehlerhafte Drosselung der Anzahl zugewiesener Ressourcen oder die Bindung unzulässige der Ressourcen nach Abschluss einer Aufgabe.

Typische Konsequenzen von uncontrolled Recursions sind im Wesentlichen:

- Denial of Service: Durch die unkontrollierte Bindung von Ressourcen werden mehr und mehr Ressourcen des betroffenen Systems in Anspruch genommen, bis die Ausführung anderer Aufgaben sich verlangsamt und schließlich zum vollständigen Erliegen kommt.

Aufgrund der häufigen fehlerhaften Anwendung von CWE-400 wird die Verwendung zur Beschreibung durch MITRE nicht mehr empfohlen. Die ursprüngliche Bedeutung zielt

auf das inkorrekte Verhalten ab, bei dem das ein Angreifer bei Ausnutzung der Schwachstelle den Ressourcenverbrauch verfolgen und einschränken soll. Oftmals wurde diese Art Schwachstelle jedoch mit den technischen Auswirkungen anderen Schwachstellen verwechselt, die einen übermäßigen Ressourcenverbrauch zur Folge haben.

Bekanntgewordene Schwachstellen

- CVE-2019-19300: Innerhalb von Profinet können Angreifer durch Ausnutzung der Schwachstelle durch die Übermittlung speziell gestalteter Pakete den Verbrauch von übermäßig vielen Ressourcen erzwingen und so das System überlasten und einen Denial-of-Service-Zustand herbeiführen.
- CVE-2022-25622: Durch eine fehlerhafte Handhabung interner Ressourcen für TCP-Segmente können Angreifer durch Übermittlung speziell gestalteter TCP-Segmente einen Denial-of-Service-Zustand für TCP-Dienste betroffener Geräte verursachen.
- CVE-2023-27321: Durch eine fehlerhafte Verarbeitung von OPC UA-Anfragen im Rahmen dieser Schwachstelle können Angreifer durch das Senden einer großen Anzahl entsprechender Anfragen alle verfügbaren Ressourcen auf einem Server verbrauchen und blockieren, sodass sie einen Denial-of-Service-Zustand herbeiführen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberngriffes über dies Schwachstellen des Typs „*Uncontrolled Ressource Consumption“* sind in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Angreifer müssen hierzu entsprechende auf die Schwachstellen angepasste Befehle oder von dem angegriffenen System zu verarbeitende Nachrichten senden. Um einen solchen Angriff auszuführen, muss der Angreifer daher lediglich in der Lage sein, Kommunikationsanfragen oder zu verarbeitende Datenpakete an das betroffene System zu senden. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden. Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.14 Double Free

Beschreibung

Die Schwachstelle „*Double Free“* (CWE-415) tritt in der Speicherverwaltung von Software auf, wenn ein Programm denselben Speicherbereich mehr als einmal freigibt (die „free()“-Funktion beispielsweise zweifach für dieselbe Speicheradresse aufruft). Wenn das System infolgedessen versucht, Speicherplatz freizugeben, der bereits freigegeben wurde, kommt es zu unvorhersehbarem Verhalten des Programms. Dies führt dazu, dass die Speicherverwaltungsdatenstrukturen des Programms beschädigt werden, was zu unerwarteten Speicheränderungen führen kann. Wenn das System bei einem zweiten Aufruf versucht, den bereits freigegebenen Speicher erneut freizugeben, kommt es zu Problemen, weil in der Implementierung nur eine Freigabe vorgesehen ist. In der Regel resultiert die Schwachstelle aus einer anderen bereits vorliegenden Schwachstelle (beispielsweise *buffer overflow* oder *unhandled error*). Die potenziellen Auswirkungen, die sich durch die Schwachstelle ergeben, erstrecken sich auf die Stabilität und Sicherheit des Systems, da Speicherfehler oftmals zu undefinierten und unkontrollierten Zuständen führen können. Angreifer können „*Double Free“* Schwachstellen unter anderem ausnutzen, indem sie das zugrunde liegende Speicherverwaltungssystem manipulieren (abhängig von der Art des Systems und der Implementierung der Speicherverwaltung) und die internen Strukturen korrumpieren. Dadurch können beispielsweise freigegebene Speicherbereiche überschrieben oder veränderte Speicheradressen verwendet werden.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Angreifer können durch die doppelte Freigabe von Speicherelementen nicht dafür vorgesehene Speicherelemente und somit Dateien oder Verzeichnisse auslesen und haben ggf. Zugriff auf vertrauliche Informationen.
- Denial of Service: Angreifer können durch die doppelte Freigabe von Speicherelementen Systeme zum Absturz bringen, neu starten, beenden oder einen übermäßigen Verbrauch von Ressourcen wie Arbeitsspeicher und Prozessorleistung herbeiführen.

- Modify Memory & Execute Unauthorized Code or Commands: Angreifer können zum Beispiel im Rahmen eines Use-After-Free-Szenarios freigegebene Speicherbereiche mit beliebigem Code manipulieren, der vom System ausgeführt wird.

Bekanntgewordene Schwachstellen

- CVE-2020-6072: Durch eine doppelte Freigabe von Speicherelementen in der Kodi-Software (Open-Source-Software zur Organisation und Wiedergabe von Medieninhalten auf verschiedenen Geräten) kann es dazu kommen, dass Angreifer betroffene Systeme abstürzen lassen oder Schadsoftware ausführen können.
- CVE-2020-11900: Durch eine doppelte Freigabe innerhalb eines Messenger-Dienstes entsteht beim Verarbeiten spezieller RTP-Pakete (Real-Time Transport Protocol)) eine Schwachstelle, durch die Angreifer Programme destabilisieren oder Schadsoftware ausführen können.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs „*Double Free“* sind oftmals keine Authentifizierungsmechanismen erforderlich, insbesondere wenn es sich um öffentliche oder frei zugängliche Software oder Dienste handelt. Ggf. ist eine Authentifizierung erforderlich, um an entsprechende Speicherbereiche zu gelangen, die von der Schwachstelle betroffen sind. Dazu müssen Angreifer zunächst in der Lage sein, betroffene Speicherbereiche gezielt zu beeinflussen, unter anderem durch die Etablierung einer Kommunikationsverbindung. Die Voraussetzungen für einen erfolgreichen Angriff hängen dabei von der spezifischen Implementierung der betroffenen Software ab.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.15 Uncontrolled Recursion

Beschreibung

Unter der CWE-Nummer CWE-674 werden eine Bandbreite von Schwachstellen bzw.

auf diesen basierenden Angriffstechniken beschrieben, welche auf einer fehlerhaften Verarbeitung von Anfragen basieren, welche zu einer unendlichen Wiederholung bestimmter programmatischer Vorgänge führen. Rekursionen sind typische Prozesse in der Datenverarbeitung, bei welchen durch iterative Vorgänge Probleme skaliert werden und Lösungen von Problemen auf iterativen Schleifen von immer kleineren Instanzen errechnet werden.

Rekursionen haben den großen Vorteil, dass sich mittels diesen auch komplexe Berechnungen bzw. programmatische Funktonen mit sehr einfachen Instruktionen ausführen lassen, jedoch führen Rekursionen schnell zu einem hohen Ressourcenverbrauch, da potenziell eine unendliche Anzahl an Iterationsschleifen möglich sind. Typischerweise werden Rekursionen durch begleitende Algorithmen gesteuert, sodass nach einer gewissen Anzahl an Iterationen oder einem plausiblen Ergebnis die Rekursionen beendet werden. Besteht nun die Schwachstelle der unkontrollierten Rekursionen, werden diese immer weiter fortgesetzt, sodass die Berechnungsschritte immer mehr Prozessorleistung und Arbeitsspeicher in Anspruch nehmen. Hierdurch steht fortwährend weniger Ressourcen für die anderen Aufgaben des Systems zur Verfügung, bis diese nicht mehr ausgeführt werden können und es zu einem Denial-of-Service kommt. Letztlich ist das betroffene System nicht mehr responsiv und kann nur durch einen Neustart, z. B. über die Beendung der Stromversorgung, wieder in Betrieb gesetzt werden. Weiterhin besteht die seltener auftretende Möglichkeit, dass unbegrenzte Rekursionen durch systemische Kontrollmaßnahmen vollständig abgebrochen werden und dabei Fehlerreports an den Auslöser versenden, welche vertrauliche Informationen über das System preisgeben, z. B. Hardwareausgestaltung, Speicherort im Arbeitsspeicher oder Dateipfade.

Typische Konsequenzen von uncontrolled Recursions sind also:

- Denial of Service: Durch unkontrollierte Rekursionen werden mehr und mehr Ressourcen des betroffenen Systems in Anspruch genommen, bis die Ausführung anderer Aufgaben sich verlangsamt und schließlich zum vollständigen Erliegen kommt.
- Information Disclosure: Werden unkontrollierte Rekursionen in einer Form beendet, welche zum Auslösen von Fehlerreports führt, können diese sensitive Informationen über das System preisgeben.

Bekanntgewordene Schwachstellen

- CVE-2018-20994: Der in die Programmiersprache Rust integrierte DNS-Handler Trust-DNS ging bei bestimmten DNS-Nachrichten in eine unendliche Rekursion über, welche das betroffene System in einen Denial-of-Service Zustand überführte.
- CVE-2020-6071: Die im DNS-Handler libmicrodns integrierte Verarbeitungsfunktion für mDNS-Nachrichten führte bei bestimmten mDNS-Nachrichten zu einer unendlichen Rekursion, welche das betroffene System in einen Denial-of-Service Zustand überführte.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über die Schwachstellen des Typs „unconrolled Recursion“ sind in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Angreifer müssen hierzu entsprechende auf die Schwachstellen angepasste Befehle oder von dem angegriffenen System zu verarbeitende Nachrichten senden. Um einen solchen Angriff auszuführen, muss der Angreifer daher lediglich in der Lage sein, Kommunikationsanfragen oder zu verarbeitende Datenpakete an das betroffene System zu senden. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden. Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.16 Out-of-bounds Write

Beschreibung

Die Schwachstelle *Out-of-bounds Write* (CWE-787) beinhaltet alle Sicherheitslücken und darauf basierende Angriffstechniken, die im Zusammenhang mit dem Schreiben von Daten außerhalb des vorgesehenen Speichers stehen.

Durch die Ausnutzung einer Out-of-bounds Write Schwachstelle sind Angreifer in der Lage, Daten außerhalb der Grenzen eines zugewiesenen Speicherbereichs zu schrei-

ben. Dies kann beispielsweise provoziert werden, indem mehr Daten in einen Puffer geschrieben werden, als dieser aufnehmen kann. Dies kann zur Überschreibung von Daten führen sowie zu Abstürzen betroffener Programme und Anwendungen. Zudem sind Angreifer dadurch potenziell in der Lage, beliebigen Code auszuführen. Im Wesentlichen kann ein Out-of-bounds Write auftreten, wenn die Länge/Größe von Eingabedaten größer ist als der dafür vorgesehene Speicherbereich, wenn Daten in einen inkorrekten Speicherbereich geschrieben werden oder wenn ein Programm den Speicherort oder die Länge/Größe der zu schreibenden Daten falsch kalkuliert. Wirksame Sicherungsmaßnahmen gegen Angriffe, welche diese Art von Schwachstellen ausnutzen, setzen vor allem auf eine angemessene Prüfung von Eingabedaten und des Schreibvorgangs hinsichtlich ausreichend großer Speicherbereiche für die Zieldaten.

Im Wesentlichen ermöglicht die Ausnutzung derartiger Schwachstellen durch Angreifer eine Verletzung der Verfügbarkeit, Vertraulichkeit und Integrität bestimmter Systeme und Daten herbeizuführen. Dies kann unter anderem folgende Konsequenzen haben:

- Information disclosure: Wenn Angreifer Daten außerhalb vorgesehener Speicherbereiche schreiben, können sie unter bestimmten Umständen beliebigen Code ausführen und dies dazu ausnutzen, illegitim sensible Daten auszulesen und Informationen zu stehlen.
- Denial of Service: Durch den Zugriffsversuch bzw. Zugriff auf nicht vorgesehene Speicherbereiche können Angreifer undefinierte Zustände und Abstürze herbeiführen, welche die Verfügbarkeit von Systemen und Programmen einschränken können.
- Modify Memory & Remote Code Execution: Durch die Ausnutzung derartiger Schwachstellen können Angreifer Speicherbereiche illegitim überschreiben und dadurch (die Integrität von) Daten beschädigen. Zudem können Angreifer unter bestimmten Umständen beliebigen Code ausführen.

Bekanntgewordene Schwachstellen

- CVE-2021-31226: Aufgrund der fehlenden Überprüfung der Größe/Länge eingehender Anfragen im Zusammenhang mit HTTP POST können einen Buffer Overflow provozieren Angreifer Remote Code Execution erzwingen, indem manipulierte HTTP-POST-Anfragen übermittelt werden, deren Uniform Resource Identifier (URI), die länger als 50 Bytes ist.

- CVE-2020-15795: Durch eine fehlerhafte Validierung der DNS-Domain-Name-Label-Parsing-Funktionalität können privilegierte Angreifer Schreibvorgänge über das Ende der zugewiesenen Struktur hinaus erwirken, sodass es zur Remode Code Execution kommt.
- CVE-2020-17437: Aufgrund einer unzureichenden Längenprüfung können Angreifer, indem sie ein "Urgent"-Flag innerhalb eines TCP-Pakets setzen, ein Out-of-Bounds Write provozieren und Denial of Service Zustände herbeiführen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes unter Ausnutzung von Schwachstellen des Typs *Out-of-bounds Write* sind in den meisten Fällen keine Authentifizierungsmechanismen erforderlich. Dabei müssen Angreifer entsprechende Netzwerkpakete an das Ziel schicken, welche durch Ausnutzung der Schwachstelle einen Out-of-bounds Write provozieren. Um einen solchen Angriff auszuführen, muss der Angreifer somit lediglich in der Lage sein, eine Kommunikationsverbindung zum betroffenen System aufzubauen. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.2.17 Loop

Beschreibung

Unter der CWE-Nummer CWE-835 „Loop“ werden eine Bandbreite von Schwachstellen bzw. auf diesen basierenden Angriffstechniken beschrieben, welche auf einer fehlerhaften Verarbeitung von Anfragen basieren, welche zu einer unendlichen Wiederholung derselben Programmteile führen. Diese erfolgen z. B. durch im Code festgeschriebene Wiederholungen einer Handlung, deren Stopp-Bedingung nicht erfüllt werden kann oder durch Angreiferhandlungen in einen unerreichbaren Zustand überführt werden können.

Die Abtrennung zu CWE-674 liegt insbesondere in den fundamentalen technischen Unterschieden: Bei CWE-674 werden im Rahmen von Rekursionsberechnungen eine unendliche Anzahl an Rekursionen ausgeführt, da die Bedienungen zur Beendigung der Rekursion nicht getroffen werden. Bei CWE-835 liegen grundlegende programmatische Schwachstellen vor, welche zu einer unendlich wiederkehrenden Ausführung von Programmteilen (Schleifen bzw. englisch „Loop“) führen. Beispielhaft sind z. B. Wiederkehrende Abfragen bei bestimmten Rückmeldungen im Netzwerkverkehr. Verliert ein Programm oder ein System die Verbindung zu einem Kommunikationspartner, sehen die meisten Programme bzw. Systeme hierfür einen automatischen Verbindungsaufbau vor. Werden hierfür keine zeitlichen Abstände oder eine maximale Anzahl an Verbindungsaufbauten festgeschrieben, folgt daraus, dass eine unendliche Wiederholung an Verbindungsaufbauten durchgeführt wird, solange keine Verbindung dauerhaft hergestellt werden kann. In anderen Fällen kommt es z. B. zu dauerhaft wiederholten Arbeitsspeicherabfragen nach bestimmten Werten, die beim Auslesen nicht erwarteter Werte zu einer permanenten Wiederholung des Auslesens führen. In beiden Fällen werden für die immer wiederkehrende Wiederholung der Abfragen bzw. Programmteile Ressourcen des betroffenen Systems aufgewendet, welche anderen Aufgaben der Systeme nicht zur Verfügung stehen. Bei einem extremen Ausmaß führt dies zu Denial-of-Service Zustände, bei denen die eigentlichen Aufgaben eines Systems nur noch verlangsamt oder gar nicht mehr ausgeführt werden können.

Typische Konsequenzen von „Loop with unreachable Exit condition“ sind also:

- Denial of Service: Die Ausführung einer Schleife ohne erreichbare Ausgangsbedingung führt zu erhöhtem Ressourcenverbrauchs des betroffenen Systems und kann dazu führen, dass ein Denial of Service-Zustand eintritt, bei dem die eigentlichen Aufgaben des Systems verlangsamt oder gar nicht mehr erfüllt werden können.

Bekanntgewordene Schwachstellen

- CVE-2021-27565: Der InterNiche TCP/IP Stack führt bei einer validen http Anfrage zu einer unendlichen Schleife, da hierbei eine fehlerhafte Codeabfrage zu einer nicht erreichbaren Exit Bedingung führt.
- CVE-2021-12663: Der DNS Handler Unbound kann mit spezifischen Abfragen dazu geführt werden, massenhaft Anfragen an von Angreifern ausgewählte Ziele auszuführen.

Ausnutzung der Schwachstellen

Zur Durchführung eines Cyberangriffes über die Schwachstellen des Typs „Loop with unreachable Exit condition“ sind in den meisten Fällen keine Authentifizierungsmechanismen notwendig. Angreifer müssen hierzu entsprechende auf die Schwachstellen angepasste Befehle oder von dem angegriffenen System zu verarbeitende Nachrichten senden. Um einen solchen Angriff auszuführen, muss der Angreifer daher lediglich in der Lage sein, Kommunikationsanfragen oder zu verarbeitende Datenpakete an das betroffene System zu senden. Abhängig vom betroffenen Standard, kann eine solche Kommunikation innerhalb eines lokalen Netzwerkes oder von außerhalb des Netzwerkes über WAN oder Internetverbindungen durchgeführt werden.

Neben der bestehenden oder temporären Kommunikationsverbindung über den entsprechenden Standard, müssen die Angreifer zum einen die entsprechende Netzwerkadresse (bei TCP/IP die IP-Adresse) kennen oder durch massenhafte zufällige Anfragen erkennen und zum anderen die bestehende Schwachstelle und die genaue Art der hierfür notwendigen manipulierten Parameter kennen.

4.3 Zusammenfassung AP 2

Die in AP 1 erfassten Schwachstellen mit Bezügen zur Netzwerkkommunikation ergeben eine ermittelte Datenbasis von 280 Schwachstellen. Im AP 2 konnten diese nun mittels der CWE-Kennungen gruppiert werden, sodass eine Übersicht über typische Schwachstellen mit Netzwerkbezug ermittelt wurde. Die so erstelle Übersicht mit 19 typischen CWE-Kennungen ermöglichte nicht nur eine Gruppierung der Schwachstellen, sondern auch eine Übersicht über mit diesen Schwachstellen einhergehenden Angriffsmöglichkeiten. Insgesamt ergab sich somit eine Übersicht über sich typischerweise durch Schwachstellen in der Netzwerkkommunikation ergebende Angriffsmöglichkeiten. Die so ermittelten Angriffsmöglichkeiten konnten nun als Basis für die im Arbeitspaket 3 durchgeführten Arbeiten zur Ermittlung und Beschreibung konkreter Angriffsmöglichkeiten auf IT-Systeme mit netzwerktechnischen Verbindungen im Zusammenhang mit kerntechnischen Anlagen weiterführend genutzt werden

5 AP 3: Bewertung der sich ergebenden Angriffsmöglichkeiten netzwerktechnischer Schwachstellen in Bezug auf kerntechnische Anlagen

Mit den bisherigen Arbeitspaketen wurden zum einen typische Schwachstellen mit Relevanz für die Netzwerkkommunikation ermittelt und zum anderen die sich aus diesen Schwachstellen ergebenden Angriffsmöglichkeiten und potenziellen generischen Auswirkungen. Eine Bewertung solcher Angriffsmöglichkeiten für kerntechnische Anlagen und Einrichtungen ist nur möglich, wenn die in AP 2 erkannten Angriffsmöglichkeiten auf typischerweise in kerntechnischen Anlagen und Einrichtungen vernetzt genutzten IT-Komponenten bzw. IT-Systeme übertragen werden und im Hinblick auf diese Komponenten bewertet werden. Hierzu sind generische IT-Komponenten, wie sie typischerweise in kerntechnischen Anlagen Verwendung finden, zu identifizieren, um anschließend die Angriffsmöglichkeiten zu identifizieren.

5.1 Typische generische IT-Komponenten kerntechnischer Anlagen

In kerntechnischen Anlagen werden eine Vielzahl unterschiedlicher IT-Systeme eingesetzt, welche für sicherheits-, sicherungs- und cybersicherheitsrelevante Aufgaben innerhalb kerntechnischer Anlagen eingesetzt werden. Dabei bilden sich IT-Systeme aus einer einzelnen oder einer Vielzahl von IT-Komponenten, um umfassende Aufgaben zu erfüllen. So bestehen moderne Brandmeldeanlagen unabhängig vom Einsatzort aus mindestens einem, meistens mehreren, Servern, Feldgeräten wie Rauchmeldern und Alarmmeldern, Clients zur Bedienung und Management und Switches für den Aufbau einer Vernetzung zwischen all diesen Komponenten. Weiterhin können je nach Einsatzbereich und zugrundeliegendem Regelwerk Vernetzungen zu weiteren komplexen IT-Systemen wie zentralen Gefahrenmeldeanlagen oder zu externen Stellen wie Notrufmeldestellen erfolgen.

Diese für den Aufbau komplexer IT-Systeme notwendigen IT-Komponenten lassen sich in generische Gruppen und Kategorien entsprechend ihrer technischen Funktionsweisen und Aufgaben aufteilen und geben einen Überblick über entsprechende relevante Aufgaben und Funktionen solcher IT-Komponenten für kerntechnische Anlagen, ohne hierbei spezifische Details sicherheits- und sicherungsrelevanter IT-Systeme öffentlich zugänglich zu machen.

Im Folgenden werden insgesamt neun generische IT-Komponenten beschrieben, welche typischerweise als Teil von IT-Systemen für sicherheits- und sicherungsrelevante Aufgaben in kerntechnischen Anlagen verwendet werden und hierbei einen gewissen Grad der datentechnischen Vernetzung erreichen.

Speicherprogrammierbare Steuerung

Speicherprogrammierbare Steuerungen (SPS) beschreiben leittechnische Systeme, welche zur Steuerung steuerbarer elektrischer, elektronischer, mechanischer oder hydraulischer Systeme eingesetzt werden. In kerntechnischen Anlagen werden solche Systeme für eine Vielzahl von Aufgaben eingesetzt. Speicherprogrammierbare Steuerungen bieten grundsätzlich die Möglichkeit zur Vernetzung an, zum einen zur Steuerung angeschlossener Systeme und Feldgeräte und zum anderen teilweise zur Vernetzung von speicherprogrammierbaren Steuerungen untereinander mit weitergehenden leittechnischen Netzwerken oder mit sonstigen IT-Systemen wie Programmiergeräten.

Die meisten heutzutage angebotenen speicherprogrammierbaren Steuerungen bieten die Möglichkeit zur Nutzung gängiger datentechnischer Verbindung, zumeist über TCP/IP basierte Anschlüsse sowie weitere Protokolle. Speicherprogrammierbare Steuerungen sind daher von einer großen Zahl an potenziellen netzwerktechnisch relevanten Angriffsmöglichkeiten betroffen; abhängig von tatsächlichen Schwachstellen in den Steuerungen bzw. deren Subkomponenten für die datentechnische Kommunikation. Zu den wesentlichen zuordenbaren Angriffsmöglichkeiten zählen die CWEs 20, 125, 130, 190, 191, 330, 331, 400, 415, 674, 787 und 835.

Server

Server sind zentrale IT-Komponenten der meisten IT-Systeme mit komplexen Funktionen oder mit Netzwerken aus einer Vielzahl von IT-Komponenten. Sie dienen zur Verarbeitung und Aufbewahrung von Daten und Programmen für sämtliche mit den Servern kommunizierenden IT-Komponenten innerhalb eines IT-Systems und können auch über IT-Systemgrenzen von verschiedenen IT-Systemen gleichzeitig genutzt werden. Eingesetzt werden diese Komponenten in allen denkbaren Funktionen innerhalb kerntechnischer Anlagen.

Da Server insbesondere zur vernetzten Datenverarbeitung und Bereitstellung genutzt werden, nutzten sie zumeist typische TCP/IP basierte Kommunikationsprotokolle, in

Spezialsystemen jedoch auch für die entsprechenden Anwendungen angepasste proprietäre und spezialisierte Protokolle.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 330, 331, 400, 415, 674, 787 und 835.

Virtuelle Server

Virtuelle Server sind Server, die rein virtuell realisiert werden und nicht auf eine spezifische Hardware festgeschrieben sind. Sie benötigen immer weiterhin eine Hardwareplattform, können jedoch auf unterschiedlichen Plattformen installiert werden, parallel genutzt werden und es können mehrere virtuelle Server auf derselben Hardwareplattform installiert werden. Ihre Funktionen sind analog zu der eines Servers, sie ermöglichen jedoch weitergehenden Flexibilität und eine effizientere Ressourcenausnutzung. Da mehrere virtuelle Server zumeist auf derselben Hardware innerhalb der virtuellen Umgebung ausgeführt werden, bietet sich eine direkte Kommunikation zwischen Servern ebenso an wie eine weitreichende Vernetzung mit den zugehörigen weiteren IT-Komponenten.

Virtuelle Server sind daher potenziell von den gleichen kommunikationstechnisch relevanten Schwachstellen betroffen wie konventionelle Server, darüber hinaus jedoch auch von Schwachstellen, die z. B. rein virtuelle Umgebungen und deren Kommunikation betreffen.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 330, 331, 400, 415, 674, 787 und 835.

Switches und Router

Switches und Router dienen zum Aufbau von Netzwerken zwischen IT-Komponenten und damit als elementare Einheit innerhalb von IT-Systemen, sowie darüber hinaus auch als kommunikative Zwischenebene von IT-Systemen. Switches bilden hierbei die Verwaltungs- und Abwicklungsebene des IP-basierten Netzwerkverkehrs und nehmen damit eine zentrale Rolle in diesem ein. Moderne Switches bieten umfassende Konfigurationsmöglichkeiten zur Festlegung, welche Komponente und welches System in welcher Form untereinander kommunizieren können, ob Kommunikation gerichtet ist und welche Art von Kommunikation über offene Ports gestattet wird. Weiter ermöglichen moderne

Switches sogenannte VLANs, also virtuelle Netzwerke, bei welchem die am Switch angeschlossenen IT-Komponenten nur innerhalb eigener begrenzter virtueller Netzwerkumgebungen kommunizieren können. Unter Routern versteht man darüber hinaus Systeme zur Kommunikation des internen Netzwerks nach außen, also z. B. in ein deutlich größeres Netz oder das Internet.

Da durch Switches die Kommunikation einer Vielzahl von IT-Komponenten bzw. IT-Systemen verbunden ist und elementare Aufgaben des Netzwerkverkehrs übernommen wird, sind diese für potenzielle IT-basierte Angriffe über und auf den Netzwerkverkehr besonders relevant.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 200, 306, 330, 331, 400, 415, 674, 787 und 835.

Feldgerät

Als Feldgeräte werde solche Komponenten beschrieben, welche in leittechnischen Systemen Messwerte bzw. Daten erheben, und Steuerungsbefehle ausführen. Dies können Temperaturfühler, Ventilsteuerungen, Startvorrichtungen und viele weitere Typen von Feldgeräten sein. Feldgeräte sind zumeist an eine einzelne oder mehrere leittechnische IT-Komponenten wie speicherprogrammierbare Steuerungen oder Controller angeschlossen und führen deren Befehle aus bzw. leiten ihre Messwerte und andere Daten an diese zur Verarbeitung und Entscheidungsfindung weiter.

Feldgeräte nutzen eine Vielzahl von unterschiedlichen Kommunikationsstandards wie auch speicherprogrammierbare Steuerungen und Controller: auf TCP/IP basierende Standards wie Profinet, Modbus TCP oder Industrial Ethernet, aber auch BUS-Standards, proprietäre Standards und analoge Datenübertragung. Abhängig von den eingesetzten Standards, sind somit unterschiedliche Angriffsmöglichkeiten denkbar.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 330, 331, 400, 415, 674, 787 und 835.

Client

Als Clients werden solche Systeme beschrieben, auf welchen Anwender zur Arbeitsausführung notwendige Programme bedienen, welche dann mit Servern und anderen IT-

Komponenten zur weiteren Verarbeitung und Datenbereitstellung verbunden sind. Sie bilden damit zumeist die Mensch-Maschine-Schnittstelle und sind der zentrale Bedienort für IT-Systemanwender. Typischerweise werden Clients aus regulären und eingeschränkt funktionalen PCs realisiert, die für die jeweiligen Aufgabe des Clients angepasst werden. Typischerweise werden Clients über TCP/IP mit den anderen IT-Komponenten des IT-Systems verbunden.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 200, 306, 330, 331, 400, 415, 674, 787 und 835.

Servicegerät/Engineering Stations

Im Gegensatz zu Clients für Systemanwender werden Servicegeräte und Engineering Stations als IT-Komponenten beschrieben, welche zur Administration, Konfiguration und Parametrierung verwendet werden. Servicegeräte werden in diesem Fall temporär, Engineering Stations dauerhaft mit den relevanten IT-Komponenten bzw. IT-Systemen verbunden und ermöglichen damit die Durchführung administrativer Arbeiten.

Dauerhaft verbundene Engineering Stations können über eine weitere Zahl an kommunikativen Schnittstellen, abhängig von den übrigen IT-Komponenten, dem Hersteller und den Anforderungen installiert werden. Servicegeräte werden darüber hinaus über klassische Netzwerkprotokolle, aber auch USB und andere datentechnisch relevante Schnittstellen im Bedarfsfall verbunden, anhängig vom zum administrierenden Gerät.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 200, 306, 330, 331, 400, 415, 674, 787 und 835.

Firewall

Firewalls beschreiben Systeme zur Beschränkung und Schutz des Netzwerkverkehrs. Firewalls dienen der Grenzsetzung von Netzwerkverkehr, können darüber hinaus diesen jedoch auch je nach Ausgestaltung überwachen und protokollieren. Firewalls werden insbesondere in Fällen eingesetzt, in denen gesicherte und ungesicherte Netzwerkverbindungen, z. B. von Standorten mit dem freien Internet, abgesichert werden sollen. Firewalls und Switche können dabei ähnliche Funktionen aufweisen oder innerhalb eines

Gerätes vereint werden, jedoch zeichnen sich dedizierte Switche durch ihre umfassenden Anschluss- und Netzwerkfunktionen aus, während Firewalls insbesondere den Netzwerkverkehr überwachen und absichern.

Als Systeme zur Absicherung der Netzwerkkommunikation und insbesondere der Netzwerke nach außen sind Firewalls von besondere im Interesse im Rahmen der zu schützenden Kommunikation und der Angreifbarkeit durch Schwachstellen in Netzwerkkomponenten.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 200, 306, 330, 331, 400, 415, 674, 787 und 835.

KVM-Switch

KVM (Keyboard, Video, Mouse) Switche sind Geräte zur Übertragung von Video- und Inputsignalen über längere Distanzen oder auf mehrere Geräte in schaltbarer Reihenfolge. KVM-Switche funktionieren typischerweise in unterschiedlicher Form, abhängig von der zu überbrückenden Distanz. KVM-Switche im Nahfeld übertragen die Signale anschlussgleich, also über die spezifischen Anschlüsse für Maus, Tastatur und Videosignale. Werden große Distanzen mit KVM-Switchen überwunden, werden diese zumeist über Netzwerksignale angesteuert. In diesem Fall findet eine Übertragung zumeist über TCP/IP basierte Kommunikationsprotokolle statt.

Grundsätzlich sind KVM-Switche in ihrer Funktionalität stark eingeschränkt auf die Übertragung von Eingaben und Bildsignalen. Solche KVM-Switche, welche auf TCP/P basieren, sind dennoch teils von netzwerkrelevanten Angriffsmöglichkeiten betroffen.

Zu den zuordenbaren Angriffsmöglichkeiten zählen im Wesentlichen die CWEs 20, 125, 130, 190, 191, 330, 331, 400, 415, 674, 787 und 835.

5.2 Angriffsmöglichkeiten über die Netzwerkkommunikation von SPS

Speicherprogrammierbare Steuerungen sind ein zentraler Bestandteil verfahrenstechnischer Anlagen und digitaler Steuerungssysteme, die unterschiedlichste Anwendungsbereiche in nahezu allen Industriebereichen haben. Auch im kerntechnischen Bereich sind speicherprogrammierbare Steuerungen zentrale Komponenten von Sicherheits- und Si-

cherungssystemen, die entsprechend relevant für sicherheits-, sicherungs- und schutzrelevante Funktionen sind. Durch ihre oftmals direkten Verbindungen zu Feldgeräten bzw. Geräten auf Feldebene sind speicherprogrammierbare Steuerungen ein kritisches Angriffsziel für Bedrohungsakteure, um ggf. auch physikalische Auswirkungen und Störungen mit Hilfe von Cyberangriffshandlungen herbeizuführen. Je nach Anwendungsgebiet und den genauen Umständen sind Netzwerke mit speicherprogrammierbaren Steuerungen weit vernetzt oder auch isoliert (insbesondere bei sicherheits- und sicherungskritischen Systemen).

Im Vergleich zu anderen generischen IT-Systemen kamen bei speicherprogrammierbaren Steuerungen in der Vergangenheit typischerweise proprietäre, herstellerspezifische Lösungen (zum Beispiel von Siemens, Omron oder Schneider Electric) in Bezug auf die Kommunikation einzelner Komponenten zum Einsatz, die üblicherweise auch nicht untereinander kompatibel waren. Es entwickelten sich mit zunehmender Verbreitung jedoch industrielle Standards, die heutzutage überwiegend eingesetzt werden. Speicherprogrammierbare Steuerungen besitzen dabei unter Umständen in ihrem modularen Aufbau auch Erweiterungsmodule für bestimmte Kommunikationsformen (z. B. Ethernet, Modbus usw.) Die Betriebssysteme sind dabei entweder für klare Aufgaben definierte geschlossene Echtzeit-Umgebungen oder auch mittlerweile vollwertige Betriebssysteme.

Grundlagen der Kommunikation

Die Kommunikation im Zusammenhang mit speicherprogrammierbaren Steuerungen findet typischerweise grundsätzlich auf drei Ebenen statt: von übergeordneten administrativen Netzwerken oder Engineering Workstations bzw. Servicegeräten zu einzelnen SPS, zwischen einzelnen SPS untereinander und von SPS zu einzelnen Feldgeräten und Komponenten. Insbesondere die Kommunikation zu den Feldgeräten und Komponenten ist für den Betrieb der SPS essenziell. Die Kommunikation zu anderen SPS oder übergeordneten Entitäten wie Engineering Work Stations kann dagegen eingeschränkt sein und beispielsweise nur temporär erfolgen.

Obwohl in der Vergangenheit oftmals proprietäre Protokolle mit eingeschränkter oder nicht vorhandener Kompatibilität zu anderen Herstellern eingesetzt wurden, findet die Kommunikation in der heutigen Zeit dagegen auch über weit verbreitete Standards oder Open-Source Protokolle statt. Oftmals werden TCP/IP basierte Kommunikationsstan-

dards für SPS untereinander oder in Verbindung mit übergeordneten Netzwerken genutzt. Typischerweise werden über die SPS-Daten und Informationen über den Status und Betriebszustand von Systemen bzw. ganzen Anlagen gesammelt, die über die entsprechende Kommunikation mit den Feldgeräten erhoben werden. Außerdem können Prozesse und Komponenten/Geräte gesteuert werden, indem entsprechende Befehle übermittelt werden. Dadurch können physikalische Zustandsänderungen herbeigeführt werden. Die von den SPS erhobenen Informationen können ggf. an ein übergeordnetes System zu Archivierungs-/Dokumentationszwecken oder zur Darstellung des Systemzustands übermittelt werden, wodurch die Lage in Echtzeit abgebildet und beurteilt werden kann. Insbesondere für sicherheits- und sicherungsrelevante Systeme mit entsprechenden schutzrelevanten Funktionen sind sensible Kommunikationsnetze mit SPS bewusst isoliert. In den meisten Fällen ist dabei mindestens die reguläre Informationstechnologie (z. B. Büro-IT) von der Verfahrenstechnologie getrennt (OT-Netzwerk, Operational Technologie).

Anwendbare Schwachstellen

Aufgrund der Kritikalität der SPS für prozesstechnische Abläufe und die potenziell verheerenden Auswirkungen von Cyberangriffen auf diese, die ggf. auch physische Auswirkungen haben können, sind SPS ein primäres Ziel von Angreifern. Auch wenn erweiterte Sicherungsmaßnahmen wie beispielsweise Air-Gaps zur Sicherung eingesetzt werden, ist es insbesondere durch die Ausnutzung von Schwachstellen für Angreifer in der Vergangenheit möglich gewesen, Angriffe auf diese Systeme auszuführen. Die hierbei in AP 2 beschriebenen und auf SPS allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Speicherprogrammierbare Steuerungen sind zur bestimmungsgemäßen Ausführung ihrer Funktionen auf ein angemessenes Management ihrer verfügbaren Ressourcen, insbesondere des Arbeitsspeichers angewiesen. Wenn durch Schwachstellen im Zusammenhang mit der Netzwerkkommunikation illegitime Zugriffe auf den Arbeitsspeicher ermöglicht werden, kann es zu Einschränkungen in der Betriebsbereitschaft und im Betrieb der SPS kommen. Relevante Schwachstellen umfassen in diesem Zusammenhang beispielsweise Out-of-Bounds Read/Write oder Integer Overflow/Underflow sowie Uncontrolled Ressource Consumption/Loop with Unreachable Exit Condition. Zudem basieren die Schwachstellen oftmals auf einer fehlerhaften Handhabung von Eingangsparametern (Improper Input Validation, Improper Handling of Length, Parameter Inconsistency etc.).

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Die Authentifizierung in Bezug auf SPS ist insbesondere bei der Parametrierung und Konfiguration ein kritischer Faktor, wenn die Aufgaben und vorgesehenen Prozesse des Geräts definiert werden. Die Ausnutzung von Schwachstellen in der Authentifizierung ermöglichen Angreifern ggf. die Übernahme der Kontrolle oder weitere maliziöse Handlungen.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf SPS ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Speicherprogrammierbare Steuerungen sind insbesondere im industriellen Umfeld/als Teil von industriellen Steuerungssystemen typischerweise von kaufmännischen oder verwaltungstechnischen Netzwerken, die oftmals vielfältige Verbindungsmöglichkeiten zu externen Diensten bieten, isoliert. Angreifer müssen zur Ausnutzung von Schwachstellen somit Verbindungs- oder Zugriffsmöglichkeiten in diese typischerweise separierten Netzwerke haben, ggf. auch über AirGaps hinweg. Dabei unterscheiden sich die sich ergebenden Angriffsmöglichkeiten insbesondere im Aufbau des entsprechenden Netzwerks in Form einer dauerhaften Netzwerkverbindung nach außen und einem Netzwerk, welches auf dauerhafte Netzwerkverbindungen verzichtet. Ohne permanente Netzwerkverbindung nach außen ist für eine erfolgreiche Angriffsmöglichkeit eine Einwirkung innerhalb des Netzwerks notwendig, die Angreifern die Nutzung des Netzwerks für die Ausnutzung der Schwachstelle ermöglicht.

Mit einer permanenten Verbindung nach außen ist Angreifern eine entsprechende Schwachstellenausnutzung möglich, wenn eventuelle Sicherungsmaßnahmen überwunden oder keine Sicherungsmaßnahmen bei der Kommunikation des Servers nach Außen getroffen werden.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf SPS über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen. Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff erforderlich, dieser ermöglicht in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung:

- Informationsabfluss: Wenn durch die Ausnutzung von Kommunikationsschwachstellen im Zusammenhang mit SPS von diesen Informationen abfließen, erhalten potenzielle Angreifer dadurch beispielsweise Zugriff auf Prozessdaten und Informationen von Feldgeräten. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der betroffenen SPS und damit der zugehörigen IT-Systeme. Ggf. können dadurch Informationen zur Unterbrechung oder Störung relevanter Prozesse erlangt werden, um auch physische Auswirkungen bei einem potenziellen Angriff herbeizuführen.

- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der SPS deren Verfügbarkeit einschränken. Dies ist für SPS oftmals ein besonders kritisches Problem, weil diese in industriellen Umgebungen neben der Informationssammlung auch Steuerungsaufgaben übernehmen. Wenn die Verfügbarkeit eingeschränkt ist, können möglicherweise Prozesse gestört, abgebrochen oder anderweitig beeinflusst werden, sodass sich unter Umständen auch physische Auswirkungen ergeben.

- Authentifizierung: Die Authentifizierung dient bei SPS grundsätzlich zum Schutz vor unbefugten Zugriffen. Im Wesentlichen ermöglichen Schwachstellen im Zusammenhang mit der Authentifizierung bei der Kommunikation mit SPS den Angreifern somit illegitime Befehle zu übermitteln, die dann ggf. von den SPS ausgeführt werden und so den Angreifern entsprechende Einflussnahmen ermöglichen. Dies kann beispielsweise die Einstellung des Betriebs, die Änderung von Prozessen oder die Übermittlung anderweitiger Schadsoftware umfassen. Entsprechend kann die Vertraulichkeit, Verfügbarkeit und Integrität dadurch beeinträchtigt werden.

- Remote Code Execution: Durch Kommunikationsschwachstellen im Zusammenhang mit Remote Code Execution können Angreifer potenziell bei entsprechender Ausnutzung durch Übermittlung speziell gestalteter Nachrichten beliebigen Code auf der

SPS ausführen und beispielsweise den Betrieb beeinträchtigen oder anderweitig manipulieren. Da SPS oftmals die Schnittstelle zu Feldgeräten sind, können Angreifer unter bestimmten Umständen somit auch physischen Einfluss auf bestimmte Prozesse nehmen, sodass RCE-Schwachstellen im Zusammenhang mit SPS besonders kritisch einzustufen sind.

Potenzielle Auswirkungen auf IT-Systeme

Speicherprogrammierbare Steuerungen stellen typischerweise das Bindeglied zwischen Systemen und Komponenten auf der Feldebene und übergeordneten prozesstechnischen Netzwerken im Rahmen industrieller Steuerungen und Prozessleitsysteme dar. Sie sind essenziell für betriebliche, sicherheitstechnische und sicherungstechnische Prozesse, indem sie diese entsprechend steuern, konfigurieren oder überwachen. Die Besonderheit an Angriffen auf SPS ist somit, dass Angreifer potenziell physische Auswirkungen auf Prozesse oder Systeme und Komponenten provozieren können. Zudem handelt es sich bei SPS generell um lohnende Angriffsziele, da durch entsprechende Manipulationen Abläufe und Prozesse gestört oder gestoppt werden können. Zudem können Angreifer ggf. wertvolle Informationen erlagen, um weitere Angriffsschritte vorzubereiten und durchzuführen. Die Konsequenzen für Vertraulichkeit, Verfügbarkeit und Integrität bei Angriffen über Kommunikationsverbindungen unter Ausnutzung von Schwachstellen sind somit schwerwiegend. Da SPS in der Regel aufgrund ihrer benötigten Konnektivität zu den Feldgeräten/übergeordneten Schnittstellen weitläufig vernetzt sind, erstrecken sich die entsprechenden Auswirkungen möglicherweise über weite Bereiche einer Anlage. Auch isolierte Systeme können betroffen sein, wenn Angreifer Air-Gaps überwinden.

Die tatsächlichen Konsequenzen sind abhängig vom Gesamtaufbau des betroffenen industriellen Steuerungssystems bzw. dem angeschlossenen Netzwerk. SPS wurden in der Vergangenheit häufig nicht nach dem Security-by-Desgin Prinzip entwickelt und weisen somit potenziell kritische Schwachstellen auf, die entsprechend ausgenutzt werden können. Die tatsächlichen potenziellen Auswirkungen hängen somit auch zu einem großen Teil von den übergeordneten Sicherungsmaßnahmen des Systems und der Anlage ab. Diese umfassen unter anderem eine entsprechende Segmentierung des Netzwerks, Härtung, den Einsatz virtueller Umgebungen und von Firewalls. Wenn sich Schwachstellen in diesen Bereichen umgeben, die Angreifer für ihre Zwecke missbrauchen, ergeben sich oftmals schwerwiegende Auswirkungen. Wenn zur Überwachung bzw. Steuerung von industriellen Prozessen eingesetzt SPS ausfallen, kann es zum vollständigen

Ausfall betroffener Systeme und Prozesse kommen, die weitreichende Auswirkungen auf das Gesamtsystem haben können.

5.3 Angriffsmöglichkeiten über die Netzwerkkommunikation von Servern

Server dienen als zentrale IT-Komponenten zur Verarbeitung und Bereitstellung von Informationen. In kerntechnischen Anlagen und Einrichtungen sind Server zentrale relevante IT-Komponenten für Aufgaben und Funktionen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung. Die meisten modernen, auf digitalen Technologien basierenden, Systeme basieren auf zentralen Programmen, welche auf vernetzten Servern ausgeführt werden und die zugehörigen IT-Komponenten ansteuern.

Server zeichnen sich dadurch aus, dass ihre Soft- und Hardware variable ist und von verschiedenen Herstellern angeboten wird. Als Betriebssysteme kommen hierbei überwiegend Linux Derivate, aber auch Microsoft Windows Server und proprietäre Betriebssysteme zum Einsatz. Anschließend werden die für den Betrieb und die Ausführung aller Aufgaben des Servers notwendige Software installiert. Als Hardware werden typischerweise verbreitete Standardkomponenten installiert. Die Netzwerkhardware wird hierbei zumeist über umfassend verbreitete und angebotene Standardsoftware und Hardware realisiert wie kommerzielle oder freie TCP/IP Stacks.

Grundlagen der Kommunikation

Für die Durchführung ihrer Aufgaben und Funktionen sind Server auf Kommunikation mit anderen IT-Komponenten wie Clients, Feldgeräte und Steuerungssysteme angewiesen. Diese datentechnische Kommunikation wird im überwiegenden Einsatzfall über TCP/IP basierte Kommunikation realisiert, im Spezialanwendungsfall mittels proprietärer oder branchenspezifischer Protokolle. Server kommunizieren entsprechend ihrer Aufgaben und Funktion fortwährend und wiederkehrend mit anderen Komponenten, gerichtet und ungerichtet, wobei sowohl Server als auch ihre Kommunikationspartner die Kommunikation starten können.

Anwendbare Schwachstellen

Aufgrund der Notwendigkeit von Servern fortwährend und wiederkehrend sowie bidirektional zu kommunizieren und der typischen Anwendung von Standardsoft- und Hardware sind Server potenziell von sehr vielen unterschiedlichen Schwachstellentypen betroffen.

Die hierbei in AP 2 beschriebenen und auf Server allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, dazu gehören auch die Netzwerkkommunikation, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche Schwachstellen basieren zumeist auf der fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation).

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Hierzu zählen die Möglichkeiten zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function und die Improper Access Control.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Server ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Server werden hauptsächlich mittels TCP/IP basierenden Verbindungen innerhalb von IT-Systemen und IT-Netzwerken eingesetzt. Entsprechend zur Nutzung der Schwachstellen müssen Angreifer im Rahmen der sich ergebenden Angriffsmöglichkeiten temporären oder dauerhaften Zugang zu mindestens einer Komponente im Netzwerk

besitzen, welche datentechnisch mit dem betroffenen Server kommuniziert. Dabei unterscheiden sich die sich ergebenden Angriffsmöglichkeiten insbesondere im Aufbau des entsprechenden Netzwerks in Form einer dauerhaften Netzwerkverbindung nach außen und einem Netzwerk, welches auf dauerhafte Netzwerkverbindungen verzichtet. Ohne permanente Netzwerkverbindung nach außen ist für eine erfolgreiche Angriffsmöglichkeit eine Einwirkung innerhalb des Netzwerks notwendig, die Angreifern die Verwendung des Netzwerks für die Ausnutzung der Schwachstelle ermöglicht. Mit einer permanenten Verbindung nach außen ist Angreifern eine entsprechende Schwachstellenausnutzung möglich, wenn eventuelle Sicherungsmaßnahmen überwunden werden oder keine Sicherungsmaßnahmen bei der Kommunikation des Servers nach Außen getroffen werden.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Server über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen. Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff nötig, dieser ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Server sind als zentrale Komponenten in IT-Systemen elementar für die Speicherung und Verarbeitung von Informationen. Schwachstellen, die z. B. durch Fehler in der Verarbeitung der kommunikativen Nachrichten ermöglichen es Angreifern beliebige und spezifische Informationen von den Servern auszulesen. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der betroffenen Server und damit der zugehörigen IT-Systeme.

- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Sever deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Server dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk. In der Konsequenz können Server ihre Aufgaben nicht mehr Erfüllungen und damit in Abhängigkeit vom Aufbau des Systems die Verfügbarkeit des gesamten IT-Systems einschränken.

- Authentifizierung: Die meisten Server sehen Authentifizierungsmechanismen zum Schutz der Server vor unbefugten Zugriffen vor. Solche Maßnahmen werden für das Serverbetriebssystem, für Zugriffe von außerhalb, für Zugriffe auf einzelne Programme und/oder für spezielle Zugriffe angewendet. Schwachstellen in Authentifizierungsverhalten in der Kommunikation entstehen z. B. durch bestimmte Schwachstellen in der Belegung von Arbeitsspeicher, bei welchen spezifische Nachrichten eine Umgehung bestimmter Authentifizierungsmechanismen für einzelne Programme oder das Betriebssystem des Servers ermöglichen. In Abhängigkeit davon welche Authentifizierung ausgehebelt werden kann und welche Rechte hierbei durch die kommunikative Schwachstelle erreicht werden, können die betroffenen Server in ihrer Vertraulichkeit, Verfügbarkeit und Integrität eingeschränkt werden.
- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von fremdem Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von Servern ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Systemübernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit des Servers erheblich beeinflusst.

Potenzielle Auswirkungen auf Gesamtsysteme

Server sind zentrale IT-Komponenten innerhalb von IT-Systemen und damit insbesondere für die zentrale Verarbeitung von Daten und Informationen verantwortlich. Server werden in einer überwiegenden Anzahl von IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen eingesetzt. Werden Server entsprechend der sich ergebenden Angriffsmöglichkeiten angegriffen, greifen die Angreifer damit auf eine der zentralen IT-Komponenten im gesamten Netzwerk zu. In der Konsequenz werden die betroffenen Systeme in ihrer Vertraulichkeit, Verfügbarkeit und Integrität in Abhängigkeit der ausgenutzten kommunikativen Schwachstelle potenziell erheblich eingeschränkt.

Damit führen Angriffsmöglichkeiten über die Kommunikation auf Server im Falle von betrieblichen, sicherheits- und sicherungsrelevanten IT-Systemen unweigerlich zu Einschränken oder vollständigem Ausfall der zugehörigen IT-Systeme und damit deren Funktionen und damit zu potenziell schwerwiegenden Konsequenzen.

Die tatsächlichen Konsequenzen sind jedoch auch abhängig vom Gesamtaufbau des betroffenen IT-Systems bzw. angeschlossenem Netzwerk. Redundante Server können den Ausfall eines Servers kompensieren, getrennte Netzwerke reduzieren die Angriffsmöglichkeiten und initialen Einwirkungsmöglichkeiten bevor es zu Angriffsmöglichkeiten über die Kommunikation kommt, Sicherungsmaßnahmen und der Einsatz getrennter Netzwerke über VLANs und Firewalls ermöglichen weiteren Schutz der eingesetzten Netzwerke und schließlich können kritische IT-Systeme in einer solchen Form genutzt werden, in welchem im Bedarfsfall relevante IT-Komponenten unabhängig von den zentralen Servern einen begrenzten Funktionsumfang bereitstellen. Diese Sicherungsmmaßnahmen sind jedoch insbesondere abhängig von der Art der vorliegenden Schwachstelle innerhalb der Kommunikation und den sich ergebenden Angriffsmöglichkeiten.

5.4 Angriffsmöglichkeiten über die Netzwerkkommunikation von virtuellen Servern

Analog zu konventionellen Servern, bei welchen jeder Server auf seiner eigenen Hardwareplattform ausgeführt wird, dienen virtuelle Server, bei welchen sich mehrere virtuelle Server eine Hardwareplattform teilen, der Verarbeitung und Bereitstellung von Informationen. In kerntechnischen Anlagen und Einrichtungen sind konventionelle Server zentrale relevante IT-Komponenten für Aufgaben und Funktionen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung. Virtuelle Server bieten die Möglichkeit einer erhöhten Flexibilität, eines einfachen Redundanzaufbaus und einer effizienten Ressourcen- und Kapazitätsnutzung. Weiterhin ermöglichen sie den einfacheren Aufbau bzw. die Integration der Server in ein umfassendes IT-Netzwerk. Auf einer Hardwareplattform können mehrere virtuelle Serverkomponenten desselben IT-Systems sowie auch unterschiedlicher IT-Systeme installiert werden.

Virtuelle Server werden auf einem sogenannten Hypervisor ausgeführt, einer Systemumgebung, die das Ausführen eines oder mehrerer virtueller Server ermöglicht. Der

Hypervisor teilt den entsprechenden virtuellen Servern anteilig Ressourcen der genutzten Hardwareplattform (CPU-Kapazität, Arbeitsspeicherbereiche, Festplattenspeicher und Netzwerkkapazität) zu, die virtuellen Server können anschließend unabhängig voneinander ausgeführt werden und mit entsprechenden Betriebssystemen und Software analog zu konventionellen Servern ausgestattet werden. Als Hardwarebasis können reguläre Serverhardware, darunter Netzwerkhardware für die TCP/IP Kommunikation eingesetzt werden.

Grundlagen der Kommunikation

Wie konventionelle Server sind virtuelle Server zur Durchführung ihrer Aufgaben und Funktionen auf die Kommunikation mit anderen IT-Komponenten wie Clients, Feldgeräte und Steuerungssysteme angewiesen. Diese datentechnische Kommunikation wird im überwiegenden Einsatzfall über TCP/IP basierte Kommunikation realisiert, wobei eine netzwerktechnische Hardware von allen virtuellen Servern auf einem Hypervisor genutzt wird. Kommunikationstechnisch kann die Kommunikation der virtuellen Server mittels VLAN eines Switches getrennt werden. Hierzu sind die Hypervisoren ausgelegt, jedoch wird dennoch von allen virtuellen Servern eines Hypervisors die gleiche Kommunikationshardware genutzt.

Anwendbare Schwachstellen

Aufgrund der Notwendigkeit von virtuellen Servern fortwährend und wiederkehrend sowie bidirektional zu kommunizieren und der typischen Anwendung von Standardsoft- und Hardware sind Server potenziell von sehr vielen unterschiedlichen kommunikationstechnischen Schwachstellentypen betroffen. Virtuelle Server sind darüber hinaus potenziell von anwendbaren kommunikationstechnischen Schwachstellen betroffen, welche über die Funktionsweisen der virtuellen Server bzw. Hypervisoren wirken. Hierbei werden die gemeinsamen Systemressourcen wie die für die TCP/IP genutzten Kommunikationsmodule ausgenutzt, um von einem virtuellen Server auf andere virtuelle Server desselben Hypervisors zuzugreifen.

Die in AP 2 beschriebenen und auf Server allgemein anwendbaren Schwachstellen lassen sich hierbei in vier Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die meisten Programme und Funktionen, dazu gehören unter anderem auch die Netzwerkkommunikation, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounds Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Derartige Schwachstellen basieren zumeist auf der fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation).

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Hierzu zählen die Möglichkeiten zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function und die Improper Access Control.

Schwachstellen der Virtualisierung: Virtuelle Server werden auf einer gemeinsamen Hardwareplattform mittels eines Hypervisors verwendet. Schwachstellen der gemeinsam genutzten Hardware wie der Netzwerkkommunikation oder der Behandlung des Arbeitsspeichers, aber auch direkte Schwachstellen des Hypervisors ermöglichen einen Angriff über die virtuellen Grenzen hinweg.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf virtuelle Server ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Virtuelle Server werden hauptsächlich mittels TCP/IP basierenden Verbindungen innerhalb von IT-Systemen und IT-Netzwerken eingesetzt. Entsprechend

müssen Angreifer zur Nutzung der Schwachstellen im Rahmen der sich ergebenden Angriffsmöglichkeiten temporären oder dauerhaften Zugang zu mindestens einer Komponente im Netzwerk besitzen, welche datentechnisch mit dem betroffenen virtuellen Server kommuniziert. Dabei unterscheiden sich die sich ergebenden Angriffsmöglichkeiten insbesondere im Aufbau des entsprechenden Netzwerks in Form einer dauerhaften Netzwerkverbindung nach außen und einem Netzwerk, welches auf dauerhafte Netzwerkverbindungen verzichtet. Ohne permanente Netzwerkverbindung nach außen ist ein für eine erfolgreiche Angriffsmöglichkeit eine Einwirkung innerhalb des Netzwerks notwendig, die Angreifern die Nutzung des Netzwerks für die Ausnutzung der Schwachstelle ermöglicht. Mit einer permanenten Verbindung nach außen ist Angreifern eine entsprechende Schwachstellenausnutzung möglich, wenn eventuelle Sicherungsmaßnahmen überwinden oder keine Sicherungsmaßnahmen bei der Kommunikation des Servers nach Außen getroffen werden.

Darüber hinaus können bei virtuellen Servern Schwachstellen der Virtualisierung genutzt werden, um von einem virtuellen Server auf einen anderen virtuellen Server des gleichen Hypervisors anzugreifen. Hierfür wird ein bestehender Zugriff auf mindestens einen virtuellen Server, z. B. durch vorhergehende Nutzung einer netzwerktechnischen Schwachstelle benötigt.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf virtuelle Server über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen. Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff nötig, dieser ermöglicht in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Virtuelle Server sind als zentrale Komponenten in IT-Systemen elementar für die Speicherung und Verarbeitung von Informationen. Schwachstellen, die z. B. durch Fehler in der Verarbeitung der kommunikativen Nachrichten ermöglichen es Angreifern beliebige und spezifische Informationen von den Servern auszulesen. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der betroffenen virtuellen Server und damit der zugehörigen IT-Systeme.

- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Sever deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Server dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk. In der Konsequenz können die Server ihre Aufgaben nicht mehr Erfüllungen und damit in Abhängigkeit vom Aufbau des Systems die Verfügbarkeit des gesamten IT-Systems einschränken. Bei virtuellen Servern kann ein Denial of Service Angriff auf einen Server potenziell alle Server des Hypervisors betreffen und damit potenziell IT-systemübergreifend wirkend.

- Authentifizierung: Die meisten virtuellen Server und Hypervisoren sehen Authentifizierungsmechanismen zum Schutz der Server bzw. Hypervisoren vor unbefugten Zugriffen vor. Solche Maßnahmen werden für das Server- und Hypervisorbetriebssystem, für Zugriffe von außerhalb, für Zugriffe auf einzelne Programme und/oder für spezielle Zugriffe angewendet. Schwachstellen in Authentifizierungsverhalten in der Kommunikation entstehen z. B. durch bestimmte Schwachstellen in der Belegung von Arbeitsspeicher, bei welchen spezifische Nachrichten eine Umgehung bestimmter Authentifizierungsmechanismen für einzelne Programme oder das Betriebssystem ermöglichen. In Abhängigkeit davon welche Authentifizierung ausgehebelt werden kann und welche Rechte hierbei durch die kommunikative Schwachstelle erreicht werden, können die betroffenen Server in ihrer Vertraulichkeit, Verfügbarkeit und Integrität eingeschränkt werden.

- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von virtuellen Servern ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Systemübernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit des Servers erheblich beeinflusst.

Potenzielle Auswirkungen auf Gesamtsysteme

Virtuelle Server sind zentrale IT-Komponenten innerhalb von IT-Systemen und damit insbesondere für die zentrale Verarbeitung von Daten und Informationen verantwortlich. Weiterhin ermöglichen virtuelle Server, dass auf einer Hardwareplattform mehrere Server eines IT-Systems, aber auch mehrere Server unterschiedlicher IT-Systeme, gleichzeitig betrieben werden. Insbesondere letzteres ermöglicht eine einfache hardwaretechnische Redundanz durch zwei oder mehrere virtuelle Serverumgebungen, die redundant zueinander funktionieren und sich im Fall eines Ausfall nahtlos ersetzen können.

Während Server umfassend in IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen eingesetzt werden, werden virtuelle Server bislang nur eingeschränkt genutzt bzw. etablieren sich nur langsam. Aufgrund der sich ergebenden größeren Vernetzungspotenziale und der angewendeten Hypervisoren, bei welchem potenziell mehrere betriebliche, sicherheits- bzw. sicherungsrelevante virtuelle Server auf dem gleichen Hypervisor und damit Hardwareplattform ausgeführt werden, gehen virtuelle Server zumeist mit einem erhöhten Grad der Vernetzung und damit der notwendigen netzwerktechnischen Kommunikation einher. Werden virtuelle Server entsprechend der sich ergebenden netzwerktechnischen Angriffsmöglichkeiten angegriffen, greifen die Angreifer damit nicht nur auf eine der zentralen IT-Komponenten im angeschlossenen Netzwerk des IT-Systems zu, sondern erreichen womöglich über die Vernetzungen gleichzeitig laufenden virtuellen Server anderer IT-Systeme auch IT-systemübergreifende Zugriffe. In der Konsequenz werden die betroffenen Systeme in ihrer Vertraulichkeit, Verfügbarkeit und Integrität in Abhängigkeit der ausgenutzten kommunikativen Schwachstelle potenziell erheblich eingeschränkt.

Damit führen Angriffsmöglichkeiten über die Kommunikation auf virtuelle Server im Falle von betrieblichen, sicherheits- und sicherungsrelevanten IT-Systemen unweigerlich zu Einschränken oder vollständigem Ausfall der zugehörigen IT-Systeme und damit deren Funktionen und damit zu potenziell schwerwiegenden Konsequenzen.

Die tatsächlichen Konsequenzen sind dabei abhängig vom Gesamtaufbau der betroffenen IT-Systeme bzw. angeschlossenen Netzwerke. Sicherungsmaßnahmen und der Einsatz getrennter Netzwerke über VLANs und Firewalls ermöglichen den Schutz der eingesetzten Netzwerke. Weiterhin können relevante IT-Systeme in derartig genutzt werden, dass im Bedarfsfall relevante IT-Komponenten unabhängig von den zentralen

Servern einen begrenzten Funktionsumfang bereitstellen. Diese Sicherungsmaßnahmen sind jedoch insbesondere abhängig von der Art der vorliegenden Schwachstelle innerhalb der Kommunikation und den sich ergebenden Angriffsmöglichkeiten.

5.5 Angriffsmöglichkeiten über die Netzwerkkommunikation von Switches

Ein Switch ist eine IT-Komponente zum Aufbau und Management eines IT-Netzwerks. Switche werden insbesondere bei komplexen IT-Systemen bestehend aus einer Vielzahl von IT-Komponenten und in IT-Netzwerken bestehend aus mehreren miteinander kommunizierenden IT-Systemen verwendet. Sie sind damit zentrale IT-Komponenten einer Vielzahl von IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung in kerntechnischen Anlagen und Einrichtungen. Je nach Ausgestaltung der verwendeten Switche können diese entweder auf Basis der komponentenspezifischen MAC-Adressen den Datenverkehr weiterleiten oder aber auf Basis von zugeordneten IP-Adressen, wobei letzteres zumeist mit umfassenderen Konfigurations- und Managementmöglichkeiten einhergeht. Diese Managementfunktionen werden zumeist zum einen genutzt, um den Netzwerkverkehr zu begrenzen, z. B. in dem im Netzwerk virtuelle Netzwerke (VLAN) etabliert werden und zum anderen zur Dokumentation und Logging des Netzwerkverkehrs.

Switches nutzten eigene Hardwareplattformen und können von einigen wenigen unterstützten Anschlüssen bis zu einer Vielzahl von Anschlüssen in 19“ Bauweise ermöglichen. Switches werden insbesondere für Ethernetkommunikation basierend auf Funk, RS-45 und Glasfasern genutzt und können wiederum mit weiteren Switchen verbunden für den Aufbau großer Netzwerke verbunden werden.

Grundlagen der Kommunikation

Switche dienen dem Aufbau, Erhalt und Management eines datentechnischen Netzwerks angeschlossener IT-Komponenten. Als zentrale Kommunikationsschnittstelle zwischen den IT-Komponenten haben sie eine zentrale Rolle in digitalen Netzwerken und stellen die Kommunikation aller IT-Komponenten des zugehörigen IT-Systems sowie unterschiedlicher miteinander kommunizierender IT-Systeme untereinander sicher. Einfache Switche nutzen hierbei zumeist eine für den Switch angepasste Firmware, während komplexe Switche mit umfassenden Managementfunktionen auch spezialisierte Be-

triebssysteme und zugehörige Software zur Erfüllung ihrer Funktionen nutzten. Herzstück von Switchen ist die netzwerktechnische Soft- und Hardware zur Verarbeitung und Übertragung der Datenkommunikation.

Switche unterscheiden sich in ihrer Kommunikation und Funktion von Routern, auch wenn insbesondere Endverbrauchergeräte die Funktionen beider Gerätetypen vereinen können. Router dienen der externen Kommunikation auf einem höheren Layer des ISO/OSI Referenzmodells, um ein Routing zu externen Kommunikationspartnern z. B. in bzw. über das Internet zu realisieren, während Switche zum Aufbau, Erhalt und Management eines lokalisierten Netzwerkes genutzt werden.

Anwendbare Schwachstellen

Switche sind die zentrale IT-Komponente für den Aufbau, Erhalt und Management eines IT-Netzwerks von IT-Systemen und IT-Systemverbünden. Sie sind daher umfassend notwendig für das Verarbeiten und Weiterleiten von netzwerktechnischer Kommunikation. Anwendbare Schwachstellen sind daher allgemein ebenso solche, welche die interne Firmware oder Software der Switche zur Verarbeitung der Kommunikation betreffen, also zum einen spezifische Kommunikationssoftware, zum anderen die allgemeine verwaltende Software der Switche. Beispielhaft ist z. B. der TCP/IP Stack IPnet, welcher in der Software VXWorks verwendet wird, welche wiederum Bestandteil des Betriebssystems HiOS ist, welches auf Switchen des Unternehmens Hirschmann verwendet wird. Für den TCP/IP Stack IPNet wurden im Jahr 2019 insgesamt 11 Schwachstellen bekannt.

Grundsätzlich lassen sich die allgemein anwendbaren Schwachstellen für Switche hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, so auch die Netzwerkkommunikation und die Spezialsoftware bzw. Betriebssysteme von Switchen Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche Schwachstellen basieren zumeist auf der Fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation.

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Die meisten Siwtche bieten zum Management zumeist Zugriffsmöglichkeiten über das angeschlossene Netzwerk an, welche mittels Authentifizierungen abgesichert werden. Kommt es zu Schwachstellen mit Möglichkeiten z. B. zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function oder die Improper Access Control, besteht die Möglichkeit, dass Angreifer nutzenden oder administrativen Zugriff auf die Switche erlangen.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Switche ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Da Switches die zentralen IT-Komponenten zum Aufbau und Erhalt von IT-Netzwerken sind, sind Switche grundsätzlich im Einsatz und mit allen kommunizierenden IT-Komponenten eines IT-Systems vernetzt. Je nach Einsatz- und Aufgabengebiet können diese Switche damit ein Inselnetzwerk erzeugen, in ein Anlagennetzwerk integriert sein oder über Router und ggf. Firewall mit dem Internet verbunden werden. Zur Ausnutzung netzwerktechnischer Schwachstellen von Switchen sind notwendigerweise Zugriffe auf das Netzwerk notwendig. Bei Inselnetzwerken ist hierzu ein initialer Zugriff auf mindestens eine IT-Komponente notwendig, bei weiter vernetzten Switches von IT-Systemen ein Zugriff über diese weitergehenden Vernetzungen.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Switche über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen, aber auch aus der Sonderstellung von Switchen als zentrale Netzwerkschaltstelle der entsprechenden Netzwerke

Dies ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Je nach Ausgestaltung, Funktionsumfang und Einsatzgebiet besitzen Switche umfassende Informationen zum Netzwerk. Einfachste Switche Nutzen eine Liste von MAC-Adressen, wohingegen komplexe Switche umfassende Protokollierung des Netzwerkverkehrs und seiner Teilnehmer ermöglichen. Bei Informationsabfluss durch Schwachstellen ist es Angreifern potenziell möglich, umfassende Informationen zum Netzwerk, dessen Aufbau, den Sicherungsmaßnahmen und bei nicht ausreichender Sicherung des Datenverkehrs auch den Inhalten des Datenverkehrs zu erreichen und damit die Vertraulichkeit des gesamten Netzwerks zu unterminieren.
- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Switche deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Switche dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk und Massenanfragen wie DDoS Angriffen. In der Konsequenz stehen die betroffenen Switche nicht zur Verfügung, wodurch die Kommunikation des gesamten Netzwerks eingeschränkt, verlangsamt oder vollständig unterbrochen wird.
- Authentifizierung: Die meisten Switche sehen Authentifizierungsmechanismen zum Schutz der Switche zur Absicherung der Administration der Switche vor. Zumeist muss sich hierzu mit einer weiteren IT-Komponente wie einem Clienten oder einem Servicegerät mit dem Switch verbunden werden. Schwachstellen in der Authentifizierung können dazu führen, dass diese Authentifizierungsmechanismen umgangen werden können, je nach Ausgestaltung der Schwachstelle auch aus dem offenen bzw. ungeschützten Netzwerbereichen. Die sich hieraus ergebenden Konsequenzen

sind für das betroffene Netzwerk und damit das oder die daran angebundenen IT-Systeme die Einschränkung der Vertraulichkeit, Verfügbarkeit und Integrität.

- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von Switchen ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Übernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit der Switche und damit aller daran angebundener IT-Komponenten und gesamten IT-Systeme stark beeinträchtigt.

Potenzielle Auswirkungen auf Gesamtsysteme

Switche sind die zentralen IT-Komponenten zur Bildung und Nutzung eines IT-Netzwerke aus verschiedenen miteinander kommunizierenden IT-Komponenten und für IT-Netzwerke bestehend aus mehreren IT-Systemen. Eine Kompromittierung dieser durch netzwerktechnische Angriffe basierend auf Schwachstellen der Kommunikation führt daher für die zugehörigen IT-Systeme mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen potenziell zu erheblichen Auswirkungen. Der Ausfall eines Switches führt zu einem Ausfall des gesamten IT-Netzwerkes, wenn keine redundanten Switche eingesetzt werden, welche nicht von den gleichen Schwachstellen betroffen sind. In der Konsequenz können die zugehörigen IT-Systeme je nach Ausgestaltung ihre Funktionen nur noch eingeschränkt oder gar nicht mehr ausführen. Sind die IT-Komponenten darauf ausgelegt, temporär eingeschränkt unabhängig vom Netzwerk zu arbeiten, sind die Ausfallkonsequenzen auf das Gesamtsystem reduziert. Eine vollständige Systemübernahme z. B. über eine Remote Code Execution Schwachstelle im Netzwerkverkehr eines Switches kann zu unkalkulierbaren Konsequenzen für die betroffenen IT-Systeme führen.

Da Switche grundsätzlich in Netzwerken eingesetzt werden, ist bei schwerwiegenden Konsequenzen aus netzwerktechnischen Schwachstellen der Switche grundsätzlich umfassende Konsequenzen für das Gesamtsystem zu erwarten. Der genaue Umfang der Konsequenzen ergibt sich schließlich aus dem Aufbau der Systeme und der geplanten Resilienz im Falle von IT-Sicherheitszwischenfällen.

5.6 Angriffsmöglichkeiten über die Netzwerkkommunikation von Feldgeräten

Feldgeräte sind die Basis von verfahrenstechnischen Anlagen und bilden die grundlegende Schnittstelle zwischen physikalischen Prozessen und digitalen Überwachungs- und Steuerungssystemen. Dabei werden von Feldgeräten sowohl Daten über den Zustand von Prozessen bzw. Anlagenteilen erfasst, physikalische Änderungen herbeigeführt und Steuerungshandlungen durchgeführt, beispielsweise über leittechnische Systeme im Rahmen einer Prozesssteuerung. Der Anwendungsbereich umfasst dabei diverse Industriebereiche und unterschiedlichste Einsatzgebiete. Auch im kerntechnischen Bereich zählen Feldgeräte zu den zentralen Komponenten von Sicherheits- und Sicherungssystemen, die entsprechend relevant für sicherheits-, sicherungs- und schutzrelevante Funktionen sind. Da durch die Manipulation von Feldgeräten weitreichende Störungen und ggf. auch physische Auswirkungen hervorgerufen werden können, sind sie ein kritisches Ziel für Angreifer insbesondere im industriellen Umfeld.

Die Kommunikation der Feldgeräte erfolgt dabei typischerweise im Zusammenhang mit speicherprogrammierbaren Steuerungen, oftmals in isolierten oder segmentierten Netzwerken. Dabei wurden in der Vergangenheit typischerweise proprietäre, herstellerspezifische Lösungen (zum Beispiel von Siemens, Omron oder Schneider Electric) in Bezug auf die Kommunikation von Feldgeräten eingesetzt, die typischerweise untereinander nur begrenzt oder gar nicht kompatibel waren. Es entwickelten sich mit zunehmender Verbreitung jedoch industrielle Standards, die heutzutage überwiegend eingesetzt werden und herstellerübergreifende Kommunikation ermöglichen. Je nach Feldgerät sind möglicherweise auch mehrere, unterschiedliche Kommunikationsformen realisiert. Da die Geräte tendenziell für sehr spezifische Anwendungsgebiete und die Erfüllung konkreter Aufgaben konzipiert sind, verfügen sie oftmals nicht über vollwertige Betriebssysteme, sondern stehen in Verbindung mit zugehörigen speicherprogrammierbaren Steuerungen. Allerdings gibt es in der heutigen Zeit auch komplexe Geräte, die eigene, für den Betrieb relevante Softwaresysteme besitzen.

Grundlagen der Kommunikation

Die Kommunikation im Zusammenhang mit Feldgeräten findet typischerweise grundsätzlich in der Kombination mit speicherprogrammierbaren Steuerungen statt. In der Regel handelt es sich um dauerhafte Kommunikationsverbindungen, die zur Überwachung oder Steuerung von (verfahrenstechnischen) Prozessen aufrechterhalten werden. Dabei

erfolgt die Einflussnahme auf diese Prozesse und ggf. die Herbeiführung physikalischer Änderungen über entsprechende Kommunikationsverbindungen und Befehle, die über übergeordnete administrative Netzwerke oder einfache Engineering Work Stations an mit den Feldgeräten verbundene speicherprogrammierbare Steuerungen übermittelt werden. Andererseits werden von Feldgeräten erhobene Prozessdaten und Messungen/Zustandswerte von den Feldgeräten an die zugehörigen SPS übermittelt und ggf. weiterverteilt oder abgerufen. Obwohl in der Vergangenheit oftmals proprietäre Protokolle mit eingeschränkter oder nicht vorhandener Kompatibilität zu anderen Herstellern eingesetzt wurden, findet die Kommunikation in der heutigen Zeit dagegen auch über weit verbreitete Standards oder Open-Source Protokolle statt, sodass eine Kommunikation von Geräten unterschiedlicher Hersteller prinzipiell möglich ist. Technisch werden dabei viele unterschiedliche Kommunikationsstandards wie beispielsweise auf TCP/IP basierende Standards wie Profinet, Modbus TCP oder Industrial Ethernet, aber auch BUS-Standards, proprietäre Standards und analoge Datenübertragung genutzt. Insbesondere für sicherheits- und sicherungsrelevante Systeme mit entsprechenden schutzrelevanten Funktionen sind sensible Kommunikationsnetze mit von Feldgeräten und SPS bewusst isoliert. In den meisten Fällen ist dabei mindestens die reguläre Informationstechnologie (z. B. Büro-IT) von der Verfahrenstechnologie getrennt (OT-Netzwerk, Operational Technologie).

Anwendbare Schwachstellen

Aufgrund der Kritikalität der Feldgeräte für prozesstechnische Abläufe und die potenziell verheerenden Auswirkungen von Cyberangriffen auf diese, die ggf. auch physische Auswirkungen haben können (insbesondere, wenn es sich um Feldgeräte mit Möglichkeiten zur Veränderung verfahrenstechnischer Prozesse handelt), sind Feldgeräte ein primäres Ziel von Angreifern. Auch wenn erweiterte Sicherungsmaßnahmen wie beispielsweise Air-Gaps zur Sicherung eingesetzt werden, ist es insbesondere durch die Ausnutzung von Schwachstellen für Angreifer in der Vergangenheit möglich gewesen, Angriffe auf diese Systeme auszuführen. Die hierbei in AP 2 beschriebenen und auf Feldgeräte allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Feldgeräte sind zur bestimmungsgemäßen Ausführung ihrer Funktionen auf ein angemessenes Management ihrer verfügbaren Ressourcen, insbesondere des Arbeitsspeichers angewiesen. Wenn durch Schwachstellen im Zusammenhang mit der Netzwerkkommunikation illegitime Zugriffe

auf den Arbeitsspeicher ermöglicht werden, kann es zu Einschränkungen in der Betriebsbereitschaft und im Betrieb der Feldgeräte kommen. Relevante Schwachstellen umfassen in diesem Zusammenhang beispielsweise Out-of-Bounce Read/Write oder Integer Overflow/Underflow sowie Uncontrolled Ressource Consumption/Loop with Unreachable Exit Condition. Zudem basieren die Schwachstellen oftmals auf einer fehlerhaften Handhabung von Eingangsparametern (Improper Input Validation, Improper Handling of Length, Parameter Inconsistency etc.).

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. mittels kryptografischer Verfahren relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Die Authentifizierung in Bezug auf Feldgeräte ist insbesondere im Zusammenhang mit den SPS ein kritischer Faktor, da zwischen diesen beiden Parteien die wesentliche Kommunikation stattfindet, beispielsweise bei Konfigurationen oder Parametrierungen, wenn die Aufgaben und vorgesehenen Prozesse des Geräts definiert werden. Die Ausnutzung von Schwachstellen in der Authentifizierung ermöglichen Angreifern ggf. die Übernahme der Kontrolle oder weitere maliziöse Handlungen. Typischerweise erfordert dabei die Manipulation von Feldgeräten eine bereits stattgefundene Kompromittierung der zugehörigen SPS.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Feldgeräte ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Bei Feldgeräten bestehen die Kommunikationsverbindung dauerhaft im Wesentlichen zu zugehörigen speicherprogrammierbaren Steuerungen. Somit setzt eine Manipulation von Feldgeräten typischerweise grundsätzlich eine bereits vorliegende Kompromittierung dieser SPS voraus. Somit ergeben sich im Wesentlichen analog die Bedingungen zur Ausnutzung vergleichbar mit den für SPS diskutierten Bedingungen: Die SPS sind insbesondere im industriellen Umfeld/als Teil von industriellen Steuerungs-

systemen typischerweise von kaufmännischen oder verwaltungstechnischen Netzwerken, die oftmals vielfältige Verbindungsmöglichkeiten zu externen Diensten bieten, isoliert. Angreifer müssen zur Ausnutzung von Schwachstellen somit Verbindungs- oder Zugriffsmöglichkeiten in diese typischerweise separierten Netzwerke haben, ggf. auch über AirGaps hinweg. Dabei unterscheiden sich die sich ergebenden Angriffsmöglichkeiten insbesondere im Aufbau des entsprechenden Netzwerks in Form einer dauerhaften Netzwerkverbindung nach außen und einem Netzwerk, welches auf dauerhafte Netzwerkverbindungen verzichtet. Ohne permanente Netzwerkverbindung nach außen ist für eine erfolgreiche Angriffsmöglichkeit eine Einwirkung innerhalb des Netzwerks notwendig, die Angreifern die Nutzung des Netzwerks für die Ausnutzung der Schwachstelle ermöglicht. Mit einer permanenten Verbindung nach außen ist Angreifern eine entsprechende Schwachstellenausnutzung möglich, wenn eventuelle Sicherungsmaßnahmen überwinden oder keine Sicherungsmaßnahmen bei der Kommunikation des Servers nach Außen getroffen werden.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Feldgeräte über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen. Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff erforderlich, in der Regel auch ein dadurch erlangter Zugriff auf zugehörige SPS; dieser ermöglicht in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung:

- Informationsabfluss: Wenn durch die Ausnutzung von Kommunikationsschwachstellen im Zusammenhang mit Feldgeräten und zugehörigen SPS von diesen Informationen abfließen, erhalten potenzielle Angreifer dadurch beispielsweise Zugriff auf Prozessdaten und Informationen von Feldgeräten. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der betroffenen Feldgeräte und SPS und damit der zugehörigen IT-Systeme. Ggf. können dadurch Informationen zur Unterbrechung oder Störung relevanter Prozesse erlangt werden, um auch physische Auswirkungen bei einem potenziellen Angriff herbeizuführen.

- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Feldgeräte mit der SPS die Verfügbarkeit einschränken. Dies ist diese Geräte oftmals ein

besonders kritisches Problem, weil diese in industriellen Umgebungen neben der Informationssammlung auch Steuerungsaufgaben übernehmen. Wenn die Verfügbarkeit eingeschränkt ist, können möglicherweise Prozesse gestört, abgebrochen oder anderweitig beeinflusst werden, sodass sich unter Umständen auch physische Auswirkungen ergeben.

- Authentifizierung: Zwischen Feldgeräten und SPS gibt es erst seit kurzer Zeit Authentifizierungen, die im Rahmen der Stärkung der Cybersicherheit in den letzten Jahren immer weiter in den Fokus rücken. Bei fehlender Authentifizierung können Angreifer problemlos bei einer kompromittierten SPS Manipulationen vornehmen. Wenn Authentifizierungsmechanismen vorhanden sind, dienen diese grundsätzlich zum Schutz vor unbefugten Zugriffen. Im Wesentlichen ermöglichen Schwachstellen im Zusammenhang mit der Authentifizierung bei der Kommunikation mit Feldgeräten und SPS Angreifern somit illegitime Befehle zu übermitteln, die dann ggf. von SPS weiter verarbeitet und verteilt und von den Feldgeräten ausgeführt werden und so den Angreifern entsprechende Einflussnahmen ermöglichen. Dies kann beispielsweise die Einstellung des Betriebs, die Änderung von Prozessen oder die Übermittlung anderweitiger Schadsoftware umfassen. Entsprechend kann die Vertraulichkeit, Verfügbarkeit und Integrität dadurch beeinträchtigt werden.

- Remote Code Execution: Durch Kommunikationsschwachstellen im Zusammenhang mit Remote Code Execution können Angreifer potenziell bei entsprechender Ausnutzung durch Übermittlung speziell gestalteter Nachrichten beliebigen Code auf Feldgeräten bzw. zugehörigen SPS ausführen und beispielsweise den Betrieb beeinträchtigen oder anderweitig manipulieren. Dabei können Angreifer unter bestimmten Umständen somit auch physischen Einfluss auf bestimmte Prozesse nehmen, sodass RCE-Schwachstellen im Zusammenhang mit Feldgeräten und SPS besonders kritisch einzustufen sind. Insbesondere neuere Feldgeräte besitzen komplexere Betriebssysteme und sind so für RCE-Schwachstellen anfällig. Bei älteren Geräten, die oftmals einen beschränkten Funktionsumfang aufweisen, ist die RCE lediglich im Zusammenhang mit der Kompromittierung zugehöriger SPS relevant.

Potenzielle Auswirkungen auf Gesamtsysteme

Feldgeräte sind kritische Komponenten in prozesstechnischen und industriellen Umgebungen und dienen einerseits durch die Erfassung und Annahme von Daten als Informationsquellen und andererseits durch die Möglichkeit der direkten Einflussnahme, unter anderem auch auf physische Prozesse, als kritische Werkzeuge zur Beeinflussung

und Steuerung von Systemen und Prozessen. Dies beinhaltet explizit auch betriebliche, sicherheitstechnische und sicherungstechnische Prozesse, wodurch sie entsprechend hochrangige Ziele für potenzielle Angreifer darstellen. Da die Kommunikation von Feldgeräten in der Regel mit SPS stattfindet, sind diese oftmals das Bindeglied zwischen der Feldebene einerseits und der Übermittlung von Befehlen oder dem Abruf von Informationen über übergeordnete Netzwerke andererseits. Eine Kompromittierung der Feldgeräte oder zugehöriger SPS ermöglichen Angreifern potenziell physische Auswirkungen auf Prozesse oder Systeme und Komponenten provozieren können und Abläufe und Prozesse stören oder stoppen können. Zudem können Angreifer ggf. wertvolle Informationen erlagen, um weitere Angriffsschritte vorzubereiten und durchzuführen. Die Konsequenzen für Vertraulichkeit, Verfügbarkeit und Integrität bei Angriffen über Kommunikationsverbindungen unter Ausnutzung von Schwachstellen sind somit schwerwiegend. Auch isolierte Systeme können betroffen sein, wenn Angreifer Air-Gaps überwinden.

Die tatsächlichen Konsequenzen sind abhängig vom Gesamtaufbau des betroffenen industriellen Steuerungssystems bzw. dem angeschlossenen Netzwerk. Feldgeräte und zugehörige SPS wurden in der Vergangenheit häufig nicht nach dem Security-by-Desgin Prinzip entwickelt und weisen somit potenziell kritische Schwachstellen auf, die entsprechend ausgenutzt werden können. Die tatsächlichen potenziellen Auswirkungen hängen somit auch zu einem großen Teil von den übergeordneten Sicherungsmaßnahmen des Systems und der Anlage ab. Diese umfassen unter anderem eine entsprechende Segmentierung des Netzwerks, Härtung, den Einsatz virtueller Umgebungen und von Firewalls. Wenn sich Schwachstellen in diesen Bereichen umgeben, die Angreifer für ihre Zwecke missbrauchen, ergeben sich oftmals schwerwiegende Auswirkungen. Wenn zur Überwachung bzw. Steuerung von industriellen Prozessen eingesetzte Feldgeräte und SPS ausfallen, kann es zum vollständigen Ausfall betroffener Systeme und Prozesse kommen, die weitreichende Auswirkungen auf das Gesamtsystem haben können.

5.7 Angriffsmöglichkeiten über die Netzwerkkommunikation von Clients

Als Client wird eine IT-Komponente in einem komplexen IT-System beschrieben, welche von Endanwendern zur IT-Systemnutzung und Steuerung verwendet wird und in das Netzwerk des IT-Systems eingebunden ist. Eine Vielzahl von IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung typischer kerntechnischer Anlagen und Einrichtungen sind auf menschliche Steuerung und Kontrolle angewiesen

oder dienen der Darstellung und Bereitstellung von Informationen für Bedienende, sodass für beide Fälle Clients in die Netzwerke der entsprechenden IT-Systeme integriert werden. Dabei ist die Nutzung von Clients abzugrenzen von administrativen Tätigkeiten, welche typischerweise auf separaten IT-Komponenten wie Servicegeräten erfolgen. Typischerweise werden auf Clients entweder handelsübliche Betriebssysteme mit entsprechender spezifischer Software zur Nutzung und Steuerung der IT-Systeme angewendet oder aber proprietäre Betriebssysteme zugehörig zum IT-System.

Als Hardware werden typischerweise verbreitete Standardkomponenten installiert. Die Netzwerkhardware wird hierbei zumeist über umfassend verbreitete und angebotene Standardsoftware und Hardware realisiert wie kommerzielle oder freie TCP/IP Stacks.

Grundlagen der Kommunikation

Für die Durchführung ihrer Aufgaben und Funktionen sind Clients auf eine temporäre oder dauerhafte Kommunikation mit weiteren IT-Komponenten der zugehörigen IT-Systeme angewiesen. Für Clients, welche zur Nutzung und Steuerung von IT-Systemen durch IT-Anwender dienen, ist eine bidirektionale digitale Kommunikation mit den übrigen IT-Komponenten des IT-Systems notwendig. Diese wird typischerweise als Kommunikationsweg zwischen eingesetzten Servern und Clients realisiert, kann jedoch auch direkt zwischen Feldgeräten und den Clients erfolgen. Clients, die als reines Anzeigensystem genutzt werden, können als monodirektionale Kommunikation ausschließlich als Empfänger von Informationen aufgebaut werden. Die datentechnische Kommunikation wird im überwiegenden Einsatzfall über TCP/IP basierte Kommunikation realisiert, im Spezialanwendungsfall mittels proprietärer oder branchenspezifischer Protokolle.

Anwendbare Schwachstellen

Clients können je nach Anwendungsfall mono- oder bidirektional kommunizieren. In beiden Fällen sind Clients grundsätzlich aufgrund der der typischen Anwendung von Standardsoft- und Hardware potenziell von sehr vielen unterschiedlichen Schwachstellentypen betroffen.

Die hierbei in AP 2 beschriebenen und auf Clients allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, dazu gehören auch die Netzwerkkommunikation, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche Schwachstellen basieren zumeist auf der Fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation.

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Hierzu zählen die Möglichkeiten zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function und die Improper Access Control.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Clients ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Clients werden hauptsächlich mittels TCP/IP basierenden Verbindungen innerhalb von IT-Systemen und IT-Netzwerken eingesetzt. Je nach Ausgestaltung des Netzwerkes, der Einschränkung des Funktionsumfanges der eingesetzten Clients und der Nutzungsziele der Clients sind diese mehr oder weniger vernetzt. Bei starker Einschränkung der Kommunikation in einem gemanagten Netzwerk besteht für Clients ausschließlich die Kommunikationsmöglichkeit mit für den Clients relevanten IT-Komponenten wie z. B. einem Server. In einem solchen Fall müssen Angreifer zur Ausnutzung kommunikationstechnischer Schwachstellen also bereits Zugang zur Kommunikation des relevanten

Netzwerkabschnittes besitzen. Clients mit einer breiteren Aufgabenstruktur haben zumeist eine erheblich weitergehende Liste an Kommunikationspartner im Netzwerk oder können zur Arbeits- und Aufgabenerfüllung der Nutzer des Clients auf das Internet vollständig oder begrenzt zugreifen. In solchen Fällen ist für die Angreifer ein unspezifischer Netzwerkzugriff ausreichend oder gar ausschließlich die Ausnutzung der des Clients durchgeführten Kommunikation mit dem Internet und entsprechender Angriffstechniken.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Clients über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen, aber auch aus dem Aufgabengebiet des Clients.

Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff notwendig, dieser ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Clients mit rein anzeigenden Funktionen in einer monodirektionalen Kommunikation können nicht von Informationsabfluss betroffen sein. Bei Clients zur Steuerung und Nutzung kann Informationsabfluss durch Schwachstellen in der Verarbeitung der Kommunikation dazu führen, dass Angreifer beliebige und spezifische Informationen des Clients auslesen. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der Clients und damit der zugehörigen IT-Systeme.
- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Clients deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Clients dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk. In der Konsequenz stehen Clients für ihre Nutzung nicht mehr zur Verfügung. Ist ausschließlich der Client betroffen, können die Kernfunktionen, sofern diese nicht von Eingaben oder Aufgaben der Benutzer abhängen, vom eigentlichen IT-System weiter ausgeführt werden.

- Authentifizierung: Die meisten Clients sehen Authentifizierungsmechanismen zum Schutz der Clients vor unbefugten Zugriffen vor. Solche Maßnahmen werden für das Betriebssystem und möglicherweise für Zugriffe auf einzelne Programme und Nutzungsschritte verwendet. Schwachstellen in Authentifizierungsverhalten in der Kommunikation entstehen z. B. durch bestimmte Schwachstellen in der Belegung von Arbeitsspeicher, bei welchen spezifische Nachrichten eine Umgehung bestimmter Authentifizierungsmechanismen für einzelne Programme oder das Betriebssystem des Clienten ermöglichen. Die sich hieraus ergebenden Konsequenzen sind abhängig von den Einsatzaufgaben des Clientens für das betroffene IT-System, grundsätzlich können die Vertraulichkeit, Verfügbarkeit und Integrität des Clienten eingeschränkt werden.
- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von Servern ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Übernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit des Clients erheblich beeinflusst.

Potenzielle Auswirkungen auf Gesamtsysteme

Clients dienen der Steuerung und Nutzung von IT-Systemen wie auch zur Anzeige von IT-Systeminformationen für die Bediener und Nutzer. Clients werden in einer Vielzahl von IT-System mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen eingesetzt, welche dauerhaften oder temporären Input für ihre Funktionen benötigen oder welche als informationsgebende IT-Systeme diese Informationen an Nutzer und Bediener weitergeben sollen. Werden diese in ihrer Vertraulichkeit, Verfügbarkeit und Integrität eingeschränkt, wird insbesondere die Möglichkeit der Bediener und Nutzer auf das IT-System einzuwirken bzw. dessen Informationen zu erhalten stark eingeschränkt, unterbunden oder es erfolgen Fehlbedienungen und die Darstellung von Fehlinformationen. Ausfälle von Clients solcher Systeme, die zwar Clients zur Informationsdarstellung oder gelegentlichen Nutzung und Eingabe von Daten nutzen, jedoch

nicht elementar für die Funktionsweise von IT-Systemen sind, führen zu geringeren Auswirkungen auf das Gesamtsystem als bei Systemen, bei denen Clients dauerhaft für zentrale Aufgaben des IT-Systems verwendet werden.

Die tatsächlichen Konsequenzen sind jedoch auch abhängig vom Gesamtaufbau des betroffenen IT-Systems bzw. angeschlossenem Netzwerk. Sicherungsmaßnahmen und der Einsatz getrennter Netzwerke über VLANs und Firewalls ermöglichen einen Schutz der eingesetzten Netzwerke. Diese Schutzmaßnahmen sind jedoch insbesondere abhängig von der Art der vorliegenden Schwachstelle innerhalb der Kommunikation und den sich ergebenden Angriffsmöglichkeiten.

5.8 Angriffsmöglichkeiten über die Netzwerkkommunikation von Servicegeräten

Als Servicegeräte wird eine Gruppe von IT-Komponenten in komplexen IT-Systemen beschrieben, welche zur Administration und partiell zur Konfiguration und Parametrisierung von komplexen IT-Systemen verwendet werden. Hierzu zählen z. B. temporär angebundene Laptops mit Spezialsoftware zur Administration und Programmierung, permanent in das IT-System eingebundener IT-Komponenten wie Engineering Work Stations und Mischformen, wie Clients, welche als virtuelle Maschinen sowohl typische Clientarbeiten von Systemnutzern als auch administrative Tätigkeiten von Administratoren ermöglichen. Eine Vielzahl von IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung typischer kerntechnischer Anlagen und Einrichtungen sind auf Servicegeräte für administrative, konfigurierende und parametrisierende Tätigkeiten angewiesen. Servicegeräte spielen damit eine besondere Rolle als zentrale Komponenten mit zumeist tiefgreifenden Zugriffen auf andere Komponenten eines komplexen IT-Systems.

Servicegeräte sind zumeist Standardgeräte wie Laptops oder Desktoprechner, welche handelsübliche Betriebssysteme und Software, zum Teil jedoch auch proprietäre Betriebssysteme und Software einsetzen. In das Netzwerk werden Servicegeräte je nach Realisierung und Aufgabenprofil temporär oder dauerhaft, zumeist über TCP/IP angebunden.

Grundlagen der Kommunikation

Für die Durchführung ihrer Aufgaben und Funktionen sind Servicegeräte auf eine temporäre oder dauerhafte Kommunikation mit den zu administrierenden, parametrisierenden oder konfigurierenden IT-Komponenten der zugehörigen IT-Systeme angewiesen. Je nach Einsatz- und Aufgabenprofil kann eine solche datentechnische Anbindung temporär oder permanent realisiert werden. Bei der Administration von einzelnen IT-Komponenten kann eine direkte temporäre Anbindung via USB ausreichend sein, für viele Aufgaben wie z. B. die Administration multipler Komponenten ist eine temporäre oder dauerhafte Anbindung in das Netzwerk des IT-Systems und damit per TCP/IP an den Router oder bei leittechnischen Komponenten mit dem Controller notwendig.

Insbesondere Servicegeräte für die Administration von IT-Komponenten sind dazu auf eine Möglichkeit zum Empfang von Softwareupdates angewiesen, um notwendige Updates im Rahmen der Administration auf den entsprechenden Komponenten zu installieren. Hierzu müssen die Updates entweder separat über mobile Datenträger auf das Servicegerät übertragen werden, oder aber über eine temporäre oder dauerhafte Quelle aus dem Netzwerk bis hin zum Internet bezogen werden.

Anwendbare Schwachstellen

Servicegeräte müssen für ihre Aufgaben mit mindestens einer weiteren IT-Komponente kommunizieren. Servicegeräte sind daher im Rahmen ihrer typischen Anwendung von sehr vielen unterschiedlichen netzwerktechnischen Schwachstellentypen potenziell betroffen.

Die hierbei in AP 2 beschriebenen und auf Servicegeräte allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, dazu gehören auch die Netzwerkkommunikation, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche

Schwachstellen basieren zumeist auf der Fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation.

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Hierzu zählen die Möglichkeiten zum Authentication Bypass by Spoofing oder Capture-replay, die Missing Authentication for Critical Function und die Improper Access Control.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Servicegeräte ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Solche Servicegeräte, die nicht nur temporär mit einzelnen IT-Komponenten verbunden werden, sind daher zumindest im geringeren Maße von potenziellen netzwerktechnischen Schwachstellen betroffen. Angreifer müssen in einem solchen Fall zum Zeitpunkt der Verbindung des Servicegeräts einen zumindest eingeschränkten Zugriff auf die temporäre netzwerktechnische Verbindung des Servicegeräts z. B. über die zu administrierende IT-Komponente erlangt haben.

Werden Servicegeräte direkt mit dem Netzwerk verbunden, um z. B. eine größere Zahl von IT-Komponenten zu administrieren oder eine dauerhafte Verbindung in und aus dem Netzwerk heraus zu etablieren, sind in solchen Fällen für die Angreifer ein unspezifischer Netzwerkzugriff ausreichend oder bei umfassenden Netzwerken mit Außenverbindungen der Servicegeräte gar reine Zugriffe von außen möglich.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Servicegeräte über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen, aber auch aus dem Einsatzgebiet des Servicegeräts.

Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff notwendig, dieser ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Servicegeräte speichern und verarbeiten Informationen, welche Relevant für die Administration, Konfiguration und Parametrisierung der übrigen IT-Komponenten eines komplexen IT-Systems sind. Schwachstellen in der Kommunikation, die zu Informationsabfluss führen, können dazu führen, dass Angreifer auf Teile oder beliebige Informationen des Servicegeräts oder zumindest des vom Servicegerät ausgetauschten Informationsgehalts erlangen können. Dazu gehören potenziell tiefgreifende Systeminformationen. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen des Servicegeräts und damit des zugehörigen IT-Systems.
- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Servicegeräte deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Servicegeräte dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk. In der Konsequenz stehen die Servicegeräte nicht mehr zur Verfügung. Da Servicegeräte, ob nun temporär verbunden oder dauerhaft in ein Netzwerk integriert, jedoch zumeist keinen dauerhaften Einsatz benötigen, sondern für wiederkehrende administrative Aufgaben genutzt werden, ist davon auszugehen, dass die weiteren IT-Komponenten und damit das betroffenen IT-System weitestgehend unabhängig von der Einschränkung der Verfügbarkeit der Servicegeräte im Rahmen von Denial of Service genutzt werden kann.

- Authentifizierung: Servicegeräte werden insbesondere für administrative Tätigkeiten eingesetzt und unterliegen daher zumeist besonderen Authentifizierungsmechanismen. Werden solche Maßnahmen durch Schwachstellen in der Kommunikation der Servicegeräte Unterlaufen, können sich hierdurch umfassende Angriffsmöglichkeiten in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität des Servicegeräts und damit des zugehörigen IT-Systems ergeben.
- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von Servicegeräten ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Übernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit des Servicegeräten und damit der zugehörigen IT-Systemen erheblich beeinflusst.

Potenzielle Auswirkungen auf Gesamtsysteme

Servicegeräte sind zentrale IT-Komponenten, welche für die Administration, Konfiguration und Parametrisierung einer Vielzahl von IT-Komponenten, welche typischerweise in komplexen IT-Systemen mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung kerntechnischer Anlagen und Einrichtungen benötigt werden. Sie können sowohl als temporär anzuschließende Komponenten in Form von Laptops wie auch als permanent angeschlossene Engineering Work Stations oder Admin-PCs eingesetzt werden. Aufgrund ihrer Aufgaben und damit einhergehenden Bedeutung können netzwerktechnischer Schwachstellen insbesondere bei umfassender Vernetzung der genutzten Servicegeräte im IT-Netzwerk der IT-Systeme zu erhebliche Auswirkungen auf die Gesamtsysteme im Angriffsfall führen. Insbesondere die Einschränkung der Vertraulichkeit, z. B. durch Umgehung der Authentifizierung oder die Möglichkeit zur Remote Code Execution kann zu schwerwiegenden Folgen für die IT-Systeme mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung kerntechnischer Anlagen führen.

Die tatsächlichen Konsequenzen sind jedoch auch abhängig vom Gesamtaufbau des betroffenen IT-Systems bzw. angeschlossenem Netzwerk sowie den getroffenen Sicherungsmaßnahmen.

5.9 Angriffsmöglichkeiten über die Netzwerkkommunikation von Firewalls

Firewalls sind eigenständige IT-Systeme oder IT-Komponenten komplexer IT-Systeme, welche zur Abgrenzung, Absicherung und Logging von Netzwerkverkehr innerhalb von Netzwerken und von Netzwerken zur Außenwelt dienen. Firewalls werden weltweit zur Absicherung von Netzwerkverkehr verwendet, so auch zum Schutz von Netzwerken mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung typischer kerntechnischer Anlagen und Einrichtungen. In ihrer einfachsten Form sind Firewalls eine Software, welche eingehende und ausgehende Netzwerkzugriffe blockiert oder durchlässt in Abhängigkeit der Einstellungen der Firewall. In komplexen Netzwerken werden zumeist Firewalls auf ihrer eigenen Hardwareplattform oder auf einer gemeinsamen Hardwareplattform von genutzten Routern oder Switchen betrieben, welche das betroffene Netzwerk vor unerwünschten und unerlaubtem Netzwerkverkehr innerhalb und nach außen schützen sollen. Hierzu werden von der ausgeführten Firewallsoftware nicht nur der Netzwerkverkehr entsprechend der Vorgaben der Firewall blockiert, sondern zumeist auch auf verdächtiges Verhalten analysiert und Ereignisse mittels Logging dokumentiert.

Firewalls auf eigenen Hardwareplattformen werden von verschiedenen großen IT-Unternehmen angeboten, wobei zumeist angepasste Betriebssysteme oder Firmware, eigene entwickelte oder zugekaufte und modifizierte Software und spezifische für die Aufgaben ausgewählter Hardware mit ausreichend Leistung gewählt werden.

Grundlagen der Kommunikation

Firewalls auf Hardwareplattformen, auch Externe, Netzwerk- oder Hardwarefirewall genannt, dienen ausschließlich der Sicherung der Kommunikation von IT-Netzwerken, zum einen zu externen Kommunikationspartnern außerhalb des Netzwerks, bei höheren Sicherheitsanforderungen aber auch innerhalb des Netzwerkes. Aufgrund ihrer Aufgaben und Rolle kommunizieren Firewalls daher zweiseitig, auf der einen Seite zum zu schützenden Netzwerk hin, auf der anderen Seite zur Außenwelt. Werden Firewalls auch zu Schutz der Netzwerkkommunikation innerhalb des zu schützenden Netzwerkes eingesetzt, kommunizieren auch innerhalb des Netzwerks IT-Komponenten zuerst mit der Firewall und dann mit weiteren Komponenten des Netzwerks. Aufgrund ihrer Aufgabe als schützende IT-Komponenten in Netzwerken kommunizieren Firewalls daher grundsätzlich mit anderen IT-Komponenten innerhalb und außerhalb des Netzwerks und wir-

ken als Sicherheitssystem der Kommunikation. Firewalls bieten daher je nach Ausgestaltung und notwendiger Technik potente Kommunikationsmodule mit zahlreichen Anschlussmöglichkeiten für TCP/IP Kommunikation.

Anwendbare Schwachstellen

Firewalls sind als Sicherheitssysteme der Kommunikation temporär oder dauerhaft einer am Kommunizieren, zum einen innerhalb des zu schützenden IT-Netzwerks und zum anderen nach außen hin zur außerhalb des zu schützenden IT-Netzwerks liegenden IT-Infrastruktur, z. B. einen größeren Anlagennetzwerk oder dem Internet. Schwachstellen, welche die Kommunikation betreffen, können daher zu schwerwiegenden Folgen nicht nur für die Firewall an sich, sondern auch die zu schützende Netzwerke dahinter betreffen. Neben klassischen netzwerktechnischen Schwachstellen im Handling und Verarbeitung des Netzwerkverkehrs können bei Firewalls auch Schwachstellen in der Firewallsoftware auftreten, welche den Netzwerkverkehr analysiert und entsprechend blockiert, weiterleitet oder als Meldung weitergibt. Solche Schwachstellen in Firewalls sind in den letzten Jahren mehrfach aufgetreten:

- Zyxel Firewalls waren von mehreren Schwachstellen im Umgang mit Anfragen und der Authentifizierung betroffen, welche Remote Code Execution und Denial of Service ermöglichten, z. B. bei der Bearbeitung von https Anfragen an die Firewalls.
- Cisco Firewalls waren von einer double free Schwachstelle betroffen, welche Angreifern die Ausführung beliebigen Codes ermöglichte.
- Sophos Firewalls waren von einer Schwachstelle einer Subsoftwarekomponente der Software Exim betroffen, welche den Emailschutz der Firewall in einer Weise betraf, dass Angreifer beliebige Befehle auf der Firewall ausführen konnten.

Grundsätzlich lassen sich die allgemein anwendbaren Schwachstellen hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, so auch die Netzwerkkommunikation und die Firewallsoftware, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Regulär wird hierfür ein Teilbereich des Arbeitsspeichers für diese Aufgaben vorgesehen. Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers sind z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-

Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche Schwachstellen basieren zumeist auf der Fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation.

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Netzwerkrelevante Schwachstellen können dazu führen, dass die von IT-Systemen bzw. IT-Komponenten vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Firewalls bieten zum Management zumeist Zugriffsmöglichkeiten über das angeschlossene Netzwerk an, welche mittels Authentifizierungen abgesichert werden. Kommt es zu Schwachstellen mit Möglichkeiten z. B. zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function oder die Improper Access Control, besteht die Möglichkeit, dass Angreifer nutzenden oder administrativen Zugriff auf die Firewalls erlangen.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf Firewalls ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Da Firewalls für die Sicherung des Netzwerkverkehrs eingesetzt werden, sind diese dauerhaft mit IT-Komponenten des zu sichernden IT-Netzwerkes ebenso wie mit einer Außenwelt, z. B. einem Anlagennetzwerk oder dem Internet, verbunden. Schwachstellen in der Netzwerkkommunikation von Firewalls benötigen eine Form von Netzwerkkontakt mit den Firewalls, bei mit dem Internet kommunizierenden Firewalls besteht diese defacto dauerhaft. Bei rein in internen Netzwerken eingesetzten Firewalls, z. B. zwischen einem besonders betrieblich, sicherheits- oder sicherungsrelevanten IT-Netzwerk einer kerntechnischen Anlage und einem Anlagennetzwerk ist der Zugriff zumindest zu einem der von der Firewall trennend wirkenden Netzwerke notwendig.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf Firewalls über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen, aber auch aus der Sonderstellung von Firewalls als Schutzbarriere zwischen zu sicherndem Netzwerk und äußeren Netzwerken wie dem Internet.

Dies ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: Werden Firewalls eingesetzt, überwachen diese umfassend ein- und ausgehenden Netzwerkverkehr, in manchen Anwendungsfällen ebenso den gesamten Netzwerkverkehr, dazu ermöglichen sie die umfassende Dokumentation des Netzwerkverkehrs. Bei Informationsabfluss durch Schwachstellen ist es Angreifern möglich, umfassende Informationen zum Netzwerk, dessen Aufbau, den Sicherungsmaßnahmen und ggf. auch den Inhalt des Netzwerkverkehrs zu erreichen und damit die Vertraulichkeit des gesamten Netzwerks zu unterminieren.

- Denial of Service: Bei Denial of Service Angriffsmöglichkeiten können Angreifer bei Ausnutzung von entsprechenden Schwachstellen in der Kommunikation der Firewalls deren Verfügbarkeit einschränken. Hierbei nutzen die Angreifer Schwachstellen in der Netzwerkkommunikation in einer Weise, die die Firewalls dazu bringt, ihre eigentlichen Funktionen nicht mehr oder nicht mehr in vorgesehener Weise auszuführen, z. B. durch die unbegrenzte Verarbeitung wiederkehrender TCP/IP Anfragen aus dem Netzwerk und Massenanfragen wie DDoS Angriffen. In der Konsequenz steht die betroffene Firewall nicht zur Verfügung, wodurch die Kommunikation zwischen den von der Firewall getrennten Netzwerkbereichen nicht aufrechterhalten wird.

- Authentifizierung: Die meisten Firewallsysteme sehen Authentifizierungsmechanismen zum Schutz der Firewalls vor unbefugten Zugriffen und zur Absicherung der Firewalladministration vor. Zumeist muss sich hierzu mit einer weiteren IT-Komponente wie einem Clienten oder einem Servicegerät mit der Firewall verbunden werden, z. B. über das gesicherte Netzwerk. Schwachstellen in der Authentifizierung können dazu führen, dass diese Authentifizierungsmechanismen umgangen werden

können, je nach Ausgestaltung der Schwachstelle auch aus dem offenen bzw. ungeschützten Netzwerbereichen. Die sich hieraus ergebenden Konsequenzen sind für das betroffene zu schützende Netzwerk und damit das oder die daran angebundenen IT-Systeme die Einschränkung der Vertraulichkeit, Verfügbarkeit und Integrität.

- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht, z. B. durch die Einschleusung von fremdem Code in den Arbeitsspeicher durch eine fehlerhafte Arbeitsspeicherbearbeitung und anschließende Ausführung durch laufende Programme. Werden entsprechende Schwachstellen in der Netzwerkkommunikation von Firewalls ausgenutzt, besteht die Angriffsmöglichkeit zur vollständigen Übernahme und die Ausführung beliebigen Codes. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit der Firewall und damit aller daran angebundener IT-Komponenten und gesamten IT-Systeme stark beeinträchtigt.

Potenzielle Auswirkungen auf Gesamtsysteme

Firewalls dienen dem Schutz von IT-Netzwerken von IT-Systemen und IT-Verbünden vor unerlaubten und schadhaften Netzwerkverkehr von Innen und Außen. Firewalls werden daher als Sicherungsmaßnahmen für IT-Systeme mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen eingesetzt, welche auf die Kommunikation mit anderen IT-Systemen, dem Anlagennetzwerk oder der Außenwelt angewiesen sind. Damit spielen sie eine bedeutende Rolle in der Sicherheitsarchitektur von IT-Netzwerken von IT-Systemen, sodass Schwachstellen die daraus resultierenden Angriffsmöglichkeiten auf Firewalls massive Auswirkungen auf die Gesamtsysteme haben können. Angriffe auf Firewalls basierend auf Schwachstellen der Firewalls bzw. deren Netzwerkkommunikation wurde bereits im nicht nuklearen Kontext erkannt, z. B. im Fall von Zyxel Firewalls im dänischen Energiesektor. Während ein reiner Ausfall einer Firewall noch zu limitierten Konsequenzen für die Kommunikation der betroffenen IT-Systemen führen kann, können ein Verlust der Vertraulichkeit und der Integrität von Firewalls zu erheblichen Folgekonsequenzen für auf Firewalls angewiesene IT-Systeme mit betrieblicher, sicherheits- oder sicherungstechnischer Relevanz in kerntechnischen Anlagen führen.

Da Firewalls grundsätzlich in Netzwerken eingesetzt werden, ist bei schwerwiegenden Konsequenzen aus netzwerktechnischen Schwachstellen der Firewalls grundsätzlich

umfassende Konsequenzen für das Gesamtsystem zu erwarten. Der genaue Umfang der Konsequenzen ergibt sich schließlich aus dem Aufbau der Systeme und der geplanten Resilienz im Falle von IT-Sicherheitszwischenfällen.

5.10 Angriffsmöglichkeiten über die Netzwerkkommunikation von KVM Switches

KVM (Keyboard, Video, Mouse) Switche sind analoge oder digitale IT-Komponenten zur Kurz- oder Langstreckenübertragung und Verteilung von Eingabesignalen über Peripherie wie Tastaturen und Mäuse sowie zur Ausgabe von Videosignalen für Bildschirme von angeschlossenen IT-Systemen. Bei ihrer Einführung ausschließlich basierend auf analogen Standards wie VGA und PS/2, werden heute digitale KVM-Switches insbesondere mit USB und HDMI/Displayport eingesetzt. Digitale KVM-Switches können ihr Signal mittels USB-C als über wenige Meter übertragen, jedoch als KVM over IP mittels TCP/IP ihre Daten über weite Strecken innerhalb von Netzwerken oder über das Internet übertragen. KVM über TCP/IP dient insbesondere zur Vermeidung der Nutzung von Remotezugriffen bei der Steuerung, Bedienung und Administration von eingesetzten IT-Systemen über ortsfremde Arbeitsplätze und abseits der Betriebssystembasis.

KVM-Switches mit IP-Unterstützung werden von verschiedenen Herstellern weltweit angeboten, wobei zugelieferte und proprietäre Netzwerktechnik eingesetzt wird.

Grundlagen der Kommunikation

Ursprünglich insbesondere als analoge Komponenten eingesetzt, wurden mit der Zeit zur Funktionserweiterung und aufgrund der Verdrängung analoger Schnittstellen wie PS/2 durch USB mehr und mehr digitale KVM-Switches auf den Markt gebracht. Mit KVM over IP wurde der Funktionsumfang von KVM-Switches auf die Netzwerkkommunikation erweitert, sodass KVM-Switches über Netzwerktechnik innerhalb von Netzwerken Anschlüsse an eine Vielzahl von IT-Systemen bzw. IT-Komponenten ermöglichen können, aber auch über das Internet an weit entfernte Standorte und Einrichtungen. Hierzu werden etablierte Standards wie IPMI (Intelligent Platform Management Interface) oder Redfish genutzt. Während IMPI als veraltetet angesehen wird und extern abgesichert werden muss, erzwingt Redfish TLS-Verschlüsselung.

KVM-Switches können aufgrund der unterschiedlichen Aufgabenfelder in sehr unterschiedlichen Netzwerken eingesetzt werden. In ihrer Aufgabe als Umschalter von Peripherie und Anzeigen für einzelne Systeme können und werden KVM-Switche komplett ohne Netzwerkfunktionen eingesetzt, beim Einsatz innerhalb einer Organisationseinheit oder einem großen IT-System können KVM-Switches als Einzelverbindung über TCP/IP, in abgetrennten VLANs oder allgemeinen im Netzwerk eingesetzt werden, um die Bedienung von IT-Komponenten wie Servern durch zentralisierte Arbeitsplätze zu ermöglichen.

Anwendbare Schwachstellen

Die Art der netzwerktechnischen Schwachstellen von KVM-Switches hängt insbesondere von der Ausgestaltung der KVM-Switche ab. Analoge KVM-Switches besitzen keine Schwachstellen im programmiertechnischen Sinn. Digitale KVM-Switches ohne Netzwerkunterstützung können zwar von Schwachstellen der Firmware betroffen sein, jedoch nicht von spezifisch netzwerkrelevanten Schwachstellen.

KVM-Switches, welche TCP/IP bzw. allgemeine Netzwerkfunktionen unterstützten können von Schwachstellen in ihrer Firmware betroffen sein. Diese Schwachstellen können zum einen die eingesetzte Firmware für die direkte Netzwerkfunktionen betreffen, aber weitere Funktionen der Firmware für das Management z. B. einer großen Anzahl angebundener Systeme oder spezialisierter Standards wie die zumeist genutzte Redfish API.

Die hierbei in AP 2 beschriebenen und auf TCP/IP nutzende KVM-Switche allgemein anwendbaren Schwachstellen lassen sich hierbei in drei Gruppen aufteilen:

Schwachstellen bei der Nutzung von Arbeitsspeicher: Grundsätzlich benötigen die allermeisten Programme und Funktionen, dazu gehören auch die Netzwerkkommunikation, Arbeitsspeicherbereiche zur Erfüllung ihrer Aufgaben. Insbesondere KVM-Switche mit zusätzlichen Funktionen wie Benutzermanagement, Massenspeicheranschlussmöglichkeiten und hoher Leistung und Bandbreite nutzen daher eine Architektur, die eine Form von Arbeitsspeicher notwendig machen kann. Die relevante eingesetzten Firmware für die Netzwerkkommunikation kann entsprechend Schwachstellen der fehlerhaften Handhabung des Arbeitsspeichers aufweisen, wie z. B. solche Schwachstellen, welche ein unautorisiertes Auslesen von anderen Arbeitsspeicherbereichen (Out-of-Bounce Read/Write) ermöglichen, die nicht für die eigentliche Funktion vorgesehen ist. Solche

Schwachstellen basieren zumeist auf der Fehlerhaften Handhabung von Parametern (Improper Handling, Improper Input Validation.

Fehlerhafte Begrenzungen und Zufälligkeit: In der Netzwerkkommunikation sind Systeme auf einzelne Rechenoperationen bzw. Codefunktionen angewiesen, die die Kommunikation ermöglichen und absichern. Hierzu zählt einerseits der Grad der Zufälligkeit (Insufficient Entropy, Use of Insufficiently Random Values), der für die Absicherung von Kommunikation z. B. über Verschlüsselungsfunktionen relevant ist, zum anderen die Sicherstellung, dass sich wiederholende Anfragen und Operationen nicht dauerhaft wiederholen und damit zur Systemüberlastung führen.

Schwachstellen der Authentifizierung: Spezifische Authentifizerungsmechanismen werden von einigen KVM-Switches mit Netzwerkfunktionen als Sicherheitsfunktionen angeboten, können jedoch von Schwachstellen betroffen sein. Netzwerkrelevante Schwachstellen können dazu führen, dass vorgegebenen Authentifizierungsmechanismen teilweise oder vollständig umgangen werden können. Hierzu zählen die Möglichkeiten zum Authentication Bypass by Spofing oder Capture-replay, die Missing Authentication for Critical Function und die Improper Access Control.

Notwendige Bedingungen zur Ausnutzung der Schwachstellen

Die Ausnutzung von Cyberangriffen über netzwerktechnisch relevante Schwachstellen auf KVM-Switches ist wie bei allen netzwerktechnisch relevanten Schwachstellen abhängig von der Vernetzung der IT-Komponente und den eingerichteten kommunikativen Möglichleiten. Je Bei starker Einschränkung der Kommunikation z. B. bei Nutzung von Insellösungen oder aber einem stark gemanagten Netzwerk müssen Angreifer zur Ausnutzung kommunikationstechnischer Schwachstellen also bereits Zugang zur Kommunikation des relevanten Netzwerkabschnittes besitzen. Werden KVM-Switches zur Signalübertragung über das Internet oder in Großnetzwerken verwendet, ist in solchen Fällen ist für die Angreifer ein unspezifischer Netzwerkzugriff ausreichend oder auch ein direktes Ansteuern der KVM-Switches aus dem Internet möglich, wie z. B. die Redfish Schwachstelle CVE-2024-54085 ermöglichte.

Sich ergebende Angriffsmöglichkeiten

Die Angriffsmöglichkeiten auf KVM-Switche über die Nutzung von Schwachstellen in der Netzwerkkommunikation ergeben sich aus den potenziellen Konsequenzen der kommunikationstechnischen Schwachstellen und aus den angesteuerten Systemen der KVM-Switches. Typische Anwendungsgebiete für KVM over IP sind z. B. die Möglichkeit zur Serversteuerung und Wartung einer Vielzahl von Servern über einen einzelnen entfernten Arbeitsplatz, aber auch z. B. die Einrichtung eines Bedienerarbeitsplatzes eines betrieblich, sicherheits- oder sicherungstechnisch relevanten IT-Systems einer kerntechnischen Anlage abseits des Installationsorts der Hardware oder an mehreren notwendigen Bedienorten in und außerhalb der Anlage.

Grundsätzlich ist für einen solchen Angriff ein Netzwerkzugriff notwendig, dieser ermöglich in Abhängigkeit vorliegender Schwachstellen Angriffsmöglichkeiten in den vier Bereichen Remote Code Execution, Denial of Service, Informationsabfluss und Authentifizierung.

- Informationsabfluss: KVM-Switche dienen zur Übertragung von Eingabedaten und der Darstellung von Ausgabedaten. Erfolgreiche Angriffe können es Angreifern potenziell ermöglichen diese Daten auszulesen und zu nutzen, z. B. mit Keyloggern. Die sich hierbei ergebenden Angriffsmöglichkeiten beeinträchtigen die Vertraulichkeit der Informationen der Clienten und damit der zugehörigen IT-Systeme.
- Denial of Service: Ermöglichen es Angriffsmöglichkeiten die Funktionsweisen eines KVM-Switches in einer Form zu beeinträchtigen, dass dieser nicht mehr vollständig oder gar nicht mehr seine Aufgaben wahrnehmen kann, kommt es zu einem Denial of Service. In der Konsequenz werden keine Signale mehr vom KVM-Switch übertragen, Wartungsarbeiten können nicht mehr stattfinden und verbundene Systeme nicht mehr bedient werden. Automatisierte Aufgaben der verbundenen IT-Systeme und IT-Komponenten funktionieren jedoch weiterhin.
- Authentifizierung: Einige KVM-Switche mit IP Funktionen bieten Authentifizierungsmechanismen an, sodass spezifische Benutzergruppen spezifische angeschlossenen IT-Komponenten ansteuern können oder die Einstellungen und Konfigurationen des KVM-Switchs ändern können. Die sich hieraus ergebenden Konsequenzen sind abhängig von den Einsatzaufgaben des KVM-Switches, grundsätzlich können die Vertraulichkeit, Verfügbarkeit und Integrität des KVM-Switches eingeschränkt werden.

- Remote Code Execution: Remote Code Execution beschreibt solche Schwachstellen, welche die Ausführung von Fremden Code auf den betroffenen Komponenten ermöglicht. In einem solchen Fall werden die Verfügbarkeit, Integrität und Vertraulichkeit des KVM-Switches erheblich beeinflusst.

Potenzielle Auswirkungen auf Gesamtsysteme

KVM-Switches dienen dem Umschalten und der Übertragung von Ein- und Ausgabesignalen für IT-Komponenten. Ihre Funktionen können diese analog, digital und über IP-Funktionen durchführen. Analoge KVM-Switches sind grundsätzlich nicht bezüglich Schwachstellen zu besorgen, da diese keine Software im herkömmlichen Sinne einsetzen. Digitale KVM-Switches ohne Netzwerkfunktionen können zwar potenziell von bestimmen Angriffsmöglichkeiten betroffen sein, jedoch nicht von netzwerktechnischen Schwachstellen. Ausschließlich solche KVM-Switches, welche Netzwerkfunktionen besitzen und welche damit in ein Netzwerk angebunden werden, sind entsprechend potenziell von kommunikativen Schwachstellen betroffen.

KVM-Switches mit IP Funktionen werden in manchen IT-System mit betrieblicher, sicherheits- und sicherungstechnischer Relevanz in kerntechnischen Anlagen eingesetzt, z. B. zur Ausgestaltung von Arbeitsplätzen abseits des Installationsortes der zentralen Hardware oder zur Bedienung und Wartung installierter Komponenten. Werden die eingesetzten KVM-Switches mit IP Funktionen in ihrer Vertraulichkeit, Verfügbarkeit und Integrität eingeschränkt, wird insbesondere die Möglichkeit der Bediener und Nutzer auf das IT-System einzuwirken bzw. dessen Informationen zu erhalten stark eingeschränkt oder unterbunden. Aufgrund der spezifischen Funktionsweise der KVM-Switche sind die tatsächlichen Auswirkungen auf das Gesamtsystem limitiert, wenn von den KVM-Switches keine weiterreichenden netzwerktechnischen Angriffe ausgehen. Schwachstellen wie CVE-2024-54085 zeigen jedoch, dass bei netzwerktechnischen Angriffen auf KVM-Switches durchaus umfassende Konsequenzen für das gesamte IT-System in Bezug auf die Vertraulichkeit, Verfügbarkeit und Integrität drohen.

Die tatsächlichen Konsequenzen sind jedoch auch abhängig vom Gesamtaufbau des betroffenen IT-Systems bzw. angeschlossenem Netzwerk. Sicherungsmaßnahmen und der Einsatz getrennter Netzwerke über VLANs und Firewalls ermöglichen einen Schutz der eingesetzten Netzwerke. Bei Einsatz von KVM-Switches über sehr große Distanzen und damit über das Internet bestehen weitere Angriffsmöglichkeiten, die auf die auf den

direkten Verbindungsaufbau der KVM-Switches resultieren. Getroffene Schutzmaßnahem wie der Einsatz verschlüsselter Kommunikation, VPN-Dienste und netzwerktechnischer Segmentierung können entsprechenden den Angriffsmöglichkeiten entgegenwirken.

5.11 Zusammenfassung AP 3

Mit den Arbeiten im Arbeitspaket 3 wurden die in den Arbeitspaketen 1 und 2 durchgeführten Arbeiten genutzt um die netzwerkrelevanten Schwachstellen und sich aus diesen ergebenden Angriffsmöglichkeiten auf generische IT-Komponenten, welche zumeist in IT-Systemen sicherheits- und sicherungsrelevanter Bedeutung in kerntechnischen Anlagen und Einrichtungen verwendet werden, zu übertragen und auszuwerten. Insgesamt neun IT-Komponenten wurden somit im Arbeitspaket 3 auf ihre Angriffsmöglichkeiten, lokalen Auswirkungen und Gesamtauswirkungen auf zugehörige IT-Systeme untersucht. Die Auswirkungen zeigen, dass netzwerktechnische Schwachstellen einzelner Komponenten eine Gefahr für das gesamte IT-System und auch die darüber hinaus vernetzten IT-Systeme sind. Insbesondere Systeme, die für die Bereitstellung des Netzwerkes fungieren, wie Switche innerhalb der Netzwerke und Router von den Netzwerken nach außen, spielen bei Angriffsmöglichkeiten und deren potenzielle Auswirkungen für kerntechnische Anlagen eine gesonderte Rolle. Insgesamt zeigt sich im Arbeitspaket 3, dass netzwerkrelevante Schwachstellen zu erheblichen Angriffsmöglichkeiten auf die betroffenen IT-Komponenten und IT-Systeme führen können.

6 Zusammenfassung und Ausblick

In kerntechnischen Anlagen eingesetzte IT-Systeme müssen entsprechend ihrer sicherheits- und sicherungstechnischen Bedeutung vor Cyberangriffen geschützt werden. Hierzu zählen auch die datentechnischen Verbindungen dieser IT-Systeme sowie ihre Kommunikation. In den letzten Jahren wurden mit Veröffentlichungen wie Amnesia:33 wiederkehrend eine Vielzahl zum Teil kritischer Schwachstellen bekannt, die in Netzwerkkomponenten eingesetzte Software betrafen. Diese Netzwerkkomponenten bzw. ihre Software werden im Rahmen der allgemeinen Lieferketten weit und teils undurchsichtig und ohne genaue Kenntnisse der letztlichen Anbieter von IT-Komponenten in diesen verbaut. So ist erwartbar, dass bereits bekannt gewordene Schwachstellen auch solche IT-Komponenten betreffen, die in IT-Systemen mit sicherheits- oder sicherungstechnischer Bedeutung in kerntechnischen Anlagen Verwendung finden. Weiterhin ist es erwartbar, dass bislang unerkannte und zukünftig bekannte und teils von Angreifern genutzte Schwachstellen die Netzwerkfunktionen solcher IT-Komponenten mit Relevanz für kerntechnische Anlagen und Einrichtungen betreffen.

Um bestehende Sicherungsmaßnahmen zu prüfen und langfristige Sicherungsmaßnahmen zum Schutz vor bestehenden, potenziellen und zukünftigen Schwachstellen in der Netzwerkkommunikation von sicherheits- und sicherungsrelevanten IT-Systemen bzw. derer IT-Komponenten zu erfassen, wurden in diesem Vorhaben bereits bekannt gewordene Schwachstellen und die sich hieraus ergebenden Angriffsmöglichkeiten ausgewertet. Die Erkenntnisse aus dieser Auswertung können zur Entwicklung und Überarbeitung von Anforderungen im SEWD-Regelwerk IT zur Cybersicherheit kerntechnischer Anlagen und Einrichtungen genutzt werden. Auch kann generisch überprüft werden, inwieweit aktuelle Regelwerksanforderungen und die daraus resultierenden Sicherungsmaßnahmen gegen derartige Angriffsmöglichkeiten wirksam oder abdeckend sind. Darüber hinaus kann es zur Entwicklung von Angriffsszenarien genutzt werden. Die Aufbereitung der Angriffsmöglichkeiten in Bezug auf Schwachstellen innerhalb der Netzwerkkommunikation bzw. der zugehörigen Soft- und Hardware wurde daher in diesem Vorhaben im Rahmen dreier technisch-wissenschaftlicher Arbeitspakete durchgeführt.

Die Fähigkeiten von potenziellen IT-Angreifern, die jeweilige Angriffsoberfläche der einzelnen kerntechnischen Anlagen und der sich daraus für die Angreifer ergebende Handlungsspielraum sowie die sich hieraus ergebende IT-Bedrohungslage ändern sich kontinuierlich mit dem Fortschritt von Wissenschaft und Technik. In Deutschland wurde zum Schutz von IT-Systemen in kerntechnischen Anlagen im Jahr 2013 die SEWD-

Richtlinie IT /BMU13n03/ erlassen, die die Umsetzung umfassender Sicherungsanforderungen für eingesetzte IT-Systeme festschreibt. Um weiterhin die Effektivität der einschlägigen Anforderungen sowie die Absicherung vor im Rahmen der Fortentwicklung von Wissenschaft und Technik möglichen IT-Einwirkungen zu gewährleisten, sind kontinuierliche Analysen und Auswertungen der möglichen Fähigkeiten von IT-Angreifern sowie gegebenenfalls Anpassungen der getroffenen Sicherungsmaßnahmen vorzunehmen.

Im Arbeitspaket 1 wurden zuerst für die Netzwerkkommunikation von IT-Systemen kerntechnischer Anlagen und Einrichtungen relevante Standards der Netzwerkkommunikation identifiziert. Hierzu wurden insgesamt 12 Standards für die Netzwerkkommunikation vorgestellt. Im weiteren Schritt wurden Schwachstellen anhand der CVE-Datenbank identifiziert, welche den einzelnen Standards als Schwachstellen zugeordnet werden konnten. Die Schwachstellen betrafen dabei überwiegend nicht die Standards selbst, sondern die zur Realisierung der Netzwerkkommunikation notwendige Software sowie durch das Alter der Standards entstandene Best Practices, welche von der verarbeitenden Software nicht vollständig umgesetzt wurden und somit eine Schwachstelle ergaben. In Arbeitspaket 1 wurden insgesamt 280 relevante Schwachstellen identifiziert.

Im Arbeitspaket 2 wurden die im vorherigen Arbeitspaket erkannten Schwachstellen entsprechend ihrer Wirkungsweise anhand der CWE-Kennungen kategorisiert und die grundsätzlichen Angriffsmöglichkeiten entsprechend der Wirkungsweise identifiziert. Hierbei wurden aus den mehr als 900 unterschiedlichen CWE-Kategorien 19 Kategorien identifiziert, welche für die im Arbeitspaket 1 und damit für die Netzwerkkommunikation relevanten Schwachstellen bedeutend sind. Somit konnten insgesamt 19 Wirkungsweisen von Schwachstellen im Arbeitspaket 2 identifiziert werden, die für Angriffsmöglichkeiten auf die Netzwerkkommunikation als relevant und möglich betrachtet werden können.

Im Arbeitspaket 3 wurden zunächst generische IT-Komponenten, welche in sicherheits- und sicherungsrelevanten IT-Systemen kerntechnischer Anlagen Verwendung finden können, identifiziert. Anschließend wurden die im Arbeitspaket 2 grundsätzlich identifizierten Angriffsmöglichkeiten auf die generischen IT-Komponenten angewendet und die so für diese IT-Komponenten spezifischen möglichen Angriffsmöglichkeiten, deren Auswirkungen auf die Komponenten, Gesamtsysteme und Netzwerke, analysiert.

Damit konnte insgesamt eine umfassende Auswertung der sich aus Schwachstellen in der Netzwerkkommunikation ergebenden Angriffsmöglichkeiten auf IT-Komponenten kerntechnischer Anlagen- und Einrichtungen durchgeführt werden. Hierdurch lassen sich die Auswirkungen solcher Angriffe auf sicherheits- und sicherungsrelevante Schwachstellen kerntechnischer Anlagen potenziell abschätzen und darauf aufbauend bestehende und mögliche zukünftige Sicherungsmaßnahmen bewerten.

Für die Zukunft können langfristig auf Basis dieses Vorhabens spezifische Untersuchungen möglicher Sicherungsmaßnahmen entsprechend bestehender nationaler und internationaler Regelwerke durchgeführt werden. Hierdurch können bei weiterführenden Untersuchungen aufbauend auf den im Rahmen der drei oben genannten Arbeitspakete durchgeführten Arbeiten, Aussagen zur Wirkungsweise dieser Regelwerke und möglicher erforderlicher weitergehender Sicherungsmaßnahmen in Bezug auf Netzwerke und Schwachstellen in der Kommunikation kerntechnisch relevanter IT-Systeme getroffen werden.

Literaturverzeichnis

/BMU13n01/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Interpretationen zu den Sicherheitsanforderungen an Kernkraftwerke, November 2013

/BMU13n02/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, Interpretations of the Safety Requirements for NPPs of 22/11/2012, November, 29th 2013

/BMU13n03/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, 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)

/BMU13n04/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, Lastannahmen zur Auslegung kerntechnischer Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter mittels IT-Angriffen (IT-Lastannahmen), VS-Vertraulich, 08.07.2013

/BMU13n05/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit, Erläuterungen für die Zuordnung der IT-Systeme von Kernkraftwerken zu IT-Schutzbedarfsklassen, VS-Vertraulich, 08.07.2013

/BMU15n01/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Sicherheitsanforderungen an Kernkraftwerke, November 2012, Neufassung vom 3. März 2015

/COP22r01/ Mazlum Copurkuyu, Thomas Barton, Extraktion und Analyse von Schlüsselwörtern in einer Literaturrecherche zu Quantum Computing, Informatik 2022, Lecture Notes in Informatic (LNI), Gesellschaft für Informatik, Bonn 2022

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

/GRS16i02/ GRS-Weiterleitungsnachricht "Schadsoftwarefund im Kernkraftwerk Gundremmingen, Block B", August 2016

/GRS16i03/ GRS-Weiterleitungsnachricht "Unregelmäßigkeiten bei wiederkehrenden Prüfungen in den Blöcken 1 und 2", September 2016

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

/GRS21r04/ GRS, IT-Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen - Stand Mai 2021, GRS - 647, ISBN 978-3-949088-36-0, August 2021

/GRS21r12/ GRS, A. Schug, O. Rest, C. Quester, IT-Sicherheit in der Lieferkette, GRS-638, 2021

/LNI22r01/ D. Demmler, D. Krupka, H. Federrath (Hrsg), INFORMATIK 2022, Lecture Notes in Informatics (LNI), Extraktion und Analyse von Schluesselwoertern in einer Literaturrecherche zu Quantum Computing

Abbildungs- und Tabellenverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-911727-39-6