Systematische Untersuchung von meldepflichtigen Ereignissen aus Sicht der Sicherung zur Ermittlung potenzieller Einwirkungspfade auf IT-Systeme

GRS - 802

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Systematische Untersuchung von meldepflichtigen Ereignissen aus Sicht der Sicherung zur Ermittlung potenzieller Einwirkungspfade auf IT-Systeme

Abschlussbericht

Alexander Schug
Laura Kleinert
Oliver Rest

Dezember 2024

Anmerkung:

Das diesem Bericht zugrunde liegende Eigenforschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4720R01640 durchgeführt.

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

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

GRS - 802
ISBN 978-3-910548-95-4

Deskriptoren

Einwirkungspfade, Ereignisse, Informationssicherheit, IT-Sicherheit, kerntechnische Anlage

Kurzfassung

Eine zentrale Aufgabe der GRS ist die Gewinnung wissenschaftlicher Erkenntnisse im Bereich der Sicherheit, der Sicherung und 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. Seit mehr als 20 Jahren etabliert sich in deutschen kerntechnischen Anlagen für sicherheitsrelevante und sicherungsrelevante Aufgaben der Einsatz von Informationstechnik. Neben informationsverarbeitenden Bürosystemen handelt es sich auch um einzelne oder vernetzte leittechnische Systeme und um Sicherungssysteme, die entsprechende sicherheits- und sicherungsrelevante Aufgaben übernehmen. In kerntechnischen Anlagen im Ausland ist dieser Etablierungsprozess noch deutlich stärker wahrzunehmen als in Deutschland, dennoch besitzt ein heutiges deutsches Kernkraftwerk hunderte verschiedener informationstechnischer Systeme.

Seit sich informationstechnische Systeme im Einsatz befinden, besteht die Möglichkeit der unerwünschten Einwirkung auf diese. Gemäß Atomgesetz (AtG) § 43 sind kerntechnische Anlagen mittels baulicher und sonstiger technischer sowie personeller und organisatorischer Maßnahmen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter zu schützen. In Deutschland wurde daher im Jahr 2013 die „Richtlinie für den Schutz von IT Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD Richtlinie IT)“ (VS-NfD) /BMU13a/ erlassen.

Um einen fortwährenden Schutz eingesetzter Informationstechnik in kerntechnischen Anlagen zu gewährleisten, ist somit eine stetige Erforschung des Standes von Wissenschaft & Technik im Bereich von Einwirkungen auf Informationstechnik notwendig. Eine Quelle zur Erforschung des sich fortentwickelnden Standes von W&T ist die Auswertung der kontinuierlich erzeugten Betriebserfahrung in kerntechnischen Anlagen, welche mittels nationalen und internationalen Reportingsystemen in Form von aufgelaufenen Ereignissen beschrieben wird.

Entsprechend wurden in diesem Eigenforschungsvorhaben nationale und international gemeldete Ereignisse kerntechnischer Einrichtungen in Bezug auf die Informationssicherheit ausgewertet und zugehörige Einwirkungspfade mit den ermittelten Ereignissen entwickelt. Diese Einwirkungspfade beschreiben den aktuellen Stand, welcher sich aus der gemeldeten Erfahrung nationaler und internationaler kerntechnischer Anlagen im Hinblick auf W&T bezüglich Einwirkungen auf informationstechnische Systeme, ergibt.

Daher wurden im vorliegenden Eigenforschungsvorhaben sämtliche gemeldeten nationalen und internationalen betrieblichen Ereignisse kerntechnischer Anlagen der Jahre 2011 bis 2021 auf solche Informationssicherheitsbezüge untersucht und entsprechend basierend auf dieser Untersuchung potenzielle IT-Einwirkungen ermittelt. In ungefähr 4% der nationalen nach AtSMV gemeldeten Ereignisse und ca. 6% der mittels der IAEA IRS Plattform gemeldeten Betriebsereignisse wurden relevante Bezüge zur Informationssicherheit bzw. digitalen Systemen erkannt, wodurch ca. 80 Ereignisse zur Auswertung in den weiteren Arbeitspaketen vorlagen.

Im Arbeitspaket 2 wurden die 80 weiteren Ereignisse teilweise im Detail ausgewertet. Die soweit ausgewerteten IT-Ereignisse dienten im Rahmen der Arbeiten am Arbeitspaket 2 der Ausarbeitung von insgesamt 9 IT-Einwirkungspfaden. Insgesamt wurden durch diese Arbeiten 9 IT-Einwirkungspfade aus gemeldeten Ereignissen kerntechnischer Anlagen abgeleitet. Darüber hinaus wurde den schnellen Entwicklungen im modernen Arbeitsumfeld im Rahmen der COVID-19 Pandemie Rechnung getragen und sich vertieft mit den Auswirkungen der Etablierung von Fernzugriffen, Homeoffice und mobilen Arbeiten auf kerntechnische Anlagen beschäftigt, wobei hierdurch der zehnte IT-Einwirkungspfad „Fernzugriffe“ entwickelt wurde, der den auch in kerntechnischen Anlagen stattfindenden Trend zur Fernarbeit in die Arbeiten des Vorhabens einfließen lässt.

Insgesamt zeigte sich im Rahmen des Vorhabens, dass mit der Auswertung von kerntechnischen Ereignissen aus Sicht der Informationssicherheit und der hieraus konsequent entwickelten IT-Einwirkungspfade eine Möglichkeit zur technisch-wissenschaftlichen Bewertung und Abgleich bestehender Informationssicherheitsanforderungen und Regelwerke entwickelt werden kann.

Abstract

One of GRS' main tasks is to gain scientific knowledge in nuclear safety, security and cybersecurity. The GRS therefore develops the basis for scientific contributions to the further development of safety and security standards both in Germany and internationally. The regulations on safety, security and cybersecurity must be continuously developed in line with technical progress to improve safety and security. Information technology has been used for safety and security-related tasks in German nuclear facilities for over 20 years. This includes information-processing IT-systems as well as individual or networked I&C systems and safety systems. This process is even more pronounced in foreign nuclear facilities, but a modern German nuclear facility still has hundreds of different information technology systems.

Since information technology systems have been in use, there has been the possibility of undesired interference with them. According to Section 43 of the Atomic Energy Act (AtG), nuclear facilities must be protected against disruptive measures or other third-party interference by means of structural, technical, personnel and organizational measures. In Germany, the confidential malicious acts IT guideline /BMU13a/ was therefore issued in 2013.

To ensure the continuous protection of information technology used in nuclear facilities, it is therefore necessary to constantly research the state of the art in the field of impacts on information technology. One source for researching the evolving state of the art is the evaluation of continuously generated operating experience in nuclear facilities, which is described by means of national and international reporting systems in the form of reported events.

Accordingly, in this research project, national and international reported events of nuclear facilities were evaluated regarding cybersecurity and associated impact paths were developed with the identified events. These impact paths therefore describe the current possibilities and potentials in regards of nuclear cybersecurity based on real systems, process and events in nuclear facilities.

Therefore, in this research project, all reported national and international operational events of nuclear facilities from 2011 to 2021 were examined for such cybersecurity references and their impacts as well as potential impacts were investigated. Relevant references to cybersecurity or digital systems were identified in approximately 4% of the

national events reported within the German national reporting system within the timeframe and approximately 6% of the operational events reported via the IAEA IRS platform, which meant that approximately 80 events were available for further evaluation.

The most promising events were furthermore evaluated in detail. These events evaluated to this extent were used to develop a total of 9 impact paths. In total 9 impact paths were derived from reported events at nuclear facilities. In addition, the rapid developments in the modern working environment in the context of the COVID-19 pandemic were considered and the effects of the establishment of remote access, home office and mobile working on nuclear facilities were dealt with in depth, whereby the tenth impact path “remote access” was developed, which incorporates the trend towards remote working, which is also taking place in nuclear facilities, into the work of the project.

Overall, the project showed that the evaluation of core technical events from a cybersecurity perspective and the resulting impact paths can be used to develop a possibility for the technical-scientific evaluation and comparison of existing cybersecurity requirements and regulations.

Inhaltsverzeichnis

1 Einleitung

Eine zentrale Aufgabe der GRS ist die Gewinnung wissenschaftlicher Erkenntnisse im Bereich der Sicherheit, der Sicherung und 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 sicherheitsrelevante und sicherungsrelevante Aufgaben der Einsatz von Informationstechnik. Neben informationsverarbeitenden Bürosystemen, handelt es sich auch um einzelne oder vernetzte leittechnische Systeme und um Sicherungssysteme, die entsprechende sicherheits- und sicherungsrelevante Aufgaben übernehmen. In kerntechnischen Anlagen im Ausland ist dieser Etablierungsprozess noch deutlich stärker wahrzunehmen als in Deutschland, dennoch besitzt ein heutiges deutsches Kernkraftwerk hunderte verschiedener informationstechnischer Systeme.

Seit sich informationstechnische Systeme im Einsatz befinden, besteht die Möglichkeit der unerwünschten Einwirkung auf diese. Gemäß Atomgesetz (AtG) § 43 sind kerntechnische Anlagen mittels baulicher und sonstiger technischer sowie personeller und organisatorischer Maßnahmen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter zu schützen. Mit dem Stuxnet Angriff auf iranische kerntechnische Einrichtungen im Jahr 2010 wurde die Sicherung in der Informationstechnik kerntechnischer Einrichtungen zu einem bedeutenden Schwerpunktthema, in welchem staatliche Regulierungsbehörden Regelwerke analog zur konventionellen Sicherung erarbeiteten.

In Deutschland wurde daher im Jahr 2013 die „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“ (VS-NfD) /BMU13a/ erlassen.

Informationstechnik und dementsprechend Einwirkungen auf Informationstechnik sind von Beginn an rapide erfolgenden Entwicklungen und damit einem sehr schnellen technischen Fortschritt ausgesetzt. Hierdurch haben sich nicht nur die Einsatzmöglichkeiten von informationstechnischen Systemen in kerntechnischen Anlagen erweitert bzw. haben diese bisherige analoge Systeme verdrängt, sondern auch die anzunehmenden Störmaßnahmen und sonstige Einwirkungen Dritter stark weiterentwickelt. Um einen fortwährenden Schutz eingesetzter Informationstechnik in kerntechnischen Anlagen zu gewährleisten, ist somit eine stetige Erforschung des Standes von Wissenschaft & Technik im Bereich von Einwirkungen auf Informationstechnik notwendig. Eine Quelle zur Erforschung des sich fortentwickelnden Standes von W&T ist die Auswertung der kontinuierlich erzeugten Betriebserfahrung in kerntechnischen Anlagen, welche mittels Reportingsystemen in Form von aufgelaufenen Ereignissen beschrieben wird.

In Deutschland werden Ereignisse gemäß Atomrechtlicher Sicherheitsbeauftragten- und Meldeverordnung (AtSMV) verpflichtend gemeldet, sodass die Betriebserfahrung hierrüber vertiefend ausgewertet werden kann. Neben technischen Mängeln und Fehlfunktionen weisen solche gemeldeten Ereignisse auch menschliche Fehlhandlungen auf und ermöglichen damit einen Einblick in potenziell einer möglichen Einwirkung vorschubleistende Sachverhalte. International steht mit dem „International Reporting System for Operational Experience“ (IRS) eine ähnliche Erfahrungssammlung zur Verfügung. Die GRS wertet diese Erfahrung bisher kontinuierlich und systematisch aus dem Blickwinkel der Sicherheit aus; aus Sicht der Sicherung und Informationssicherheit jedoch nur in Einzelfällen. Insbesondere Ereignisse, welche technische Mängel, Fehlfunktionen oder menschliche Fehlhandlungen in Bezug auf informationstechnische Systeme beschreiben, ermöglichen jedoch umfassendere Rückschlüsse auf die Informationssicherheit kerntechnischer Anlagen und das Fortschreiten von W&T der eingesetzten Technik. Hieraus lassen sich entsprechend tatsächlich aufgetretene Einwirkungspfade, wie auch potenziell mögliche Einwirkungspfade, ermitteln.

Entsprechend werden in diesem Eigenforschungsvorhaben nationale und international gemeldete Ereignisse kerntechnischer Einrichtungen in Bezug auf die Informationssicherheit ausgewertet und zugehörige Einwirkungspfade mit den ermittelten Ereignissen

entwickelt. Diese Einwirkungspfade beschreiben den aktuellen Stand, welcher sich aus der gemeldeten Erfahrung nationaler und internationaler kerntechnischer Anlagen im Hinblick auf W&T bezüglich Einwirkungen auf informationstechnische Systeme, ergibt.

2 Stand von Wissenschaft & Technik

Mit der Steigerung der Leistungsfähigkeit informationstechnischer Systeme, kommt es zu einer zunehmenden Verbreitung derselben in kerntechnischen Anlagen. Darüber hinaus werden zunehmend bislang analoge Systeme, aufgrund der zum Teil ausschließlichen Verfügbarkeit digitaler Systeme, mit informationstechnischen Systemen ersetzt. Infolge dieser Prozesse nahm der Anteil von informationstechnischen Systemen in deutschen und internationalen kerntechnischen Anlagen stetig zu. Zeitgleich zu diesem Anstieg hat sowohl die generelle Anzahl an Einwirkungen als auch die Art der Einwirkungen auf informationstechnische Systeme zugenommen. Mit dem Stuxnet Angriff von 2010 ist die Erforschung von Einwirkungen auf informationstechnische Systeme, insbesondere von Kernkraftwerken, verstärkt in den Fokus von Wissenschaft & Technik gerückt.

Auf die Einwirkungen mittels der Schadsoftware Stuxnet wurde von der GRS mit der Weiterleitungsnachricht 2010/07 bzw. 2010/07a /GRS10i01/ reagiert. Aufgrund von Stuxnet wurde erstmalig weltweit aufgezeigt, dass direkte schadhafte Einwirkungen mit Anlagenschäden, über Einwirkungen auf die Informationstechnik von kerntechnischen Anlagen, möglich sind. Die Schadsoftware zeigte einen umfassenden Einwirkungspfad über USB-Sticks in die Anlage und anschließender entsprechender Weiterverbreitung unter Ausnutzung bis dahin unbekannter Schwachstellen in Betriebssystemen und Leittechniksystemen, auf. Als Konsequenz aus der WLN 2010/07 bzw. 2010/07a /GRS10i01/, begann unter Beteiligung der GRS die Entwicklung einer Richtlinie zur Verhinderung von potenziellen Eingriffen auf informationstechnische Systeme in Deutschland, welche als SEWD-Richtline IT (VS-NfD) /BMU13n03/ im Jahr 2013 bekanntgemacht wurde.

Seit 2013 hat sich der Stand von Wissenschaft & Technik im Bereich der Informationstechnik stark weiterentwickelt. Eine stärkere Vernetzung, ein starker Trend zu einer verzweigten und bausteinbasierten Entwicklung führten zur Ausbildung einer umfassenden Softwarelieferkette. Vormals analoge Systeme wurden aus monetären Gründen und Beschaffungsschwierigkeiten von digitalen Systemen aus dem Markt gedrängt, wodurch in weiterer Folge die softwarebasierte Kommunikation durchweg an Bedeutung zunahm. Gleichzeitig haben sich die schadhaften Einwirkungen konsequent fortentwickelt.

Die GRS begleitet diese Entwicklungen wissenschaftlich und hat mit dem Bericht GRS-647 /GRS 21r04/ im Mai 2021 einen umfassenden Überblick zur Entwicklung der Bedrohungslage in Bezug auf industrielle Steuerungssysteme und kritische Infrastrukturen veröffentlicht. In dieser Arbeit wurden, die sich seit Jahren abzeichnenden Entwicklungen im Bereich der Einflussnahme durch Dritte auf die Informationssicherheit anhand publik gewordener Einwirkungsereignisse in kritischen Infrastrukturen, erfasst und ausgewertet. Die Arbeit wird im Rahmen des Vorhabens FKZ 4721R01610 kontinuierlich fortgesetzt, um den Stand von Wissenschaft & Technik im Bereich der Informationssicherheit dauerhaft zu erfassen. In dem Bericht GRS-638 /GRS21r12/ wurden im Jahr 2021 die von der GRS erworbenen Erkenntnisse zu Einwirkungen über Lieferketten auf kerntechnische Anlagen, kritische Infrastrukturen und andere informationstechnische Systeme, veröffentlicht. Darüber hinaus wird im Hinblick auf die Informationssicherheit von Lieferketten, von der GRS, weiterhin im Rahmen des Vorhabens FKZ 4721R01630 im Hinblick auf die potenziellen Ein- und Auswirkungen auf kerntechnische Anlagen geforscht.

Die Beschreibung von tatsächlichen und potenziellen Einwirkungen ermöglicht im Rahmen der Informationssicherheit die Ermittlung von erforderlichen Sicherungsmaßnahmen zum Erreichen eines ausreichenden Schutzniveaus. Daher ist die kontinuierliche Beobachtung und Ermittlung von Entwicklungen im Bereich der Informationstechnik ein notwendiges Mittel zur Fortschreibung des Standes von Wissenschaft & Technik. Insbesondere im kerntechnischen Bereich ist es bisher nach Kenntnissen der GRS jedoch nicht zu einer solchen ausführlichen Auswertung der aktuell zur Verfügung stehenden IT-Einwirkungspfade auf kerntechnische Anlagen gekommen. Im Gegensatz zu Einwirkungen auf nicht nukleare Informationstechnik und kritische Infrastrukturen, ist die Anzahl der öffentlich bekannt gewordenen IT-Einwirkungen auf kerntechnische Anlagen sehr gering, sodass nur ein geringer direkter Erfahrungswert über solche Anlagen und damit geringe Erkenntnis zum Stand von Wissenschaft & Technik vorliegt. Die kontinuierlich im Rahmen von nationalen und internationalen Reportingsystemen veröffentlichten Ereignisse aus der Betriebserfahrung kerntechnischer Anlagen bieten jedoch über direkte Einwirkungen hinausgehende Einblicke in den Umgang mit Informationssystemen in kerntechnischen Anlagen. Solche Erfahrungen umfassen daher neben direkten Einwirkungen auch menschliche Fehlhandlungen, systematische und sporadische Systemfehler und weitere Ereignisse. Diese Ereignisse ermöglichen Rückschlüsse auf potenzielle informationstechnische Eingriffe auf diese Systeme, sodass sich hieraus direkte IT-Einwirkungspfade im kerntechnischen Kontext ableiten lassen.

Nach bisherigen Erkenntnissen ist eine solche systematische Auswertung der Betriebserfahrung im Hinblick auf die Informationssicherheit und potenzielle IT-Einwirkungen ein Novum.

Damit zeigt sich, dass bisher ein Forschungsbedarf einerseits zur Auswertung der Betriebserfahrung aus Sicht der Informationssicherheit und darüber hinaus zur Entwicklung von potenziellen Einwirkungspfaden aus diesen Erkenntnissen heraus besteht. Die somit entwickelten IT-Einwirkungspfade ermöglichen damit langfristig auch einen Abgleich mit bislang in Deutschland gültigen Sicherungsmaßnahmen und können daher einen Beitrag zur Fortschreibung des nationalen (und auch internationalen) kerntechnischen Regelwerks bezüglich der Informationssicherheit darstellen.

3 AP 1: Identifikation von meldepflichtigen Ereignissen mit IT-Sicherheitsrelevanz

Meldepflichtige Ereignisse gemäß AtSMV ermöglichen seit 1965 einen Einblick in die nationale Betriebserfahrung von kerntechnischen Anlagen und deren vertiefte Auswertung, darüber hinaus werden international Ereignisse von den Mitgliedsstaaten freiwillig über die IRS-Plattform der Internationalen Atomenergie-Behörde (IAEA) seit 1980 gemeldet. Über beide Meldesysteme liegen somit jeweils mehrere tausend Ereignisse aus über 40 Betriebsjahren kerntechnischer Anlagen, zumeist Kernkraftwerke, vor. Um eine effiziente und effektive Erkennung von gemeldeten Ereignissen mit Informationssicherheitsrelevanz zu ermöglichen, sind dafür geeignete Verfahren zum Screening der Ereignisse zu nutzen. Weiterhin ist es sinnvoll, den Zeitraum der gemeldeten Ereignisse zu präzisieren.

Im Arbeitspaket 1 wurde daher zu Beginn des Vorhabens der zu betrachtende Zeitraum zur Identifikation von meldepflichtigen Ereignissen mit Informationssicherheitsrelevanz identifiziert. Die Einführung von informationstechnischen Systemen in kerntechnischen Anlagen begann bereits vor mindestens 20 Jahren, mit dem Stuxnet Angriff sind Einwirkungen auf und über diese Systeme deutlich in den Fokus der Aufmerksamkeit gerückt. Gleichzeitig basieren viele nationale sowie internationale Regelwerke, Richtlinien und Leitlinien auf den Erfahrungen und Rückschlüssen, die aus dem Stuxnet Angriff 2010 gewonnen wurden. Hiermit rückten insbesondere die Ereignisse in den Fokus, welche nach 2010 gemeldet wurden. Daher wird zur Ausarbeitung von IT-Einwirkungspfaden, welche auf gemeldeten Ereignissen mit Informationssicherheitsrelevanz basieren, ein Analysezeitraum ab dem 01.01.2011 in Betracht gezogen. Im Arbeitspaket 1 sind daher sämtliche Ereignisse seit dem 01.01.2011 im Rahmen des Screenings auf Informationssicherheitsrelevanz hin, in den Blick genommen worden.

Dies führte zu einer gemeldeten Ereignismenge von ca. 1.000 nationalen und ca. 900 internationalen Ereignissen im Zeitraum von 2011 bis 2022. Um den Umfang der Ereignisse auf Aussagen, Informationen und Relevanz bezüglich der Informationssicherheit zu überprüfen, wurden geeignete Screeningmethoden verwendet.

3.1 Angewendete Screeningmethoden

Im betrachteten Zeitraum sind ca. 1900 nationale und internationale Ereignisse kerntechnischer Anlagen gemeldet worden.

Aufgrund dieses enormen Umfangs wurden im Vorhaben frühzeitig Methoden in Betracht gezogen, um insbesondere Ereignisse mit Informationssicherheitsrelevanz zu identifizieren mit folgenden Merkmalen: Einerseits die direkte Beteiligung digitaler Systeme oder den Rückschluss auf Prozesse mit Beteiligung digitaler Systeme.

Im Rahmen etablierter Screenings von vorliegenden Datensätzen wird grundsätzlich die Analyse anhand festgelegter Kenngrößen vollzogen. So werden Ausreißer identifiziert, inkorrekte Daten erkannt und Abweichungen herausgestellt. Für die textliche Analyse wird zumeist auf maschinenunterstützte Auswertung von Schlagworten, Multi-Wort-Phrasen und wiederkehrende sprachliche Konstruktionen zurückgegriffen. Sowohl für nationale als auch internationale Ereignisse standen Methoden wie die Schlagwortsuche zur Verfügung. Darüber hinaus werden für das Screening von Texten insbesondere Titel- und Abstract-Screenings als anerkannte Screeningmethoden empfohlen. Zusätzlich werden sowohl nationale als auch internationale Ereignisse entsprechend ihrer Merkmale kategorisiert, sodass ein Screening anhand ausgewählter Merkmale möglich ist. /COP22r01/

Aufbauend hierauf wurden insgesamt drei Screeningmethoden initial für das Screening von Ereignissen im Rahmen des Vorhabens verwendet:

- Maschinelles Auslesen von Schlagworten und Wort-Kombinationen
- Manuelles Auswerten von Ereigniszusammenfassungen
- Auswertung von kategorisierten Ereignissen

Mit allen drei Verfahren gemeinsam, konnte ein zielsicheres Screening der Ereignisse mit Bezug zu IT-Systemen sichergestellt werden. Dazu wurden die drei Screeningmethoden parallel genutzt und die entsprechenden Ergebnisse untereinander abgeglichen. Bei Überschneidungen sowie besonders auffälligen Ergebnissen der Auswertung der Zusammenfassung, wurde im Detail der IT-Bezug festgestellt.

3.2 Screening von nationalen Ereignissen

Im Beobachtungszeitraum von 2011 bis 2022 wurden ca. 1000 gemeldete nationale Ereignisse über die VERA-Datenbank zur Verfügung gestellt.

Davon entfallen 858 auf die Jahre 2011 bis 2020. Aufgrund der Zeitverzögerung von Ereigniseintritt bis zur endgültigen Meldung sind die im Vorhaben ebenfalls untersuchten Jahre 2021 und 2022 unvollständig für eine umfassende Auswertung.

Von den 858 im Zehnjahreszeitraum 2011 bis 2020 gemeldeten nationalen Ereignissen wurden insgesamt 32 Ereignisse mit Bezügen zu IT-Systemen, also dem direkten Einsatz von IT-Komponenten oder aber Ereignissen im Rahmen von Prozessen, die auf einsetzbare IT-Komponenten Rückschlüsse ermöglichen, vorgelegt, wie in Abb. 3.1 dargestellt wird:

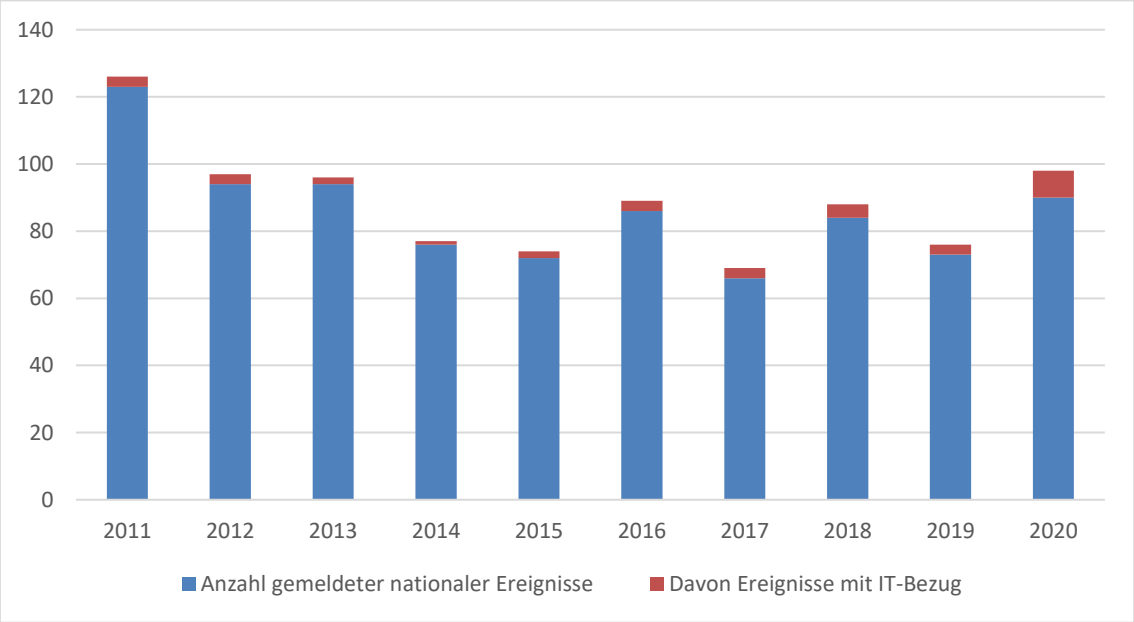

Abb. 3.1 Gemeldete nationale kerntechnische Ereignisse der Jahre 2011 bis 2020

Blau: Anzahl der gemeldeten Ereignisse; Rot: Anzahl der davon mit IT-Bezug identifizierten Ereignisse

Die Anzahl der nationalen Ereignisse mit IT-Bezug bleibt mit Ausnahme des Jahrs 2020 durchgängig im niedrigen einstelligen Prozentbereich und umfasst zumeist 1 bis 4 erkannte Ereignisse. Obwohl in den letzten zwei Jahrzehnten intensive Modernisierungsmaßnahmen in deutschen kerntechnischen Anlagen umgesetzt wurden, sind

IT-Systeme bei den nationalen Ereignissen damit sehr gering repräsentiert. Insbesondere Materialermüdungen sind häufig wiederkehrende Ereignisse, von welchen IT-Systemen ausgesprochen selten betroffen sind.

3.3 Screening von internationalen Ereignissen

Im Beobachtungszeitraum von 2011 bis 2022 wurden ca. 900 gemeldete internationale Ereignisse über die IRS-Datenbank der IAEA zur Verfügung gestellt. Davon entfallen 812 auf die Jahre 2011 bis 2020. Aufgrund der Zeitverzögerung zwischen Ereigniseintritt bis zur endgültigen Meldung, sind die im Vorhaben ebenfalls untersuchten Jahre 2021 und 2022 unvollständig für eine umfassende Auswertung der gescreenten internationalen Ereignisse.

Von den 812 im Zehnjahreszeitraum 2011 bis 2020 gemeldeten internationalen Ereignisse wurden insgesamt 47 Ereignisse mit Bezügen zu IT-Systemen, also dem direkten Einsatz von IT-Komponenten oder aber Ereignissen im Rahmen von Prozessen, die auf einsetzbare IT-Komponenten Rückschlüsse ermöglichen, vorgelegt, wie in Abb. 3.2 dargestellt wird:

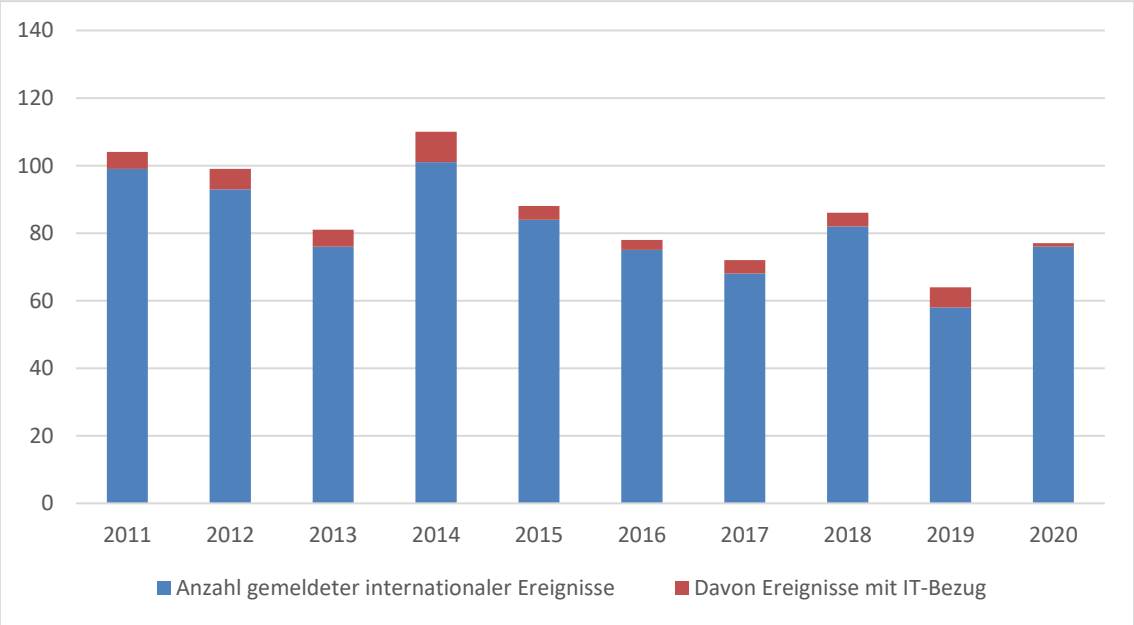

Abb. 3.2 Gemeldete internationale kerntechnische Ereignisse der Jahre 2011 bis 2020

Blau: Anzahl der gemeldeten Ereignisse; Rot: Anzahl der davon mit IT-Bezug identifizierten Ereignisse

Die Anzahl der internationalen Ereignisse mit IT-Bezug ist mit Ausnahme des Jahres 2020 durchgängig höher als bei den nationalen gemeldeten Ereignissen. Aufgrund von Neubaumaßnahmen sowie international von Deutschland abweichenden Regeln und Erfahrungen zum Umgang und Einsatz von IT-Systemen in auch sicherheits- und sicherungstechnisch relevanten Bereichen, ist von einem vermehrten Einsatz von IT-Systemen in internationalen kerntechnischen Anlagen auszugehen. Mit insgesamt ca. 50 % mehr Ereignissen mit IT-Bezug im Vergleich zu den nationalen Ereignissen hat sich diese Annahme bestätigt.

3.4 Zusammenfassung AP 1

Es wurden mehr als 1900 Ereignisse der nationalen VERA-Datenbank wie auch der internationalen IRS-Datenbank der IAEO auf Bezüge zu IT-Systemen untersucht. In den annähernd vollständig vorliegenden Ereigniszeiträumen von 2011 bis 2020 wurden insgesamt 79 Ereignisse mit IT-Bezügen identifiziert, wovon ca. 60 % auf internationale Ereignisse zurückzuführen sind. Mittels der Anwendung etablierter Screeningmethoden, wie der maschinellen Auslesung von Schlagworten und dem Abstract-Screening konnte eine entsprechend breite Bandbreite von Ereignissen mit IT-Bezügen identifiziert werden. Obwohl die Gesamtzahl der identifizierten Ereignisse insgesamt nur 4 % beträgt, wurde damit mit dem AP 1 das Ziel erreicht eine ausreichende und umfassende Datenbasis für die weiteren Arbeitsschritte der folgenden Arbeitsprogramme auszuarbeiten.

4 AP 2 Ermittlung potenzieller Einwirkungspfade

Mit den gescreenten Ereignissen liegen mehr als 70 Ereignisse kerntechnischer Anlagen aus den Jahren 2011 bis 2021 vor, welche Rückschlüsse auf potenziell mögliche Einwirkungspfade bieten. Als Einwirkungspfad wird hierbei als Pfad verstanden, welcher unter bestimmten Umständen von sonstigen Dritten ausgeführt werden kann, um auf ein oder mehrere IT-Systeme mittels distinktiven Vorgehensweisen einzuwirken. Abgegrenzt wird innerhalb der Pfade zwischen distinktiv unterscheidbaren Handlungen, mit welchen Handlungen eines weiteren Einwirkungspfades beschrieben werden. Zur Ausarbeitung von Einwirkungspfaden sind die im Rahmen des Screenings erhaltenen Informationen noch nicht vollständig auswertbar, hierfür ist eine spezifische detaillierte Auswertung der gescreenten Ereignisse notwendig, wobei hierfür insgesamt 27 repräsentative Ereignisse ausgewählt wurden. Diese Auswertung wurde beginnend im Rahmen des Arbeitspakets 2 ausgeführt um anschließend IT-Einwirkungspfade zu entwickeln.

4.1 Detaillierte Auswertung von Ereignissen mit IT-Bezug

Nationale, nach AtSMV meldepflichtige Ereignisse in kerntechnischen Anlagen sowie internationale Ereignisse publiziert über die IRS-Plattform der IAEA, werden seit langer Zeit von der Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH vertieft ausgewertet. Da hierbei jedoch nur bei unmittelbarem Vorliegen von IT-Sicherheitsvorfällen wie z. B. einer Virusinfektion, auch auf den Einfluss auf/von IT-Systemen und den sich hieraus ergebenden IT-Sicherheitsimplikationen eingegangen wird, ist eine detaillierte Auswertung der gescreenten Ereignisse notwendig. Hierbei konnte aufbauend auf die bereits im Rahmen der bisheriger Auswertung erlangten Erkenntnisse, weiterführend gearbeitet werden.

Alle Ereignisse wurden entsprechend der tatsächlichen und potenziellen Konsequenzen, der grundlegenden und unterstützenden Ursachen, der von den Betreibern beschriebenen Lektionen, der eingeleiteten Maßnahmen, der betroffenen IT-Systeme, der Zugänglichkeit dieser sowie der Redundanz hin ausgewertet. Weiterhin wurden vertieft entsprechende Lektionen für die IT-Sicherheit ausgewertet. In den Abschnitten 4.1.1 und 4.1.2 werden diese Auswertungen zusammenfassend für die jeweiligen Ereignisse dargestellt.

Über die Ereignisse hinaus wurde in diesem Vorhaben auf die veränderten Arbeitsumgebungen im Rahmen der COVID-19 Pandemie reagiert. Auch im kerntechnischen Umfeld wurden vermehrt, sofern möglich, Arbeiten von den Anlagen in heimische Umgebungen überführt. Dieser Trend hat sich sowohl im Inland mit klar definierten Grenzen sowie im Ausland mit weniger klar definierten Grenzen gezeigt. Aufgrund dieser neuen Arbeitsumgebung sind neue potenzielle IT-Einwirkungspfade denkbar, welche sich jedoch noch nicht in meldepflichtigen Ereignissen niedergeschlagen haben. Um dennoch die aktuellen Entwicklungen im Forschungsvorhaben mitzubetrachten, wurde daher neben der detaillierten Auswertung nationaler und internationaler Ereignisse auch eine Konferenz mit dem Focus auf Cybergefahren im Rahmen neuer Arbeitsumgebungen im Heimumfeld (mobiles Arbeiten, Homeoffice) besucht.

4.1.1 Nationale Ereignisse

Die detailliert ausgewerteten nationalen meldepflichtigen Ereignisse nach AtSMV mit IT-Bezug werden in Tab. 4.1 dargelegt

Tab. 4.1 Ausgewertete nationale Ereignisse mit IT Bezügen

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
2011/040: Abweichung bei den eingesetzten Kalibrierwerten von Aktivitätsmessstellen nach Austausch von Messumformern	Messgeräte zur Aktivitätsüberprüfung müssen regelmäßig kalibriert werden. Hierbei werden Kalibrierfaktoren eingesetzt. Seit Austausch der Messumformer von analog zu digital wurden falsche Kalibrierfaktoren verwendet, ein zu niedriger Aktivitäts-Messwert wurde somit bestimmt.	Gezielte Manipulation von Kalibrierwerten wie auch von Messgeräten ist denkbar, um fehlerhafte Freimessungen zu erreichen. Manipulation vor Ort oder über Datenbanken möglich, auch über die Lieferkette.
2021/044: Ausfall des Drehzahlgebers der Laufbrücke der BE-Lademaschine	Bei Revisionsarbeiten kam es zu einem Defekt an einem Drehzahlgeber der Laufbrücke der BE-Lademaschine. Die Betriebsbremsen wurden mit zwei Sekunden Verzögerung ausgelöst, ursächlich war ein Überlastung der internen BUS-Verbindung	Die interne BUS-Verbindung wurde durch Datenströme überlastet. Diese Überlastung der Kommunikation wie auch Überlastung von IT-Komponenten selbst kann durch externe Aktionen beeinflusst bzw. ausgelöst werden.
2012/066: Unverfügbarkeit der automatischen Schließanregung von Brandschutztüren aufgrund Fehler in der Steuerung der Brandmeldeanlage	Im Rahmen einer WKP (wiederkehrenden Prüfung) wurde die automatische Schließfunktion von vier Brandschutztüren nicht bei Aktivierung der zugeordneten Brandmelder ausgelöst. Ursächlich ist Konfigurations-/Parameteranpassung durch einen Techniker entgegen der Arbeitsanweisung	Durch fehlerhafte Konfiguration/Manipulation wurden entsprechende IT-Funktionen der Brandmeldeanlage Außerkraftgesetzt. Konfigurations- und Parametermanipulationen sind für eine Vielzahl von IT-Systemen denkbar.

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
2012/504: Funktionsstörung an der Lüftungsanlage PG	Die Steuerung der Lüftungsanlage erhielt ein Softwareupdate. Nachfolgend kam es wiederholt zur Messung von Differenzdruck-Grenzwertüberschreitungen. Ursächlich war, dass mit dem Softwareupdate die Grenzwertauslösung auf eine Spanne von 0 Sekunden geregelt wurde, sodass kurzfristige Druckschwankungen zur Auslösung der Differenzdruck-Grenzwertüberschreitung führten.	Softwareupdates sind für IT-Systeme aus sicherheits- oder sicherungstechnischen Gründen wiederkehrend notwendig. Solche Updates ermöglichen jedoch auch über die Lieferkette einen Einfluss dritter auf betroffene IT-Systeme. In diesem Fall lag eine menschliche Fehlhandlung während der Installation des Softwareupdates vor.
2013/066: Fehlerhafte Auslösung von Brandschutzklappen im USUS infolge einer Störung in der Brandmeldeanlage MF51	Aufgrund eines unbekannten Softwarefehlers in der Brandmeldeanlage kam es zu Fehlauslösungen zweier Brandschutzklappen in beiden vorhandenen Redundanzen des USUS-Gebäudes. Der Fehler war nicht reproduzierbar.	Softwarefehler bieten typischer Weise Angriffspunkte für sonstige Einwirkungen Dritter. Gezielte Manipulationen der betroffenen Systeme sind denkbar.
2015/007: Fehlerhaft eingestellte Parameter für den Start der Konzentrationsberechnung nach Filterwechsel an Aerosolmessstellen	Durch eine fehlerhafte Parametrisierung wurde auf dem Anzeige- und Überwachungssystem der Aerosolaktivitätsmessstellen der Kaminfortluftüberwachung ein falscher Status angezeigt wurde.	Durch fehlerhafte Parametrisierung wurden entsprechende Anzeigen fehlerhafte Zustände dargelegt. Konfigurations- und Parametermanipulationen sind für eine Vielzahl von IT-Systemen denkbar.

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
2015/503: Abweichung von spezifischen Werten bei der WKP der Krananlagen SMF11/SMF12	Nach Umrüstung wurde eine WKP an einer Krananlage ausgeführt. Digitale Steuerungskomponenten zeigten hierbei Abweichungen von spezifisch festgelegten Werten auf und betrafen neben der Steuerung die Bremszeiten und die Richtungsüberwachung des Haupthubwerks wie auch eine nicht umgesetzte Schlüsselschalter-Quittierung	Im Rahmen der Projektierung und Umsetzung der Funktionen der umgerüsteten Krananlage kam es zu einer fehlerhaften Parametrisierung und Konfiguration der zu Krananlage gehörenden Steuerungskomponenten. Konfigurations- und Parametermanipulationen sind für eine Vielzahl von IT-Systemen denkbar.
2016/022: Detektion von Büroschadsoftware auf mehreren Rechnern	Auf verschiedenen IT-Systemen der betroffenen Anlage wurden alte Windows-Schadsoftwaren entdeckt. Diese wurden über USB-Sticks innerhalb der Anlage verbreitet und betrafen auch solch einen USB-Stick, mit welchem zuvor Daten vom Visualisierungsrechner der Lademaschine ausgelesen wurden.	Aufgrund des fehlerhaften Einsatzes von USB-Sticks konnten, die innerhalb der Anlage genutzten „Luftschnittstellen“ von Schadsoftware überwunden werden. Hierbei wurden Prozess-Vorgaben nicht eingehalten. Entsprechende Übertragung von Schadsoftware mittels Wechseldatenträgern ist grundsätzlich eine Einwirkungsmöglichkeit auf IT-Systeme
2016/025: Virenbefund auf Rechnern der Anlagensicherung	Nach Ereignis 2016/022 wurde im betroffenen Kernkraftwerk eine Untersuchung der eigenen IT-Systeme durchgeführt, bei welcher Schadsoftware auf eingesetzten und ersatzweise gelagerten Rechnern des Personen-Kontroll-Systems gefunden wurde. Es handelte sich um Schadsoftwaren aus dem Jahr 2010 und früher. Es ist von einer Infektion bei Installation und Lieferung des Systems auszugehen.	Der Schadsoftwareeintrag wurde über Fehler im Rahmen der Installation und Lieferung möglich, also eine Einwirkung über die Lieferkette. Darüber hinaus kam es noch zu Verbreitungen der Schadsoftware über bestehende Netzwerkverbindungen.

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
2016/044: Baugruppenfehler in einer Brandmeldezentrale	Während der WKP einer Brandmeldeanlage wurde festgestellt, dass Signale von insgesamt sieben Brandmeldeleitungen nicht weitergeleitet wurden. Diese Fehler traten 14 Tage später erneut auf. Ursächlich sind Fehler in der Firmware, die bei bestimmten Handbefehlen den Übergang von Baugruppen in einen fehlerhaften Zustand ermöglichten.	Die Schwachstellen in den Baugruppen der Brandmeldeanlage sind, solange sie softwareseitig nicht behoben werden, ein potenzielles Einfallstor für Schadsoftware und gezielte Manipulationen.
2017/001: RESA wegen Ausfall des Gateway-Rechners TXS/TXP	In der Anlage übernimmt TELEPERM® XS (TXS) die Aufgaben des Reaktorschutzes und TELPERM® XP (TXP) die Aufgaben der betrieblichen Leittechnik. Über einen Gateway-Rechner erhält das TXP System Informationen vom TXS-System. Dieser Gatewayrechner ist aus unbekannten Gründen abgestürzt, der Informationsfluss wurde unterbrochen, eine RESA eingeleitet.	Direkte Ausgestaltung von betrieblicher Leittechnik und Reaktorschutz auf Basis von IT-Systemen. Schwachstelle/Manipulation führt zu Ausfall des Datenflusses.
2018/059: Unterbrechung der Signalübertragung der Gefahrenmeldeanlage zur Warte	Es kam zum wiederholt auftretenden Ansprechen einer Störmeldung der Gefahrenmeldeanlage. Diese Meldung wurde als nicht relevant eingestuft und die zur Meldung gehörende Kommunikationsschnittstelle sollte getrennt werden. Es wurde das falsche Kabel getrennt, sämtliche Störmeldungen wurden nicht mehr übertragen.	Mechanische Einwirkung auf IT-Kommunikation ausführende Komponenten führt zu einer Unterlassung der Meldung von Störmeldungen von der Gefahrenmeldeanlage zur Warte der Anlage. Betriebszustände werden potenziell nicht erkannt, Bewertung von Situationen durch das Personal erschwert.

4.1.2 Internationale Ereignisse

Die detailliert ausgewerteten internationalen gemeldeten Ereignisse über die IRS-Plattform der IAEA mit IT-Bezug werden in Tab. 4.2 dargelegt.

Tab. 4.2 Ausgewertete internationale Ereignisse mit IT Bezügen

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
8312: Automatic Scram from Reactor High Pressure During Main Turbine Load Rejection Test	Bei einem Lastabwurftest bei 43 % Leistung wurde die TUSA ausgelöst, jedoch erfolgte keine automatisch auszulösende RESA. Ein solches Signal zur RESA sollte vom digitalen elektrohydraulischen Steuerungssystem der Turbine automatisch an das Reaktorschutzsystem erfolgen. Da jedoch der hierfür gemessene Turbinendruck unterhalb der Grenzwerte blieb, erfolgte die festgeschriebene RESA nicht.	Die betroffenen IT-Systeme haben fehlerfrei gearbeitet, waren jedoch fehlerhaft konfiguriert, sodass den vorgegebenen Maßnahmen (automatische RESA nach TUSA) nicht gefolgt wurde. Bei direkten Zugriff auf ein solches System kann damit die Auslösung sicherheitstechnischer Maßnahmen verzögert werden.
8485 und 8602: Short Time Unviability of Computer Information and Control System (KIC) Operator Stations	Die Anlage nutzt ein Computer Information and Control System (KIC) als zentrale Leitstelle für die leittechnische Infrastruktur des Kraftwerks und ist vollständig digital realisiert. Kernstück sind ein zentraler Server und ein Server für historische Daten. Nach Wartungsarbeiten wurde der Historienserver wieder mit dem zentralen Server verbunden, woraufhin das gesamte KIC nicht mehr zur Verfügung stand, die Steuerungsplätze der Warte nicht mehr genutzt werden konnten und ein Anlagenausnahmezustand vorlag. Beim Anschluss des historischen Servers wurden so viele Daten auf einmal übertragen, dass die Hardware des zentralen Servers überlastet wurde.	Die Hardware von IT-Systemen muss entsprechend der von diesen Systemen verarbeiteten Daten leistungsgemäß ausreichend ausgestattet werden. In allen drei Ereignissen kam es zu Vorfällen, bei denen dies nicht der Fall war, ein Ausfall der Systems ist die Folge. Solche durch Überlastung herbeigeführte Systemausfälle können auf unterschiedliche Weisen unabsichtlich und absichtlich herbeigeführt werden.
8507 und 8665: Computer Virus Found on Various Plant Laptops and Media	Auf der Brennelementlademaschine zugehörigen Laptops wurde Schadsoftware gefunden. Daraufhin wurden weitere Systeme überprüft und mehr betroffene Laptops und fest installierte PCs mit Schadsoftware entdeckt. Die ersten Infektionen traten 4 Jahr vor Entdeckung auf.	Der Schadsoftwareeintrag wurde aufgrund dauerhafter nichtbeachteter Vorschriften im Umgang mit Wechseldatenträgern ermöglicht. Und zeigt damit sowohl Charakteristiken der Einwirkungen über Wechseldatenträger wie auch (nicht wissender) Innentäter.

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
8551 und 8532: Recent Issues related to the Commercial grade dedication of Allen Bradley 700-RTC Relays (NRC Information Notice 2016-01)	Zeitrelais eines Notstomdiesel zeigten sich als nicht zuverlässig. Es wurden baugleiche Ersatzteile eingebaut. Auch diese waren unzuverlässig. Es zeigte sich, dass die Zeitrelais keine elektromagnetische Verträglichkeit aufwiesen. Diese fehlte, weil die Zeitrelais vom Hersteller überarbeitet wurden und dabei digitale programmierbare Bausteine in die Zeitrelais eingebaut wurden.	Entgegen der Erwartung wiesen Komponenten digitale Bauteile auf. Diese wurden vom Hersteller in die Komponenten eingebaut, ohne Typenbezeichnung, Anleitung oder ähnliches zu ändern und den Anwendern dies mitzuteilen. In Eingangstests wurden die Änderungen nicht erkannt. Unerwartete digitale Komponenten werden nicht entsprechend der Vorgaben zum Schutz von IT-Systemen geschützt und sind daher anfällig, erfüllen zumeist gleichzeitig jedoch nicht die Spezifikationsanforderungen.
8545: Incidents involving Configuration Control at Wylfa Power Station During 2012	Während des „Inter Reactor Exchange“ (IRX) Vorhabens wurden weitere Maßnahmen installiert, um sicherzustellen, dass die Reaktoren nicht kritisch werden können. Aufgrund von Flüchtigkeitsfehlern und mangelnden Tests wurde eine selbstprogrammierte Lösung zur Warnung bei Anhebung von Steuerstäben fehlerhaft implementiert, sodass während der IRX arbeiten das Anheben von Steuerstäben nicht korrekt gemeldet wurde.	Das neue Warnsystem sollte verhindern, dass mehr als ein Steuerstab einer bestimmten Sorte gleichzeitig angehoben wird. Diese Anzeigen konnte das System nicht ausführen, da es fehlerhaft programmiert und getestet wurde. Fehlerhafte Software, geliefert oder selbst programmiert, kommt vor, fehlerhafte Tests verschärfen das Problem.
8576 und 8375: Programmable Technology in Qualified Relays results in Expiration of Qualification	In mehreren Anlagen wurden Relays aufgefunden, welche für den sicherheitsrelevanten Einsatz als analoge Systeme qualifiziert waren, jedoch digitale programmierbare Bausteine beinhalteten.	Unerwartete digitale Komponenten werden nicht entsprechend den Vorgaben zum Schutz von IT-Systemen geschützt und sind daher anfällig, erfüllen zumeist gleichzeitig jedoch nicht die Spezifikationsanforderungen.

Ereignisnummer	Kurzzusammenfassung	IT-Bezüge
8657: Level Fluctuation of Steam Generator caused by sudden close of Feedwater Flow Control Valve	Ein Speisewasserventil schloss sich unerwartet innerhalb von 3 Sekunden von vollständiger Öffnung zu keiner Öffnung. Ursächlich war eine programmierbare Leittechnikkarte, deren Ausgangssignal von 20mA auf 4mA abgefallen ist.	Es lag ein nicht nachvollziehbarer Zufallsfehler vor, der sich bei identischen Karten nicht wiederholte. Bei einer angenommenen Manipulation besteht keine Steuerungsfähigkeit mehr für das betroffene Ventil. Bei flächendeckender Manipulation würde umfassende leittechnische Funktionen nicht mehr bereit stehen.
8671: KIC Operator Station short unavailability	Mitarbeiter der Warte erkannten, dass das rechnerbasierte Computer Information and Control System (KIC) nicht verfügbar war. Ursache war, dass anstatt dem programmierbaren Parameter „1ARE003KU“ der Parameter „1APA003KU“ konfiguriert wurde, wodurch das System einen Fehler erkannte und den KIC-Server stoppte. Gemäß der Dokumentation sollte der Parameterfehler nicht zu einem Systemstopp führen.	Fehlerhafte Parametrisierungen sind typische Fehler im Umgang mit digitalen Komponenten und können sowohl unbeabsichtigt als auch im Rahmen von sonstigen Einwirkungen Dritter herbeigeführt werden.
8791: Faked In-Service Inspections	Im Rahmen der Untersuchung eines gemeldeten Ereignisse ist erkannt worden, dass die regelmäßigen Untersuchungen nicht durchgeführt wurden und deren Ergebnisse gefälscht wurden.	Auch wenn die betroffenen System keine digitalen Systeme waren, so sind deutliche Übertragbarkeiten auf IT-Systeme feststellbar, da wiederkehrende software- und hardwareseitige Integritätsprüfungen für IT-Systemen unerlässlich sind.

4.1.3 Fernzugriffe

Mit der COVID-19 Pandemie entstand ab 2020 ein deutlicher Trend zur Verlagerung von Telearbeit innerhalb von Arbeitsstandorten zur Telearbeit unter Nutzung von Heimarbeitsplätzen. Um einen Einblick in die sich hieraus ergebenden Einwirkungs- und Sicherungsmöglichkeiten der Informationstechnik kerntechnischer Anlagen zu erhalten, wurde deshalb im Rahmen dieses Forschungsvorhabens die Konferenz „Cyber Security Summit“ des Informationssicherheitsunternehmens Mandiant virtuell besucht. Die Konferenz fand als hybride Konferenz in Washington D.C sowie auf einer virtuellen Plattform statt. Unter dem Stichwort „Defending The New Normal“ waren die zentralen Themenaspekte hierbei, die sich mit der Umorganisation der Arbeitswelt im Rahmen der COVID-19 Pandemie ergebenden Gefahren für die Informationstechnik von Unternehmen, Behörden und kritischer Infrastruktur. Referiert wurde im Verlauf der Konferenz von Herstellern, von Informationssicherheitsberatern, von Regierungsmitarbeitern und von Anwendern aus der Industrie sowie des Infrastrukturbereiches.

Mit der COVID-19 Pandemie hat eine drastische Umgestaltung innerhalb der Arbeitswelt stattgefunden. Zuvor war Telearbeit mittels Heimarbeitsplätzen eher die Ausnahme, während der Pandemie wurde die Telearbeit mittels Heimarbeitsplätzen in den USA und Europa zur Hauptarbeitsform auf dem Gebiet des Telearbeitens. So wurde während der Konferenz dargelegt, dass über 50 % der Telearbeit in den USA aktuell von zuhause aus durchgeführt wird und mehr als 30 % zusätzlich in hybriden Wechselsystemen arbeiten. Auch nach der Pandemie wird erwartet, dass es keine Rückkehr mehr zu überwiegenden Anwesenheitspflicht gibt und das Wechselmodel von Heim- und Büroarbeitsplatz die Mehrheit der Telearbeiten repräsentieren wird. Hieraus ergeben sich eine Vielzahl von neuen Einwirkungsmöglichkeiten. Es wurden innerhalb kürzester Zeit die für die Heimarbeit notwendigen Technologien wie VPN-Verbindungen, Netzwerkanbindungen, Cloudarbeitsplätze und Cloud-Datenspeicher innerhalb von Unternehmen und Behörden etabliert, sodass die Aspekte der Informationssicherheit in diesem Umfeld insbesondere zu Beginn der Pandemie nicht ausreichend gewürdigt wurden und es vermehrt informationsbasierte Angriffe auf diese Technologien gab. Die daraufhin eingeführten Informationssicherheitsmaßnahmen wie Mehrfaktorauthentifizierungen für VPN-, Netzwerk- und Cloudzugänge wurden von den Mitarbeitern nicht immer positiv angenommen, da diese als disruptiv für den Arbeitsprozess betrachtet wurden. Weiterhin führte die Einführung von Arbeitsüberwachungsmaßnahmen dazu, dass die Mitarbeiter zur Umgehung dieser Maßnahmen gegen die Informationssicherheitsvorschriften verstießen.

So wurden unbekannte Programme, welche die dauerhafte Simulierung eines Arbeitsprozesses für die Überwachungsprogramme versprachen, ohne Absprache mit Vorgesetzten und Informationssicherheitsbeauftragten heimlich auf den Arbeitssystemen installiert. Insgesamt sank infolge der Umgestaltung der Arbeitswelt vor dem Hintergrund der COVID-19 Pandemie das informationstechnische Sicherungsniveau, während gleichzeitig die Aufgabenlast der Informationssicherheitsbeauftragten in Unternehmen und Behörden stark anstieg. Eine insgesamt erhöhte Anzahl von Ereignissen, welche vom Heimarbeitsplatz schwieriger zu bearbeiten waren, führte hier zu einer Überlastung von Mitarbeitern der Informationssicherheit, was in weiterer Folge zu Unternehmenswechseln und Kündigungen führten und die Situation so weiter verschärfte.

Während des Forschungsvorhaben wurde darüber hinaus bekannt, dass international wie auch national vermehrt die Möglichkeit zur Heimarbeit in kerntechnischen Anlagen umgesetzt wurde. Hierzu zählen insbesondere verwaltende Arbeiten und Büroprozesse. Gleichfalls jedoch weitergehende administrative Tätigkeiten und auch vereinzelte Fernwartungen für IT-Systeme, bei denen dies als möglich und sicher angesehen wird.

4.1.4 Auswertung internationaler Ereignisse in Bezug auf Prozesse und eingesetzte IT-Systeme

Mittels des Screening von internationalen Ereignissen auf IT-Bezüge wurden im Laufe des Arbeitspakets 1 auch Einsichten in den Einsatz von IT-Systemen in kerntechnischen Anlagen außerhalb Deutschlands gewonnen. Bisher ist die Informationslage über solche IT-Systeme und die von diesen IT-Systemen ausgestalteten Prozesse innerhalb nicht deutscher kerntechnischer Anlagen relativ gering. Um für zukünftige Forschungsarbeiten diese Datenlage auszubauen, wurden sämtliche über das IRS-System gemeldeten internationalen Ereignisse, bei welchen IT-Bezüge zu erkennen waren, auf die betroffenen IT-Systeme sowie die von diesen IT-Systemen ausgeführten Prozesse hin analysiert. In der folgenden Tab. 4.3 werden diese entsprechend ausführlich dargelegt.

Tab. 4.3 Internationale Ereignisse mit IT Bezug und zugehörigen IT Prozessen bzw. IT Systemen

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8312	Unverfügbarkeit eines RESA-Signals	Mexiko	Digital Electro Hydraulic Conrol System (DEHC), Digitale Hydraulische Drehzahlregelung	Steuerung der Turbinendrehzahl (Kontrolliert die Leistung und die Drehzahl der Hauptturbine)
8224	Auslösung des Überstromschutzes einer Notspeisepumpe	Hungary	Breaker´s protection device stored data	Digitale Speicherung von Daten des Überstromschutzes einer Notspeisepumpe
8292	Verlust der externen Stromversorgung an beiden Blöcken (LOOP) durch fehlerhafte Relais Modifikation	USA	Digitales Schutzrelaissystem	Allgemein Relaissystem: Detektion von Fehlern und anderen Anomalitäten, welche die Schaltanlage (bzw. das Equipment (Armaturen/Einrichtungen) beeinflussen oder in Verbindung mit dem Hauptgenerator stehen. Isolation der betroffenen Armaturen/Einrichtungen von den anderen, sowie die Reduzierung des Einflusses/Auswirkungen des Fehlers auf ein Minimum zu begrenzen. Aufteilung des Relaisschutzsystems: Zone A, B und G. Betroffen ist hier Zone G: Hauptgenerator, sowie Generatorregler, einphasig gekapselte Stromschiene, Sternpunktverbindung, Generatorleistungsschalter. Aufgabe Zone G Überschutzrelais: Öffnen der Leistungsschalter des Hauptgenerators zur Isoaltion von Zone G von den anderen Zonen, Abschalten der Generatorregler oder der Turbinen, Blockierung der Motorantriebstrennung
8301	Fehlauslösung des Vergiftungssystems während Prüfungen	Rumänien	Programmierbarer Digitalvergleicher (Digitaler Komparator)	Elektronischer Schaltkreis, der zwei digitale Werte vergleicht.

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8545	Ereignisse aufgrund erfolgter Änderungen zum Transfer von Brennelementen	Großbritannien	Softwarecode im Data Processing System (DPS) (Datenverarbeitungssystem).Modifikation der Software für die Alarmierung im Falle des Ein- und Ausfahrens von Steuerstäben.	DPS: Verarbeitet eingehende Informationen aus verschiedenen Quellen und updatet die Formate durch ein individuelles Software-Paket (Druck, Temperatur, usw.). Hier geht es im spezifischen, um die Alarmsignale in Bezug auf die Steuerstäbe.
8576	Unerkannter Einsatz nicht qualifizierter Relais mit programmierbaren Bauelementen	Finnland	Programmierbare Relais, die als nicht programmierbar qualifiziert wurden. Mehrere in zwei Anlagen.	Spannungsüberwachungsrelais in der Schaltanlage des Lüftungssystems (Crouzet MUSF 260 AC/DC_65-260V und Crouzet EUSF/ 90-260VAC/VDC). Relais der Notstromdiesel (ABB NF62E und ABB NF44E) sowie Relais der Serie ABB AF (siehe IRS-Meldung 8375). Relais (Carlo Gavazzi DIB02 und DUB01) in Gleichrichtern (Ellego Powertec EVV 26/500 LX LH SH H KV). Relais in der Gleichstromversorgung der Notstromerzeugungsanlage, in den Gleichrichtern von Pumpen des Primärkreislaufs und in der Versorgungsspannungsüberwachung des Steuerstabantriebssystems. Zeitrelais (Schneider Zelio RE7) im Nebenkühlwassersystem. Hersteller: Crouzet, ABB, Gavazzi, Ellego
8558	Ausfall der Druckluftversorgung	USA	Teil der Druckluftversorgung	Fehlerhafte nicht näher beschriebenen Logikschaltung
8671	Vorübergehende Unverfügbarkeit der Bedienstationen des rechnerbasierten Informations- und Steuerungssystems	China	Rechnerbasiertes Informations- und Steuerungssystems (KIC)	Dieses System wird von der Schichtmannschaft zur Visualisierung des Anlagenzustandes, für die Steuerung einiger Geräte oder die Änderung von Parametern verwendet. Überwachung und Kontrolle der Bedienstation wurde vom Backupsystem übernommen.
8512	Unzureichende Testprozedur für intelligente Gerätesteuerungen	Großbritannien	Intelligente Gerätesteuerung	Mikroprozessorbasierte Steuerung der Armatur über eine Ethernet-Schnittstelle (Abblaseregelventil eines Dampferzeugers), MOORE MYCRO 353 Controller

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8507	Computervirus-Funde auf mehreren Laptops und Wechselmedien	Großbritannien	Service-PC der Brennelement Lademaschine/Wechseldatenträger	Prozesse bis hin zur Brennelement Lademaschine. Wechseldatenträger und Servicegeräte können etliche IT-Systeme infizieren und Prozesse beeinflussen.
8501	Kurzschluss bei Arbeiten an einer Freiluftschaltanlage	Russland	Untersystem der Turbinensteuerung (ASUT). Automatisiertes Digitalsystem der Turbinensteuerung	Durchführung von Operationen zur Steuerung der Funktionsgruppe sowie zur Steuerung von Dampfeinlassorganen der Turbine mit Hilfe des elektrohydraulischen Systems der Turbinenregelung in allen Betriebsarten der Turbinenanlage
8602	Vorübergehende Unverfügbarkeit des rechnerbasierten Informations- und Steuerungssystems	China	Rechnerbasiertes Informations- und Steuerungssystems (KIC)	Dieses System wird von der Schichtmannschaft zur Visualisierung des Anlagenzustandes, für die Steuerung einiger Geräte oder die Änderung von Parametern verwendet. Rechner auf der Warte für 30 min unverfügbar. Umschaltung des KIC auf Backupsystem.
8485	Kurzzeitige Unverfügbarkeit der Rechner des rechnerbasierten Informations- und Steuerungssystems	China	Rechnerbasierten Informations- und Steuerungssystem KIC (beinhaltet CCT (zentraler Server) und SAR8 (Server))	Dieses System wird von der Schichtmannschaft zur Visualisierung des Anlagenzustandes, für die Steuerung einiger Geräte oder die Änderung von Parametern verwendet. Überwachung und Kontrolle der Bedienstation wurde vom Backupsystem übernommen.
8297	Leckage am Reaktordruckbehälter aufgrund von nicht ausreichend vorgespannten Bolzen	USA	Digitales Display	Nicht näher genanntes Display zur Zustandsanzeige.
8247	Falsche Nachricht bei Notfallübung versendet	Großbritannien	Schnellwarnsystem (rechnerbasiertes Notsignalsystem)	Erlaubt der Warte Notfall-Nachrichten per Telefon, Fax oder emergency scheme papers zu senden. Informiert über Anlageninterne und -externe Notfälle. Maßnahme: Schnellwarnsystem des Simulators kann nur noch Notfallübungsnachrichten rausschicken.

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8791	Gefälschte Inspektionen	Deutschland	Aktivitätsüberwachungssystem (Aerosol-/Jod-Störfallmonitor)	Überwachung der Aktivität. Murr Elektronik, Typ MPS20-230/24 Single Phase
8551	Probleme mit Relais des Typs Allen Bradley 700-RTC	USA	Relais (integrierter Schaltkreis durch CPLD (Complex Progammable Logic Device) ersetzt	Zeitrelais des Typs Allen Bradley 700-RTC. Generatorschalter zweier Notstromgeneratoren konnten nicht geschlossen werden.
8657	Abfall des Dampferzeugerfüllstands aufgrund Schließen des Speisewasser-Durchflussregelventils	China	Digitale Leittechnikkarte	Typ S200-CCA-SC; der Hersteller ist nicht bekannt. Eingesetzt für die Ventilsteuerung.
8714	Abblasen eines Dampf-erzeugers aufgrund fehlerhafter Vorgaben aus der rechnerbasierten Leittechnik	Ukraine	Rechnerbasierte Leittechnik der Überdruckabsicherung	Genaue Typenbezeichnungen nicht bekannt.
8658	Schwankungen im Dampferzeuger-Füllstand durch ein geschlossenes Ventil in der Speisewasserversorgung aufgrund Softwarefehlbedienung	China	Bedienstation des zentralen Datenverarbeitungssystems (KIT centralized data processing system)	Dieses System wird von der Schichtmannschaft zur Visualisierung des Anlagenzustandes, für die Steuerung einiger Geräte oder die Änderung von Parametern verwendet. Überwachung und Kontrolle der Bedienstation wurde vom Backupsystem übernommen.
8516	RESA nach TUSA der Hauptturbine	Mexiko	Rechnerbasierte elektrohydraulische Turbinenregelung (DEHC)	Kontrolliert die Leistung und die Drehzahl der Hauptturbine, übersendet Daten an weitere Leittechniksysteme.
8946	Erdschluss in der 750-kV-Schaltanlage	Russland	Generatorschutzsystem in Block 4	Unbekannte “Siemens Terminals” für das remote protection system für den Turbinengenerator 4.

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8665	Infektion eines Arbeitsplatzcomputers mit einem Computervirus nach Verstößen gegen Dienstanweisungen	Litauen	Arbeitsplatzcomputer/Servicegerät	Organisation von Instandhaltungs- und Reparaturarbeiten aller Kräne des Kraftwerks (installierte Software Simatic Step 7, Internetzugang ist notwendig)
8782	Manuelle Reaktorschnellabschaltung nach Ausfall der Zwangsumwälzpumpe in einer Treibwasserschleife	USA	Notfallreaktions- und Informationssystems (ERIS)	Onlineüberwachung von diversen Prozessvariablen. Überwacht analoge und digitale Eingangssignale in bestimmten Intervallen, kalkuliert ausgewählte Eingangssignale, verarbeitet die Daten und zeigte diese an.
8398	Bypass des Sicherheitsbehälters durch die Trennung von Impulsleitungen der Ansteuerung eines Sicherheitsventils zu einem unzulässigen Zeitpunkt	Südafrika	Management Programm	Alle Prozesse die mit der Revisionsplanung in Zusammenhang stehen werden in einem digitalen Management Programm verarbeitet.
8209	Neue Erkenntnisse zur Brennstabbelastung bei KMV-Störfällen	USA	Modellierungstool für das Not- und Nachkühlsystem	Berücksichtigung der Abbrandabhängigkeit der Wärmeleitfähigkeit von Brennstoffpellets für das Not- und Nachkühlsystems mit ASTUM-Rechencode der Westinghouse Electric Company
8956	Reaktorschnellabschaltung aufgrund eines zu geringen Füllstandes im Dampferzeuger	Argentinien	Steam Generators Power Water Control System (Boiler Level Control-BLC-Program)	Regulierung des Dampferzeugerfüllstandes durch bspw. die Kontrolle des Füllstandsvegelventils.

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8728	Reaktorschnellabschaltung nach Schutzabschaltung einer Hauptspeisewasserpumpe	USA	Operator Control Station (OCS) (Integrated Control System (ICS)) with an Operations Interface Touchscreen (OIT)	Das OIT zeigt die Turbinenkontroll- und Signalsysteminformationen an. Das MFP Speed Control System steuert das Einspeiseventil (Hoch- und Niederdruck) zur Kontrolle der Turbinendrehzahl über das ICS oder manuell durch den Operator. Das ISC umfasst auch Indikatoren und Alarme in Zusammenhang mit der Turbinenperformance.
8934	Reaktorschnellabschaltung aufgrund der Abschaltung von drei Hauptkühlmittelpumpen	Russland	Leittechnikschrank mit Einrichtungen zur Überwachung (hardware and software instrumentation)	Kurzschluss in Leittechnikschrank. Aufgaben der digitalen Leittechnik nicht vollständig bekannt.
8945	Verstöße gegen geltende Regelwerksanforderungen bei der Verifizierung und Validierung digitaler Leittechniksysteme	USA	Digitale Leittechniksysteme	Unbekannte Nutzung von digitalen Leittechniksystemen
8986	Fehlsignale im Neutronenflussmess- und -überwachungssystem zur Begrenzung der Reaktorperiode im Reaktorschutzsystem aufgrund mangelhafter Softwareverifizierung und -validierung	Russland	Neutronenflussmesssystem und Neutronenüberwachungssystem (NFMS)	Überwachung des Neutronenflusses in allen Betriebszuständen des Reaktors, Überwachung der räumlichen Leistungsdichteverteilung im Reaktorkern.
8989	Auslösung des Notkühlsystems während des Anfahrvorgangs aufgrund der Fehlbedienung eines handbetätigten Schalters	Indien	Computerbasiertes Informationssystem	Aufgaben zur Überwachung des Notkühlsystems

IRS-Nr.	Kurzbeschreibung	Land	IT-System	Prozesse und Hersteller (wenn veröffentlicht)
8023	Nichtverfügbarkeit von HD-Einspeisesystemen durch Fehleinstellung der Durchsatzregler und Nichterkennung der Fehleinstellung durch ungeeignete Prüfung	USA	Digitale Speisewasserregelung	Regelung des Speisewassers, Fehleinstellung der Durchsatzregler des Typs Bailey Type 701.

4.2 Entwicklung von IT-Einwirkungspfaden

Die in Abschnitt 4.1 ausgewerteten gemeldeten kerntechnischen Ereignisse mit IT-Bezügen zeigen in unterschiedlicher Form Angriffsoberflächen und Möglichkeiten zur Einwirkung auf kerntechnisch genutzte IT-Systeme auf. Diese Erkenntnisse zusammenzuführen und fortzuschreiben, ermöglicht die Entwicklung von Einwirkungspfaden auf IT-Systeme kerntechnischer Anlagen, welche im Falle von Einwirkungen sonstiger Dritter potenziell genutzt werden können. Anschließend ermöglichen diese Einwirkungspfade eine zielgenaue Untersuchung, der zum Schutz potenziell betroffener IT-Systeme notwendigen Sicherungsmaßnahmen. Daher beschreiben Einwirkungspfade neben der konkreten Einwirkung auf ein IT-System, die für die Einwirkung notwendigen Bedingungen zur Realisierung der Einwirkung, die potenziellen Auswirkungen sowie die möglichen weiteren Verbreitungen und Übergänge zu nachfolgenden Einwirkungspfaden.

Mit der Auswertung der gemeldeten nationalen und internationalen Ereignisse kristallisierten sich insgesamt neun unterschiedliche Einwirkungspfade mit IT-Bezug heraus, welche neun verschiedene Pfade bzw. Formen der Einwirkung sonstiger Dritter auf kerntechnische IT-Systeme nachvollziehbar beschreiben. Diese IT-Einwirkungspfade sind:

- **Servicegeräte:** Ausnutzung von sogenannten Servicegeräten, welche für die Installation, Datenübertragung und andere Verfahren an diese IT-Systeme angeschlossen werden, welche externe IT-Systeme für entsprechende Verfahren benötigen.
- **Unerkannte IT-Komponenten:** Die absichtliche oder versehentliche Einbringung von Systemen mit unerkannten IT-Komponenten in kerntechnische Anlagen.
- **Überlastung von IT-Systemen:** Die gezielte Herbeiführung von IT-Systemüberlastungen zur Störung der Funktion von IT-Systemen.
- **Lieferkette:** Die Beeinflussung oder Manipulation von Soft- und/oder Hardware, welche an kerntechnische Einrichtungen geliefert wird.
- **Wechseldatenträger:** Die Verbreitung von Schadsoftware über Wechseldatenträger, sowohl bei Datentransport in der Anlage als auch von außen in die Anlage.
- **Versionsmanagement:** Die Beeinflussung von Prozessen zum Verwalten und Ausspielen von Softwareversionen, insbesondere bei Anwendung von Versionierungssoftware und die Manipulation von ausgespielten Softwareupdates über diese.

- **Parametrierung und Konfiguration**: Beeinflussung der in IT-Systemen variablen Parameter sowie der Konfiguration.
- **Netzwerkverbindungen:** Beeinflussung der IT-Systeme mittels Zugriffen, Schadsoftwareübertragung und Verbreitung über bestehende Netzwerkverbindungen.
- **Innentäter:** Die direkte Beeinflussung von IT-Systemen durch auf diese zugreifende Personen mit Vertrauensverhältnis.

Darüber hinaus ergibt sich nachfolgend aus der COVID-19 Pandemie und dem fortgesetzten Trend der Überführung von Arbeiten in das häusliche Umfeld, eine Zunahme der Fernzugriffe. Der IT-Einwirkungspfad **Fernzugriffe** beschreibt hierbei Einwirkungen über temporäre oder dauerhaft bereitgestellte Fernzugriffsmöglichkeiten auf IT-Systeme innerhalb kerntechnischer Anlagen.

4.2.1 Pfadstruktur

Einwirkungspfade bzw. in diesem Fall IT-Einwirkungspfade beschreiben die notwendigen Handlungen und sich daraus ergebenden Möglichkeiten im Rahmen spezifischer Einwirkungsmöglichkeiten auf IT-Systeme.

Zur Beschreibung der entsprechenden IT-Einwirkungspfade werden daher beginnend die hierfür notwendigen Schritte beschrieben. Diese Schritte unterliegen in den meisten Fällen sowohl notwendigen Bedingungen, die für die Einwirkungen vorliegen müssen, als auch hinreichenden Bedingungen, welche die Einwirkungen vereinfachen oder erfolgversprechender machen können.

Im Anschluss erfolgte eine weitere Ausarbeitung des Einwirkungsfades, mit der Darstellung von Zwischenschritten mit dem Ziel der Beeinflussung von IT-Systemen, weiterer Verbreitung und abschließend zum Ende des Einwirkungspfades. Diese Endpunkte beschreiben definierte Übergänge zu anderen IT-Einwirkungspfaden und münden schließlich in potenzielle Zielhandlungen infolge von Einwirkungen.

Diese Zielhandlungen und ihre Auswirkungen werden im Rahmen der Analyse der IT-Einwirkungspfade aufgeteilt auf sowohl *beobachtete Auswirkunge*n im Rahmen der ausgewerteten Ereignisse, als auch *theoretisch denkbare* Auswirkungen bei direkter zielgerichteter Manipulation über die ausgeführten IT-Einwirkungspfade.

IT-Einwirkungspfade werden nicht nur unter bestimmten Bedingungen ermöglicht, es bestehen auch Möglichkeiten für Maßnahmen zur Mitigation, Aufdeckung und Unterbrechung. Diese Möglichkeiten unterscheiden sich und stellen potenzielle Beeinflussungen und Maßnahmen im Einwirkungsfall dar.

4.2.2 Servicegeräte

IT-Systeme mit sicherheits- und sicherungstechnischer Bedeutung sind in den allermeisten Anwendungsfällen auf wiederkehrende Eingabe von Parameterdaten, Programmierungen, Steuerungsbefehlsketten oder die Installation und Wartung von Updates angewiesen. IT-Systeme ohne eigene Eingabefunktionen sind hierbei auf unterstützende IT-Systeme angewiesen, welche über bestehende Schnittstellen die notwendigen Daten für den regulären betrieblichen Ablauf übertragen. Diese unterstützenden IT-Systeme werden in den meisten Fällen je nach Aufgabe als Programmiergerät, Parametrisiergerät oder aber als Engineering Work Station bezeichnet. Aus IT-sicherheitstechnischer Perspektive lassen sich diese Geräte zusammenfassend als Servicegeräte beschreiben, welche sowohl stationär als auch mobil z. B. in der Form eines Laptops eingesetzt werden können. Servicegeräte können je nach Verwendungs- und Sicherungskonzept nur für ein einziges IT-System verwendet werden oder für eine Gruppe von IT-Systemen.

Servicegeräte bieten somit temporäre oder dauerhafte Verbindungen zu IT-Systemen, welche in kerntechnischen Anlagen bedeutsame betriebliche oder sicherheits- bzw. sicherungstechnische Funktionen übernehmen. Im Rahmen von IT-Einwirkungen sind somit IT-Einwirkungen über den Pfad der Servicegeräte als nicht zu unterschätzende Einwirkungsmöglichkeiten zu sehen. Im Rahmen dieses Pfades bestehen verschiedene Möglichkeiten zur Pfadinitialisierung und damit beginnender Beteiligung der Servicegeräte. Das Pfadende ist mit effektiver Einwirkung auf potenzielle Zielsysteme erreicht.

Die Beteiligung von Servicegeräten bei IT-Einwirkungen wurden bereits mehrfach im Rahmen von IT-Ereignissen dokumentiert.

Hierbei steht insbesondere das IRS-Ereignis 8507, welches am 10. Oktober 2014 in Dungeness in Großbritannien stattfand, im Vordergrund. Im Folgenden wird unter Betrachtung dieses und weiterer Ereignisse, in welchen IT-Einwirkungen unter Beteiligung von Servicegeräten stattfanden, ein umfassender IT-Einwirkungspfad „Servicegeräte“ entwickelt und ausführlich dargelegt.

4.2.2.1 Der Einwirkungspfad „Servicegeräte“

Servicegeräte für IT-Systeme mit betrieblicher, sicherheits- und sicherungstechnischer Bedeutung sind die zentralen Steuerungs- und Programmierzugriffssysteme und damit von besonderem sicherheits- und sicherungstechnischem Interesse. Je nach Einsatz und Nutzungskonzept reichen die temporären oder dauerhaften Verbindungen der Servicegeräte von einem einzelnen bis zu einer Mehrzahl an sicherheits- und sicherungstechnisch relevanten Geräten. Zusätzlich müssen auch Servicegeräte in den meisten Fällen mit Daten versorgt werden, z. B. wenn die Hersteller der mit den Servicegeräten bedienten Leittechnik neue Updates veröffentlichen oder aber die Software der Servicegeräte selbst, eine neue Version erhält. Der auf Nutzung der Servicegeräte basierende IT-Einwirkungspfad bündelt somit eine Reihe möglicher Anfänge sowie eine Reihe möglicher Pfadenden und Weiterentwicklungen, welche gänzlich die Nutzung der Servicegeräte einbinden.

Pfadeinleitung

Im Rahmen des Einwirkungspfades auf Servicegeräte für sicherheits- und sicherungstechnisch bedeutsame IT-Systeme in kerntechnischen Anlagen werden eine Reihe möglicher Initialereignisse gebündelt, welche den Pfad einleiten. Hierzu zählen:

- Einwirkungen bei Dateneingang mittels Wechseldatenträgern
- Einwirkungen im Rahmen von Updateprozessen
- Einwirkungen in der Beschaffung
- Direkte Einwirkungen auf das Servicegerät

Somit bestehen eine Reihe von Möglichkeiten zur initialen Einleitung des Einwirkungspfades. Hierbei können unter anderem die Einwirkungspfade „Wechseldatenträgerinfektion“, „Updateprozess“, und „Manipulation im Rahmen von Beschaffung und Installation“ im Servicegerät Einwirkungspfad enden.

Zusätzlich können auch direkte eingebende Tätigkeiten auf das Servicegerät den Einwirkungspfad beginnen. Der Einwirkungspfad hat somit insgesamt vier verschiedene Anfangsstränge.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Servicegeräte“ einzuleiten, sind folgende Bedingungen zwingend notwendig:

- Existenz von Servicegeräten für sicherheits- oder sicherungstechnisch relevante Funktionen einer kerntechnischen Anlage und Nutzung derselben

Sobald ein oder mehrere Servicegeräte für sicherheits- und sicherungstechnisch relevante Funktionen verwendet werden, ist potenziell eine Einwirkungsmöglichkeit über diese Servicegeräte möglich. Aufgrund der verschiedenen einleitenden Möglichkeiten ist dies unabhängig von tatsächlichen Datentransfers zu diesen Servicegeräten. Auch wenn keine Updates, Programmüberträge oder sonstige datentechnischen Übertragungen vorgesehen oder möglich sind, können im Rahmen spezifischer initialisierender Ereignisse IT-Einwirkungen über betroffene Servicegeräte gestartet werden.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Durch erweiterte Nutzungen, Datenaustausch, erweiterte Zugriffsmöglichkeiten und die Nicht-Einhaltung von Sicherungsvorschriften bzw. dem Fehlen dieser, wird die Möglichkeit der Einleitung des IT-Einwirkungspfades „Servicegeräte“ erweitert bzw. vereinfacht. Im IRS-Ereignis 8057 wurde die entdeckte IT-Einwirkung auf ein Servicegerät möglich, weil mehrfach Daten mittels Wechseldatenträgern zwischen verschiedenen Systemen getauscht wurden und die hierbei gültigen Maßnahmen und Regeln nicht vollständig eingehalten wurden.

Unterstützend wirkt somit jede Form von regelmäßigen und sporadischen Datentransfer. Jede Datenzuführung, ob diese betrieblich oder sicherheitstechnisch (z. B. aufgrund von Updates) geboten ist, ist eine potenzielle Einleitung des IT-Einwirkungspfades. Bei regelmäßigen oder sporadisch durchgeführten Updates werden Updatedaten von fremden, auswertigen Stellen bis auf das entsprechende Servicegerät übertragen, sodass mehrfache Einwirkungspotenziale bei den Zwischenschritten der Datenübertragung möglich sind. Werden zusätzlich Schutzmaßnahmen und Regeln nicht ausreichend beachtet, steigt die Wahrscheinlichkeit der Einwirkungsmöglichkeiten.

Pfadzwischenschritte

Nach initialer Einwirkung auf Servicegeräte kann, je nach Einwirkungsform, die Einwirkung auf betroffene IT-Systeme weiter eskaliert werden. Hier zählt die vollständige Systemkontrolle, die automatisierte Verbreitung auf weitere Servicegeräte sowie Wechseldatenträger. Je nach Einwirkungsform kann ein betroffenes Servicegerät die mit diesem Gerät verbundenen Wechseldatenträger für eine Sprunginfektion auf weitere Servicegeräte genutzt werden, wenn die Wechseldatenträger für mehrere Systeme verantwortlich sind. Im Falle des IRS-Ereignisses 8507 waren schlussendlich anlagenweit mehr als 30 Laptops und zwei stationäre PCs von dem einwirkenden Ereignis betroffen.

Pfadende und Pfadübergänge

Servicegeräte dienen der Bedienung von spezifischen IT-Systemen, welche keine vorhergesehenen Eingabe- oder Interaktionsmöglichkeiten in dem Umfang bieten, welche betrieblich oder aus sicherheits- oder sicherungstechnischen Gründen notwendig sind. Hierfür werden Servicegeräte in regel- oder unregelmäßigen Abständen mit den eigentlichen IT-Systemen über bestehende Schnittstellen verbunden, sodass ein Datenaustausch zwischen den Servicegeräten und den IT-Systemen stattfindet. Bei Servicegeräten, welche als stationäre Engineering Work Station ausgelegt werden, besteht eine solche Verbindung potenziell dauerhaft.

Der IT-Einwirkungspfad „Servicegerät“ endet mit der IT-Einwirkung auf die von den Servicegeräten unterstützten IT-Systeme. Dies können z. B. programmierbare Logik-Controller, Schutzschalter mit digitaler Technik, Motorsteuerungen oder ähnliches sein. Je nach Systemaufbau können die Einwirkungen dort weiterverbreitet werden, wodurch der Pfad „Leittechnikverbreitung“ ausgelöst werden kann.

4.2.2.2 Pfadauswirkungen

Die Auswirkungen des IT-Einwirkungspfades „Servicegeräte“ sind abhängig von der Anwendung der Servicegeräte sowie der mit den Servicegeräten bedienten IT-Systemen. Weiterhin führen datentechnische Verbindungen, auch temporäre, zu weiteren potenziellen Auswirkungen. Mit dem IRS-Ereignis 8507 und dem ME-Ereignis 2016/022 sind zwei Ereignisse in kerntechnischen Anlagen bekannt geworden, bei welchen der IT-Einwirkungspfad „Servicegeräte“ mit betroffen war.

Real beobachtete Auswirkungen

In den analysierten Ereignissen ist kein Fall bekannt geworden, bei dem eine absichtlich herbeigeführte Einflussnahme auf Servicegeräte zu einer weiterführenden Einflussnahme von weiteren IT-Systemen führte. Demgegenüber stehen aber mehrere Fälle, bei welchen es zu Infektionen von Servicegeräte mit generischem, teilweise lange veraltetem Schadcode kam. Diese Einflussnahmen blieben eine Zeit lang unentdeckt und die Servicegeräte wurden in dieser Zeit an weitere IT-Systeme angeschlossen.

Die Servicegeräte wurden über Wechseldatenträger infiziert. Hierbei wurden geltende Vorschriften zum Umgang mit Wechseldatenträgern missachtet. Im Falle des IRS-Ereignisses 8507 wurden hierbei insgesamt drei Vorschriften verletzt, sodass eine unbestimmte Anzahl an Laptops, zwei fest installierte PCs und eine Mehrzahl an Datenträgern mit der Schadsoftware infiziert wurden. Die ersten Infektionen fanden im Jahr 2010 statt, weitere im Jahr 2013 und darüber hinaus, entdeckt wurden diese ca. 5 Jahre später, im Jahr 2015. Dabei wurde auch ein Servicegerät der „Fuel Route“, also der Brennelementlademaschine, infiziert. Da es sich bei der Schadsoftware um eine generische, relativ alte Schadsoftware handelte, ist davon ausgegangen worden, dass weder gezielt auf die programmierbare Leittechnik, welche von dem Servicegerät angesteuert werden kann, eingewirkt wurde noch effektive Einwirkungen über die Schadcodeverteilung hinaus stattfanden. Auf den Betrieb der Anlage sowie die Sicherheit der Anlage hatte das Ereignis somit keine effektive Wirkung.

Ähnlich bei dem ME-Ereignis 2016/022 Hier wurde ebenfalls über USB-Sticks eine Schadsoftware auf IT-Systeme der Anlage überspielt. Über einen Übungsrechner kam es zu einer Verschleppung der Schadsoftware auf ein Servicegerät der Brennelement-Lademaschine. Dieser Vorfall wurde 2016 entdeckt, jedoch konnte die ersten Infektionen mit der Schadsoftware auf das Jahr 2010 terminiert werden. Auch in diesem Fall ist davon auszugehen, dass die Schadsoftware nicht auf von dem Servicegerät angesteuerte programmierbare Leittechnik zugreifen konnte und abgesehen von der Verbreitung keine weiteren effektiven Einwirkungen stattfanden.

Potenzielle Auswirkungen

Servicegeräte dienen der Übertragung von Daten, z. B. Programm- bzw. Firmwareupdates oder neuen Programmierung, an die von ihnen bedienten IT-Systeme wie z. B. programmierbare Leittechniksysteme. Gleichzeitig werden solche Updates und Programmierungen in den meisten Fällen direkt vom Hersteller oder einem Zulieferer bezogen, also von außerhalb des IT-Sicherheitsraums. Damit bilden Servicegeräte oftmals die einzige Brücke vom über die Anlage hinausgehenden IT-Raum bis zu kritischen IT-Systemen der Anlage. Im Rahmen des „IT-Einwirkungsfalls“ kann die Beeinflussung der Servicegeräte somit schwerwiegende sicherheits- und sicherungstechnische Auswirkungen haben.

Wird auf das Servicegerät eingewirkt, jedoch nicht pfadübergreifend direkt auf andere IT-Systeme, bestehen weiterhin eine große Anzahl an möglichen sicherheits- und sicherungstechnisch relevanten Auswirkungen. Einwirkende können unter anderem:

- Eingaben und Daten des Servicegerätes auslesen. Kommt es zu regelmäßiger Übertragung von Daten an andere Systeme oder USB-Sticks, können diese Daten weitergesendet werden. Somit wird die Vertraulichkeit des Servicegerätes verletzt. Weiterhin können so vom Servicegerät ausgeführte Verbindungen und Datenübertragungen ausgelesen werden, was die Vertraulichkeit weiterer Systeme verletzt.
- Eingaben und Daten des Servicegerätes manipulieren. Hiermit wird die Integrität des Servicegerätes verletzt, Einwirkenden ist es möglich unerkannte oder erkennbare Manipulationen durchzuführen, welche von dem Servicegerät im Rahmen der Nutzung auch weitergegeben werden können. Z. B. bei Eingabe und Übersendung von Parametern für Steuerungssysteme. Die Integrität dieser Systeme wird somit ebenfalls verletzt.
- Das Servicegerät in einer Weise zu manipulieren, dass die Ausführung der Funktionalitäten des Servicegerätes auf erkennbare oder nicht erkennbare Weise unterbleibt, wodurch die Verfügbarkeit verletzt wird.

Die Manipulation von Servicegeräten ermöglicht somit eine umfassende Einwirkung über das Gerät hinaus auf sicherheits- und sicherungsrelevante IT-Systeme. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Vom IT-Einwirkungspfad „Servicegeräte“ ausgehend, können bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade entspringen und damit pfadübergreifende Auswirkungen erreichen. Primär werden Servicegeräte zur Unterstützung von IT-Systemen angewendet, welche selbst keine direkte Interaktionsmöglichkeit für Programmierungen, Parametrisierungen und Aktualisierungen bieten. Sie sind damit ein entscheidender Übergang für die Einwirkung auf solche Systeme und können somit unter anderem einleitend für folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „Wechseldatenträger“: Servicegeräte werden, wenn sie für Updates genutzt werden, potenziell mit Wechseldatenträgern verbunden. Werden hierbei keine Vorkehrungen getroffen, kann sowohl der IT-Einwirkungspfad „Servicegeräte“ durch den IT-Einwirkungspfad „Wechseldatenträger“ ausgelöst werden, also auch umgekehrt das Servicegerät zur Weiterverbreitung des IT-Einwirkungspfades „Wechseldatenträger“ führen, wenn mehrere Wechseldatenträger verwendet werden.

- IT-Einwirkungspfad „Netzwerkverbindung“: Wird ein Servicegerät mit einem IT-System mit datentechnischen bzw. Netzwerkverbindungen zu weiteren Komponenten oder IT-Systemen verbunden, können über diese Verbindung weitere Angriffsschritte durchgeführt werden.

- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Werden Servicegeräte mit IT-Systemen verbunden, kann es unter Umständen und bei entsprechender Manipulation zur Überlastung bestimmter Teile oder des Gesamtsystems kommen.

Weitere Auswirkung über den IT-Einwirkungspfad „Servicegeräte“ existieren immer in dem Fall, dass sicherheits- und sicherungsrelevante IT-Systeme mit Servicegeräten direkt bedient oder indirekt (temporäre) Datenübertragungen stattfinden.

4.2.2.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Servicegeräte“ verschiedene theoretische Einleitungen und kann weiterhin zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen Interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung ein.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche die potenziellen Auswirkungen des IT-Einwirkungspfades „Servicegeräte“ reduzieren. Hierbei wird von einer erfolgreichen Einwirkung bis zum Servicegerät ausgegangen. Mitigierend wirken insbesondere Faktoren der Reduzierung der datentechnischen Verbindungen. Dies können administrative Regelungen zur Nutzung, ein auf Sicherheit- und Sicherung ausgerichtetes Updatemanagement sowie die Erhöhung der Anzahl der Servicegeräte und damit die Reduzierung der Kontakte pro Servicegerät sein.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die sofortige Beendigung eines IT-Einwirkungspfades. Für Servicegeräte stehen hierbei verschiedene Verfahren der Überwachung und regelmäßigen Untersuchungen zur Verfügung: Virenscans, Datenabgleiche, Eingabeprotokolle, Zugriffsdokumentation, Datenverkehrsüberwachung, Dummysystemtests. Wird eine Einwirkung entdeckt, wird der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen.

Unterbrechende Faktoren

Abseits der Pfadunterbrechungen nach Aufdeckung bestehen verschiedene Möglichkeiten IT-Einwirkungspfade bei Systemübergang zu unterbrechen. Der IT-Einwirkungspfad besitzt insgesamt drei grundverschiedene Systemübergange: Von einem anderen IT-System, einem Wechseldatenträger oder von einem Einwirkenden auf das Servicegerät, von einem Servicegerät auf einen Wechseldatenträger oder ein anderes Servicegerät oder von einem Servicegerät auf das von dem Servicegerät bediente IT-System. Hierbei bieten sowohl administrative Regelungen zum Umgang mit diesen Systemen, Zugriffskontrollen, Unterbringungsschutz und datentechnische Untersuchungen vor und während Datenübertragungen die Möglichkeit Einwirkungen zu unterbrechen, bevor sie den IT-Einwirkungspfad „Servicegeräte“ einleiten können oder aber von Servicegeräten ausgehend weitere Einwirkungen ermöglichen.

4.2.2.4 Pfadzusammenfassung Servicegeräte

Der IT-Einwirkungspfad „Servicegeräte“ ist unter den beschriebenen Gesichtspunkten als schwerwiegender Einwirkungspfad mit zentralen Einwirkungsmöglichkeiten anzusehen. Der IT-Einwirkungspfad „Servicegeräte“ kann auf verschiedenste Weise eingeleitet werden, da Servicegeräte auf direkte Eingaben sowie Datenübertragungen, welche zum Teil aus anlagenfremden Quellen bezogen werden, angewiesen sind. Gleichzeitig bieten Servicegeräte in Teilen die einzigen direkten datentechnischen Übertragungen zu einigen sicherheits- und sicherungsrelevanten IT-Systemen an. Die hierdurch ermöglichten Auswirkungen des Einwirkungspfades sind daher potenziell schwerwiegend. Die Verhinderung solcher IT-Einwirkungen bzw. deren Auswirkungen sind, zusätzlich stark davon abhängig, dass entsprechende Richtlinien zu Zugriffen, Datenübertragungen und Servicegerätemanagement in einer solchen Form eingehalten werden.

4.2.3 Unerkannte IT-Komponenten

Mit fortschreitender Digitalisierung werden mehr und mehr alltägliche Anwendungen zum Teil unerkannt digitalisiert. Aufgrund der fortschreitenden Optimierung der Produktionssysteme und der daraus resultierenden Kostenreduzierung von digitalen Komponenten, werden diese oftmals auch in Systemen eingesetzt, welche zuvor analog gesteuert wurden und bei denen Käufer weiterhin eine analoge Steuerung erwarten. Diese Problematik betrifft nicht nur Systeme von Konsumenten, sondern auch industrielle gesteuerte Systeme. Ein bekanntgewordener Fall ist das IRS-Ereignis 8576, welches beschreibt, wie in einer kerntechnischen Anlage verschiedene Relais aufgefallen sind, welche entgegen der Qualifizierung doch digitale Komponenten beinhalteten. Hierdurch war die Qualifizierung erloschen und es wurden somit vor der Entdeckung nicht qualifizierte Relais in der Anlage eingesetzt. Da solche IT-Komponenten bereits bei der Herstellung in die betroffenen Systeme integriert wurden, besteht beim IT-Einwirkungspfad „Unerkannte IT-Komponenten“ eine Einwirkungsmöglichkeit von außerhalb der Anlage direkt auf steuernde Systeme zuzugreifen.

4.2.3.1 Der Einwirkungspfad „Unerkannte IT-Komponenten“

Beim IT-Einwirkungspfad „Unerkannte IT-Komponenten“ kommt es zum aktiven Einsatz von Systemen, welche als nicht IT-technisch qualifiziert wurden, jedoch entgegen den Angaben des Herstellers und der Erkennung während der Qualifizierung IT-technische Bausteine bzw. Komponenten beinhalten.

Solche unerkannten IT-Komponenten sind z. B. programmierbare Bausteine, welche anstatt einer analogen Steuerungselektronik die Steuerung des Systems übernehmen. Eine derartige unerkannte Integration von IT-technischen Bausteinen bzw. Komponenten kann z. B. daher entstehen, dass aufgrund von Kostenersparnissen Baulinien vereinheitlicht werden, dies jedoch dem Verkaufs- oder Dokumentationsteam (bzw. deren Übersetzung) nicht mitgeteilt wird. Es kommt auch vor, dass Händler nicht ausreichend von den Produktänderungen bzw. Überarbeitungen informiert wurden. Wenn schließlich die fehlerhafte Beschreibung im Rahmen des Erwerbs, der Qualifizierung und des Einbaus innerhalb der kerntechnischen Anlage nicht auffällt, kann dies im Rahmen des IT-Einwirkungspfades „Unerkannte IT-Komponenten“ unter Umständen genutzt werden.

Pfadeinleitung

Der Einwirkungspfad „Unerkannte IT-Komponenten“ beginnt bereits außerhalb der kerntechnischen Anlagen ab dem Zeitpunkt, ab dem IT-technische Komponenten in ein System eingebaut werden, welches nicht IT-technisch qualifiziert ist und dennoch eingesetzt wird. Ein solcher Einbau wird z. B. im Rahmen von Modellreihenvereinheitlichung, Modellaktualisierung oder aber grundsätzlich qua Design durchgeführt. Wird dieser Einbau nicht entsprechend kommuniziert, sei es mit potenziellen Käufern über die Designdokumente oder den Verkäufern und Zwischenhändlern, bleibt ein solcher Einbau potenziell unerkannt. Bestehen keine offensichtlichen IT-technischen Verbindungen wie LAN- oder USB-Anschlüsse und unterbleibt aufgrund der Modellreihenerfahrung oder aber der Zertifizierung des Herstellers eine ausreichende Qualifizierung, bleiben die IT-Komponenten potenziell unentdeckt.

Produktänderungen sind z. B. im Rahmen der ISO 9001 mit allen Kunden zu kommunizieren, wodurch im Beschaffungs- und Qualifizierungsverfahren solcher zertifizierter Anbieter ein Grundvertrauen angesetzt wird. Wird dennoch die Kommunikation unterlassen, wie im Beispiel der IRS-Meldung 8576, erhöht sich die Gefahr der Integration von Systemen mit unerkannten IT-Komponenten.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Notwendig zur Einleitung des Einwirkungspfades „unerkannte IT-Komponenten“ ist der aktive Einbau von IT-Komponenten in als nicht IT-technisch deklarierte Systeme vor der Inbesitznahme solcher Systeme durch die anwendende kerntechnische Anlage.

Ein solcher Einbau ist aus Gründen der Kosteneffizienz, der Zuliefererumstände oder der Baureihenmodernisierung z. B. für den Hersteller gegeben. Bisher nicht beobachtet, jedoch möglich, ist auch der klandestine Einbau von IT-technischen Komponenten in Systeme, welche als nicht IT-technisch ausgelegt sind.

Nach dem Einbau ist eine Nichterkennung der IT-technischen Komponenten in den betroffenen Systemen notwendig um den IT-Einwirkungspfad „unerkannte IT-Komponenten“ auszulösen.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Die Nichterkennung der IT-technischen Komponenten wird insbesondere aufgrund mangelhafter Kommunikation unterstützt. Werden Änderungen am Design von Systemen vorgenommen und somit IT-technische Komponenten in diese Systeme eingebaut, ist z. B. nach ISO 9001 eine Mitteilung an die Kunden notwendig. Wird dies unterlassen, wird im Rahmen der Qualifizierung durch die kerntechnischen Anlagen fälschlicherweise eine Baugleichheit angenommen. Eine mögliche Erkennung der IT-technischen Komponenten findet dann nicht mehr statt. Dasselbe gilt für aktualisierte Datenblätter, Nutzerbedienanleitungen und Informationen an die Verkäufer. Wird über die IT-technischen Komponenten nicht informiert und sind diese auch nicht durch z. B. typische Datenschnittstellen wie LAN oder USB erkennbar, wird die Annahme der nicht IT-technischen Systemeigenschaft erleichtert.

Weiterhin sind Prozesse zur Beschaffung und Qualifizierung der kerntechnischen Anlagen unterstützend für den IT-Einwirkungspfad „unerkannte IT-Komponenten“. Je oberflächlicher, je weniger spezifisch und basierend auf blindem Vertrauen ein solcher Prozess aufgebaut wird, desto höher ist die Wahrscheinlichkeit, dass nicht angegebene IT-technische Komponenten in als nicht IT-technisch deklarierten Systemen verborgen bleiben.

Pfadzwischenschritte

Wird der Qualifizierungsprozess durch die kerntechnische Anlage abgeschlossen, kann es ab diesem Punkt zu einem Einsatz der betroffenen Systeme mit unentdeckten IT-technischen Komponenten kommen. Einmal beschafft und qualifiziert, können die betroffenen Systemen überall dort installiert werden, wo sie gebraucht werden.

Werden die betroffenen Systeme als Ersatzsysteme für aktuell im Betrieb befindliche Systeme verwendet, kann sich der Installationszyklus und damit der Einwirkungspfad über einen langen Zeitraum strecken. Es kann im Rahmen des aktiven IT-Einwirkungspfades „unerkannte IT-Komponenten“ somit zu einer über die Zeit immer weitergehenden Verbreitung der Systeme kommen. Wurden die Systeme nicht nur für eine einzelne kerntechnische Anlage qualifiziert, sondern für einen Betreiber mehrerer kerntechnischer Anlagen, können die betroffenen Systeme anlagenübergreifend verbreitet werden.

Pfadende und Pfadübergänge

Da die betroffenen Systeme mit unerkannten IT-technischen Komponenten eben nicht als IT-Systeme betrachtet und installiert werden, ist durchgehend davon auszugehen, dass diese Systeme entsprechend datentechnischen Schnittstellen noch bei der Installation in irgendeiner Form datentechnisch mit anderen IT-Systemen verbunden werden. Auch von temporären Anschlüssen ist nicht auszugehen, andernfalls wäre eine sofortige Erkennung der IT-technischen Komponenten der Systeme zwingend anzunehmen. Der IT-Einwirkungspfad „unerkannte IT-Komponenten“ endet somit im Anschluss des Einbaues der betroffenen Systeme und es kommt zu keinen weiteren, pfadübergreifenden Verknüpfungen mit anderen IT-Einwirkungspfaden.

4.2.3.2 Pfadauswirkungen

Die Auswirkungen des IT-Einwirkungspfades „unerkannte IT-Komponenten“ sind aufgrund der erwartbar nicht vorhandenen datentechnischen Verbindungen ausschließlich abhängig vom Einsatzgebiet der betroffenen Systeme. Mit dem IRS-Ereignis 8576 ist bisher ein umfassendes Ereignis entdeckt wurden, in welchem mehrere Relais in zwei verschiedenen kerntechnischen Anlagen entdeckt wurden, welche entgegen der Qualifizierung IT-technische Komponenten beinhalteten.

Real beobachtete Auswirkungen

In den analysierten Ereignissen ist kein Fall bekannt geworden, bei welchem eine absichtlich herbeigeführte Einflussnahme auf bzw. mittels Systemen mit unentdeckten IT-Komponenten durchgeführt wurde.

Demgegenüber steht das IRS-Ereignis 8576, bei welchem solche Systeme mit unerkannten IT-Systemen mehrfach in den kerntechnischen Anlagen des gleichen Betreibers verbaut wurden. Zwischen der ersten Entdeckung und dem vermutlich erstmaligen Einbau vergingen insgesamt 5 Jahre, in welchen die IT-Komponenten in den betroffenen Systemen unentdeckt blieben; in einem Fall waren es sogar 7 Jahre.

Hierbei wurde der erstmalige Fall im Rahmen der Qualifizierung eines neues Relais entdeckt. Der Betreiber erwarb neue Relais des gleichen Herstellers wie die bisher eingebauten Relais für die Spannungsüberwachung eines sicherheitsrelevanten Systems und führte einen Qualifizierungsprozess aus. Im Rahmen dieses Prozesses ist aufgefallen, dass sowohl das neu erworbene Relais als auch das seit 5 Jahren eingesetzte Relais des Herstellers, programmierbare Bausteine beinhalteten. Die beiden Relais waren somit IT-Systeme und daher nicht qualifizierbar, die Anforderungen für den Einsatz für die Spannungsüberwachung eines sicherheitsrelevanten Systems sahen den Einsatz von nicht IT-technischen Systemen vor.

In Folge des Ereignisses führte der Betreiber ein Programm zur Entdeckung von programmierbaren Komponenten in als nicht IT-technisch deklarierten Systemen durch. Hierbei sind insgesamt drei weitere Vorfälle entdeckt worden, bei welchen Relais entgegen der Qualifizierung und Deklaration mit programmierbaren Komponenten ausgestattet waren. Zum einen wurden defekte Relais eines Notstromdiesels ausgetauscht, wobei beim Einbau der Ersatzrelais dann die IT-technischen Komponenten aufgedeckt wurden, es kam also zu keinem Einsatz. Weiterhin wurden zwei Relais in einem System der Sicherheitsklasse 3 identifiziert, welche programmierbare Technik beinhalteten. Der namhafte Hersteller gab bei der Qualifizierung an, dass in den Relais keine IT-technischen Bausteine verwendet werden. Mit den Ergebnissen der Untersuchung konfrontiert, wurde eingeräumt, dass nach einer Überarbeitung nun doch programmierbare Bausteine in den Relais eingebaut werden. Schließlich wurden Relais in einem Gleichrichter gefunden, wobei man entdeckte, dass seit 7 Jahren ein typverwandtes, aber nicht das geplante Relais eingebaut wurden. Beide Relaistypen beinhalteten programmierbare Technik und verstießen damit gegen die Qualifizierungsannahmen.

Keines der genannten Relais führte zu einem Relaisausfall aufgrund der eingebauten unerkannten IT-Komponenten, es ist zu keiner erkennbaren Einwirkung über die IT-Komponenten gekommen. Es kam somit zu keiner tatsächlich Ausnutzung der unerkannten IT-Komponenten bzw. einer Einwirkung.

Potenzielle Auswirkungen

Potenziell können die Auswirkungen eine hohe sicherheits- bzw. sicherungstechnische Bedeutung erreichen. Werden Systeme mit nicht erkannten IT-Komponenten in sicherheits- bzw. sicherungstechnischer Funktion eingebaut, wird aufgrund der falschen Annahmen kein IT-Sicherheitskonzept oder anderweitige IT-technische Regelungen auf das betroffene System angewendet. Somit werden z. B. keine Integritätsprüfungen durchgeführt, die eingesetzte Software wird nicht auf ihre Eigenschaften wie Stabilität untersucht. Wird an das System aufgrund der sicherheits- bzw. sicherungstechnischen Bedeutung eine gewisse nachgewiesene Ausfallwahrscheinlichkeit vorgeschrieben, kann diese bei unerkannten IT-Komponenten nicht vollständig geprüft werden, da keine spezifischen Untersuchungen der eingebauten Soft- bzw. Firmware möglich ist. Weiterhin ist denkbar, dass Einwirkende direkte Manipulation der eingesetzten Soft- bzw. Firmware durchführen und diese aufgrund der Unkenntnis der eingesetzten IT-Komponenten nicht entdeckt werden. Da jedoch keine datentechnischen Verbindungen anzunehmen sind, ist keine direkte (Fern)-Steuerung der betroffenen Systeme anzunehmen. Einwirkende können dann:

- Die eingesetzte Soft- bzw. Firmware in einer solchen Weise manipulieren, dass die Betriebsfunktionen unerkannt oder erkannt nicht mehr ausgeführt werden können, wodurch die Verfügbarkeit verletzt wird.
- Die eingesetzte Soft- bzw. Firmware in einer solchen Weise manipulieren, dass die Systeme erkennbar oder unerkennbar Funktionen ausführen, die nicht erwartet werden. In Folge können z. B. die aufgezeichneten Daten verfälscht werden oder manipulierend in die Betriebsfunktionen eingegriffen wird, wodurch die Integrität verletzt wird.

Somit sind bei Anwendung des IT-Einwirkungspfades „unerkannte IT-Komponenten“ erhebliche Einwirkungen auf die betroffenen Systeme denkbar. Die sich hieraus ergebende sicherheits- und sicherungstechnische Bedeutsamkeit kann schwerwiegende Ausmaße erreichen.

Pfadübergreifende Auswirkungen

Die vom IT-Einwirkungspfad „unerkannte IT-Komponenten“ betroffenen Systeme werden als nicht IT-technische Systeme qualifiziert und entsprechend installiert.

Bei einer solche Installation ist durchgehend davon auszugehen, dass keine datentechnischen Verbindungen aufgebaut werden. Eine solche Verbindung wäre ein so klares Indiz für verbaute IT-Komponenten, dass eine umgehende Intervention zu erwarten ist. Der Pfad „unerkannte IT-Komponenten“ hat nach bisherigem Stand keine direkten pfadübergreifenden Auswirkungen.

Es kann zu indirekten pfadübergreifenden Auswirkungen kommen, wenn die vom IT-Einwirkungspfad „unerkannte IT-Komponenten“ in einer solchen Weise funktionieren, dass sie weitere IT-Einwirkungen und deren Auswirkungen nicht entdeckten bzw. aufdecken.

4.2.3.3 Pfadblockierende Faktoren

Da der IT-Einwirkungspfad „unerkannte IT-Komponenten“ bereits außerhalb der betroffenen kerntechnischen Anlagen beginnt, sind entsprechende Maßnahmen zur Minimierung des Risikos bzw. zur Unterbrechung des Einwirkungspfades entsprechend darauf gerichtet, dass es zu keiner Integration betroffener Systeme in die Anlagen kommen kann.

Mitigierende Faktoren

Mitigierende Faktoren sind solche Faktoren, welche die potenziellen Auswirkungen des IT-Einwirkungspfades einschränken oder gänzlich aufheben. Im Falle des IT-Einwirkungspfades „unerkannte IT-Komponenten“ sind die mitigierenden Faktoren begrenzt, da der Einbau eines betroffenen Systems mit unerkannten IT-Komponenten bereits die Endstufe des Einwirkungspfades ist. Mitigierende Maßnahmen basieren somit auf einer strategisch günstigen Verbreitung von typidentischen Systemen, sodass im Falle von unentdeckten IT-Komponenten nicht mehrere Redundanzen oder mehrere Anlagenfunktionen gleichzeitig betroffen sind. Wird in der Beschaffung darauf geachtet, dass typidentische oder herstelleridentische Systeme nicht mehrfach in den gleichen sicherheits- bzw. sicherungsrelevanten Funktionen verwendet werden, werden die Auswirken des Einwirkungspfades „unerkannte IT-Komponenten“ potenziell reduziert.

Aufdeckende Faktoren

Der wichtigste blockierende Faktor des IT-Einwirkungspfades „unerkannte IT-Komponenten“ ist die Aufdeckung. Durch die Aufdeckung noch vor der Beschaffung bzw. dem Einbau wird der Einwirkungspfad vollständig unterbunden. Hierzu sind eine Reihe von Maßnahmen möglich:

- Umfassende Kommunikationsbeziehung mit dem Hersteller
- Umfassendere Kommunikation zwischen den kerntechnischen Anlagen, um die Ergebnisse von Qualifizierung und Produktwarnungen langfristig zu teilen
- Ein kritisches Beschaffungs- und Qualifizierungsverfahren, welches unabhängig von den Angaben des Herstellers bzw. Anbieters qualifizierende Maßnahmen durchführt.
- Ein verbreitetes Bewusstsein für die Problematik und damit eine einhergehende kritische Haltung auch gegenüber langjährig etablierten neu bezogenen Komponenten
- Ein Prüfsystem für im Betrieb befindliche, außer Betrieb genommene und in den Betrieb zu übernehmende Systeme.
- Ein Report- und Reaktionssystem für Auffälligkeiten.

Sobald ein von unerkannten IT-Komponenten betroffenes Systems erkannt wird, sei dies durch Zufall oder im Rahmen der Qualifizierungs- und Betriebsmaßnahmen oder nach Notifikation durch den Hersteller, muss eine entsprechende Reaktion ausgehend auf festgelegten Maßnahmen erfolgen. Der Einwirkungspfad wird dann durch die Aufdeckung und die ergriffenen Maßnahmen unterbrochen.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Unerkannte IT-Komponenten“ nimmt seinen Ausgangspunkt außerhalb betroffener kerntechnischer Einrichtungen. Gleichzeit kommt es zu keiner direkten Übertragung von einem betroffenen System auf ein nicht betroffenes System, eine datentechnische Kommunikation ist nicht anzunehmen. Der IT-Einwirkungspfad „Unerkannte IT-Komponenten“ wird somit nur dann unterbrochen, wenn eine Aufdeckung des IT-Einwirkungspfades stattfindet und darauf eine entsprechende anforderungsgemäße Reaktion veranlasst wird.

4.2.3.4 Pfadzusammenfassung unerkannte IT-Komponenten

Der IT-Einwirkungspfad „unerkannte IT-Komponenten“ ist unter den beschriebenen Gesichtspunkten ein mittelschwerer Einwirkungspfad. Aufgrund der nicht anzunehmenden datentechnischen Verbindungen führt eine einmalige Einwirkung über diesen Pfad nicht zu einer potenziellen weiteren Verbreitung. Die Einwirkung selbst auf das betroffene System kann als schwerwiegend angesehen werden, da Systeme betroffen sind, auf welche keine IT-Sicherheitskonzepte angewendet werden und welche eine hohe sicherheits- oder sicherungstechnische Bedeutung erreichen können. Die Aufdeckung des IT-Einwirkungspfades „unerkannte IT-Komponenten“ kann zusätzlich je nach Gerätebauart und dem Informationsfluss des Herstellers schwierig sein. Insgesamt ist daher die sicherheits- und sicherungstechnische Bedeutung des Einwirkungspfades nicht zu unterschätzen.

4.2.4 Überlastung von IT-Systemen

Eingesetzte IT-Systeme sind für die korrekte Ausführung ihrer Programmierung darauf angewiesen, dass die Hardware der IT-Systeme die dazu notwendigen Rechenoperationen in der vorhergesehen Zeit erfolgreich durchführt. Sind die maximalen Rechenoperationen der Hardware des IT-Systems je Zeiteinheit geringer als die für die Durchführung notwendigen Rechenoperationen je Zeiteinheit, verzögern sich die Ausgaben des IT-Systems. Bleibt dieser Zustand langfristig erhalten, verlangsamt sich das IT-System immer weiter und es kommt zu einer Denial-of-Service (DoS-) Bedingung, bei der aufgrund von Überlastung das IT-System seine Aufgaben nicht mehr erfüllt. Eine solche DoS-Bedingung kann sich auch im Rahmen von IT-Einwirkungen auslösen lassen, indem entweder spezifische Schwachstellen von Systemen ausgenutzt werden oder aber mit einer hohen Anzahl von Anfragen ein IT-System überlastet wird.

Im kerntechnischen Bereich werden IT-Systeme für eine Vielzahl von Aufgaben in unterschiedlichen Bereichen angewendet. Eine wichtige Aufgabe ist in modernen kerntechnischen Anlagen z. B. die konstante und dauerhafte Aufstellung auflaufender Daten und die Analyse und Weiterverarbeitung dieser für Zustandsdarstellungen. IT-Systeme werden jedoch auch zur Eingabe von Steuerbefehlen oder aber zur Steuerung von Anlagenfunktionen angewendet. Kommt es bei einem solchen IT-System zu einer DoS-Bedingung, steht dieses temporär nicht mehr zur Verfügung und die von dem IT-System bediente Anlagenfunktion kann unter Umständen nicht entsprechend ausgeführt werden.

Mit den IRS-Ereignissen 8485 und 8671 sind zwei Ereignisse bekannt geworden, bei welchen aufgrund von Überlastung der Hardware die digitalisierten Warten der betroffenen kerntechnischen Anlagen vorrübergehend nicht verfügbar waren. Die Ereignisse basieren nicht auf der IT-Einwirkung Dritter, sondern auf einem durchgeführten Wartungsprozess, der mit den darauffolgenden großen Datentransfers zu einer Überlastung eines zentralen Servers und damit dem Ausfall der Warten führte. Ein solcher überlastender Datenverkehr ist jedoch auch durch Einwirkungen Dritter herbeiführbar und somit der IT-Einwirkungspfad „Überlastungen von IT-Systemen“ aus diesen Ereignissen ableitbar.

4.2.4.1 Der Einwirkungspfad „Überlastung von IT-Systemen“

Wie beschrieben wird für die korrekte Ausführung von Aufgaben von IT-Systemen eine ausreichende Ausstattung im Bereich der Hardware benötigt. Im Falle des IT-Einwirkungspfades „Überlastung von IT-Systemen“ kommt es durch Einwirkungen zu einer Überlastung der Hardware. Um eine solche Überlastung induzieren zu können, sind grundsätzlich drei verschiedene Verfahrensweisen denkbar:

- Die Ausnutzung von Schwachstellen durch Schadsoftware oder manuelle Eingaben
- Die massenhafte Durchführung automatischer Anfragen über Netzwerkverbindungen
- Die lokale Eingabe von umfassenden überlastenden Anfragen

Neben direkten Einwirkungen sind somit insbesondere datentechnische Verbindungen, permanente und temporäre, dazu geeignet um den IT-Einwirkungspfad „Überlastung von IT-Systemen“ einzuleiten und auszuführen.

Pfadeinleitung

Der Einwirkungspfad „Überlastung von IT-Systemen“ kann auf die bereits genannten Arten eingeleitet werden. Neben der direkt auf das betroffene IT-System einwirkenden Einwirkung besteht somit auch eine Pfadeinleitung bei Einwirkung auf datentechnisch permanent oder temporär verknüpfte Systeme. Auch über Servicegeräte kann der Einwirkungspfad ausgelöst werden.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Notwendig für die Einleitung ist ein datentechnischer Wirkungsweg auf das betroffene IT-System. Unabhängig wie dieser ausgestaltet ist, ist hiermit eine Einwirkung in Form einer induzierten Überlastung möglich. Zu den datentechnischen Verbindungen zählen:

- Dauerhafte datentechnische Kommunikation mit IT-Systemen
- Temporäre datentechnische Kommunikation mit IT-Systemen über Netzwerke
- Temporäre datentechnische Kommunikation mit IT-Systemen über Wechseldatenträger
- Datentechnische Einwirkung über Permanentdatenträger
- Datentechnische Einwirkung über Servicegeräte
- Direkte Einwirkung über Eingabebefehle

Mit jedem der genannten Punkte besteht die Möglichkeit der Einleitung des IT-Einwirkungspfades. Dabei kann die Einwirkung über Schwachstellen ausnutzende Schadsoftware, massenweise legitime datentechnische Anfragen oder spezifische überlastende datentechnische Anfragen stattfinden.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Jeder einzelne genannte Aspekt reicht aus zur Einleitung des Einwirkungspfades. Mit jedem weiteren Aspekt erhöht sich die Möglichkeit der Einwirkung. Weiterhin werden diese Einleitungsvorgänge durch verschiedene unterstützende Bedingungen erleichtert oder in ihrer Effektivität gesteigert:

- Dauerhafte datentechnische Kommunikation mit IT-Systemen:
  Besteht eine solche Kommunikation, können massenhaft legitime Anfragen über diese an das verbundene IT-System verschickt werden und somit das betroffene System überlastet werden. Eine solche Massenversendung wird insbesondere dann ermöglicht, wenn keine Netzwerküberwachung besteht, welche ein Massenversenden blockiert oder auf ein für das betroffene IT-System akzeptables Maß reguliert wird.
  Je mehr IT-Systeme permanent datentechnisch verbunden sind, desto höher sind die Möglichkeiten der Einwirkung und auch der Wahrscheinlichkeit der unabsichtlichen Überlastung von Hardware

- Temporäre datentechnische Kommunikation mit IT-Systemen über Netzwerke:
  Temporäre datentechnische Kommunikation zwischen IT-Systemen kann auf gleiche Weise genutzt werden wie permanente Kommunikation. Die Auslösung des IT-Einwirkungspfads „Überlastung von IT-Systemen“ kann dadurch erleichtert werden, dass keine Kontrollmechanismen verwendet werden und keine automatische Trennung der Verbindung zulässig ist.

- Temporäre datentechnische Kommunikation mit IT-Systemen über Wechseldatenträger:
  Wechseldatenträger können der Übertragung von Schadcode auf IT-Systeme Vorschub leisten. Solcher Schadcode kann dann die Anforderungen an die Hardware drastisch erhöhen und diese damit überlasten. Die Einwirkung wird erleichtert, wenn Protokolle und Handlungsweisungen zur Vermeidung solcher Einwirkung nicht eingehalten werden. Dies wird im IT-Einwirkungspfad „Datenträger“ dargelegt.

- Datentechnische Einwirkung über Permanentdatenträger:
  Permanente Datenträger können, wie Wechseldatenträger, der Übertragung von Schadcode Vorschub leisten. Dies wird im IT-Einwirkungspfad „Datenträger“ dargelegt.

- Datentechnische Einwirkung über Servicegeräte:
  Der IT-Einwirkungspfad „Servicegeräte“ erläutert die Bedingungen zur Einleitung einer Einwirkung mittels Servicegeräten.

- Direkte Einwirkung über Eingabebefehle:
  Direkte Steuerungsbefehle können ebenfalls eingesetzte Hardware von IT-Systemen überlasten. Bestehen keine Protokolle und Verfahrensweisen zur Benutzung von IT-Systemen, vergrößern sich potenziell die direkten Einwirkungsmöglichkeiten. Bei nicht optimierter Software vergrößert sich das Potenzial solcher Einwirkungen.

Die Auslösung der Überlastung eines IT-Systems ist zusätzlich teilweise von der eingesetzten Hardware abhängig. Besitzt diese Hardware eine große Leistungsreserve gegenüber ihren alltäglichen Aufgaben, können durch Dritte ausgelöste oder im Betrieb ausgelöste Belastungsspitzen möglicherweise ohne Überlastung verarbeitet werden. Demgegenüber stehen knappe Leistungsreserven, die womöglich bereits durch ein hohes Aufkommen legitimer betrieblich anfallender Bearbeitungsdaten überlastet werden.

Pfadzwischenschritte

Wird ein IT-System vom IT-Einwirkungspfad „Überlastung von IT-Systemen“ betroffen, sind die davon weiter gehenden Einwirkungsschritte von der Vernetzung des betroffenen IT-Systems abhängig. Bei keiner bestehenden Vernetzung führt eine Überlastung zu einer Verlangsamung und gegebenenfalls zu einem Ausfall des IT-Systems, jedoch wird davon kein weiteres IT-System betroffen. Der IT-Einwirkungspfad endet an dieser Stelle. Bestehen direkte datentechnische Verbindungen eines betroffenen IT-Systems, kann es zur Betroffenheit weiterer IT-Systeme kommen, z. B. wenn diese IT-Systeme von Daten des ursprünglichen IT-Systems abhängig sind. Besteht ein ausgedehntes IT-Netz und der IT-Einwirkungspfad „Überlastung von IT-Systemen“ betrifft zentrale Servereinheiten des Netzes, können alle IT-Systeme des Netzwerkes betroffen sein und nicht mehr ordnungsgemäß arbeiten. So geschehen bei den IRS-Ereignissen 8485 und 8671, bei welchen jeweils ein zentraler Server einer digitalen Warte überlastet wurde und die Funktion der gesamten digitalen Warte temporär nicht verfügbar war.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Überlastung von IT-Systemen“ endet zum einen mit dem Ende der Überlastung, welche wiederum auf verschiedene Arten und Weisen beendet wird. Bei Überlastung durch Anfragen aus einem IT-Netzwerk heraus kann eine temporäre Unterbrechung des Netzwerkverkehres oder Abkopplung des Anfragenstellers die Einwirkung beenden. Überlastungen durch Schadcode sind zumeist erst mit einer vollständigen Bereinigung der betroffenen IT-Systeme zu beenden, sie können auch nach temporärer Beendigung der Überlastung unvermittelt wieder auftreten. Überlastung von IT-Systemen durch überlastende manuelle Befehlseingaben können durch Aufhebungsbefehle, ein finales Abarbeiten der Befehlsketten oder aber einen Systemneustart beendet werden.

Die Pfadübergänge zu weiteren IT-Einwirkungspfaden sind abhängig von den bestehenden datentechnischen Verbindungen und der Art, wie die Einwirkung stattfand. Es kann zu Interaktionen mit den IT-Einwirkungspfaden „Servicegeräte“, „Wechseldatenträger“ und weiteren kommen.

4.2.4.2 Pfadauswirkungen

Die Pfadauswirkungen des IT-Einwirkungspfades „Überlastung von IT-Systemen“ sind insbesondere davon abhängig, wie und in welcher Intensität die Überlastung stattfindet. Weiter ist zu betrachten, ob und *welche* weiteren IT-Systeme und Anlagenfunktionen von den betroffenen IT-Systemen abhängig sind.

Real beobachtete Auswirkungen

Bisher sind zwei bekannte Fälle von überlasteten IT-Systemen über das internationale Meldungswesen der IRS bekannt geworden, die Ereignisse 8485 und 8671. In beiden Fällen kam es zu einer deutlichen Überlastung eines zentralen IT-Systems der digitalen Leitwarte der betroffenen kerntechnischen Anlage. Aufgrund von Wartungsarbeiten kam es dabei im Netzwerk der digitalen Warte in beiden Fällen zu einer sehr hohen Leistungsanfrage an den zentralen Server, welche diesen überlastete. Dadurch stockten sämtliche Terminals der Warte und die Warte wurde für ca. 1 Stunde für nicht verfügbar erklärt, die Ersatzwarte wurde in der Zwischenzeit in Betrieb genommen. Die betroffenen Server setzten jeweils relativ alte Hardware ein und waren außerhalb des Ereignisses dauerhaft mit bereits 70 % der Rechenkapazität ausgelastet. In Folge der ungeplanten Leistungsanfrage in Folge der Wartungsarbeiten stieg die Auslastung deutlich über 100 %, wodurch die für den Wartenbetrieb notwendigen Prozesse nicht wie vorhergesehen ausgeführt wurden. Es handelte sich hierbei nicht um eine von Dritten ausgeführte IT-Einwirkung auf die IT-Systeme.

Potenzielle Auswirkungen

Potenziell können über den IT-Einwirkungspfad „Überlastung von IT-Systemen“ einzelne IT-Systeme, IT-Netzwerke und die von diesen ausgeführten Anlagenfunktionen in ihrer Verfügbarkeit beeinträchtigt oder gänzlich unterbrochen werden. Auch aufgrund der verschiedenen Anfangsmöglichkeiten des IT-Einwirkungspfades kann potenziell jedes IT-System, auf welches zugegriffen oder datentechnisch kommuniziert wird, von dem IT-Einwirkungspfad betroffen sein. Insbesondere sind jedoch größere Netzwerk- und Verbundsysteme bedroht, da hier eine große Menge an Daten verkehrt und datentechnische Verbindungen zu vielen weiteren IT-Systemen vorhanden sind. Die Auswirkungen solcher Netzwerkausfälle sind als schwerwiegend anzusehen, wenn die Netzwerke sicherheits- und sicherungsrelevante Aufgaben ausführen.
In den meisten Fällen kann die Einwirkung nach Aufdeckung wieder gestoppt werden.

So können bestimmte Netzwerkanfragen innerhalb von IT-Netzen unterbunden werden, Anfragen mit hohem Rechnerressourcenverbrauch können unterbrochen oder abgebrochen werden und IT-Systeme, welche aufgrund der Auslastung in ihrer Funktion gestört sind, können neu gestartet werden.

Wird der IT-Einwirkungspfad „Überlastung von IT-Systemen“ nicht durch massenhafte Netzwerkanfragen oder direkte Eingaben ausgelöst, sondern mittels Schadsoftware auf dem betroffenen IT-System ausgeführt, besteht eine hohe Wahrscheinlichkeit weiterer Einflussnahme von Schadsoftware. Hierzu zählt die Verletzung der Integrität und Vertraulichkeit der Systeme wie auch potenzielle Weiterverbreitung der Schadsoftware auf weitere IT-Systeme. Die potenziellen Auswirkungen solcher Schadsoftware wird insbesondere im IT-Einwirkungspfad „Wechseldatenträger“ dargelegt.

Pfadübergreifende Auswirkungen

Zu pfadübergreifenden Auswirkungen kommt es in dem Fall, dass entweder die Einwirkungsursache sich weiterverbreiten kann oder aber, dass durch die Überlastung der IT-Systeme potenziell weitere Einwirkungen möglich sind. Insbesondere Einwirkungsursachen über Zwischenträger wie Servicegeräte oder Wechseldatenträger haben somit potenziell übergreifende Auswirkungen auf die entsprechenden Einwirkungspfade. Kommt es zu Einzeleinwirkungen z. B. über direkte Eingaben, ist ein Übergreifen als unwahrscheinlich anzunehmen. Werden IT-Systeme überlastet, kann IT-Einwirkungen Vorschub geleistet werden. Dies gilt insbesondere für IT-Systeme mit Sicherungsfunktionen. Sind solche IT-Systeme temporär nicht einsatzbereit, können weitere IT-Einwirkungen über verschiede IT-Einwirkungspfade potenziell unentdeckt bleiben. Der IT-Einwirkungspfad „Überlastung von IT-Systemen“ kann somit je nach betroffenem IT-System als vorhergehender Einwirkungspfad dienen und weitere Einwirkungspfade erleichtern bzw. deren Aufdeckung erschweren.

4.2.4.3 Pfadblockierende Faktoren

IT-Einwirkungen, welche zur Überlastung von IT-Systemen führen, können auf verschiedenste Weise unterbunden werden. Hierzu zählen Möglichkeiten zur Mitigation der Auswirkungen eines solchen IT-Einwirkungspfades ebenso wie aufdeckende Faktoren und schließlich automatische und manuelle Möglichkeiten der Pfadunterbrechung.

Mitigierende Faktoren

Kommt es zu einer Überlastung eines IT-Systems in Folge von IT-Einwirkungen oder einem Betriebsereignis, kann dies zur Einschränkung oder dem vollständigen Ausfall der von dem IT-System ausgeführten Anlagenfunktion führen. In den Beispielen der IRS-Ereignisse 8485 und 8671 kam es zu einem zeitweiligen vollständigen Ausfall der digitalen Warte der kerntechnischen Anlagen. Mitigierend für den Effekt der Ereignisse standen jedoch die Ersatzwarten einsatzbereit zur Verfügung und wurden überbrückend genutzt. Entsprechend der Ereignisse können alternative oder redundante IT-Systeme mitigierend auf die Auswirkungen der überlasteten Hardware wirken. Insbesondere in IT-Netzwerken kann somit verhindert werden, dass der Ausfall eines Systems auf mehr Systeme überspringt.

Mitigierend wirkt neben der Bereithaltung von redundanten Systemen auch eine Netzwerkeinschränkung, sodass eine solche Einwirkung sich nicht weiterverbreiten kann oder jedes im Netzwerk befindliche System durch nicht vorgesehene Anfragen überlastet wird.

Über die Konfiguration und die Aktualität von IT-Systemen können IT-Einwirkungen auf die Auslastung von IT-Systemen eingeschränkt oder gänzlich gestoppt werden. Befehlsmöglichkeiten, welche zu einer DoS-Bedingung führen können, sind als Softwareschwachstellen angesehen und werden in der Regel nach Aufdeckung durch die Hersteller mittels Updates eingeschränkt. Spezifische Konfigurationen von Netzwerken und IT-Systemen unterbinden in Teilen oder vollständig massenhafte oder fehlerhafte Anfragen, welche zu DoS-Bedingungen führen können.

Aufdeckende Faktoren

IT-Einwirkungen zur Herbeiführung der Überlastung von IT-Systemen fallen auf, sobald die Auswirkungen der Überlastungen von Anlagenpersonal wahrgenommen werden. Frühzeitige Aufdeckung des IT-Einwirkungspfades „Überlastung von IT-Systemen“ ist zum einen im Rahmen der vorhergehenden IT-Einwirkungspfade wie „Servicegeräte“ oder „Wechseldatenträger“ möglich, zum anderen aber auch mit Überwachungsfunktionen. So können bestehende IT-Netzwerke insbesondere auf ihren Netzwerkverkehr überwacht werden und Auffälligkeiten in Folge massenhafter Anfragen entdeckt werden.

Auch die Hardwareauslastung von IT-Systemen kann überwacht werden, sodass betrieblich bedingte, aus Betriebsereignissen entstehende oder durch Einwirkungen induzierte Belastungsspitzen erkannt werden können und Gegenmaßnahmen ergriffen werden können.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Überlastung von IT-Systemen“ wird immer dann unterbrochen, wenn die Überlastung eines oder die Überlastung mehrerer Systeme gestoppt wird. Dies geschieht in der Regel nach Erkennung der Überlastung durch automatische oder manuelle Systeme. So kann eine Netzwerküberwachung genutzt werden, um automatisch Massenanfragen zu stoppen, welche zu einer Überlastung führen können. Auch auf den IT-Systemen kann z. B. durch Priorisierung von Systemprozessen verhindert werden, dass bestimmte Anfragen zu einer Überlastung führen. Manuell können überlastende Prozesse in manchen Fällen gestoppt werden oder mittels Systemneustarts die Funktionsfähigkeit der IT-Systeme wiederhergestellt werden.

4.2.4.4 Pfadzusammenfassung Überlastung von IT-Systemen

Der IT-Einwirkungspfad „Überlastung von IT-Systemen“ kann durch unterschiedlichste initiale Einwirkungen, unter anderem verschiedene weitere IT-Einwirkungspfade wie „Servicegeräte“ oder „Wechseldatenträger“ ausgelöst werden. Sind Einwirkungen über diesen Pfad erfolgreich, kann ein betroffenes IT-System seine Aufgaben mit den bestehenden Rechnerressourcen nicht mehr vollständig ausführen und verlangsamt sich; stellt den Dienst im Rahmen einer DoS-Bedingung ein oder bricht vollständig zusammen. Der IT-Einwirkungspfad „Überlastung von IT-Systemen“ hat somit insbesondere aufgrund der hohen Anzahl an möglichen Auslösern und der potenziell netzwerkeumfassenden Auswirkungen, eine sicherheits- und sicherungstechnische Bedeutung.

4.2.5 Lieferkette

Im Rahmen der Digitalisierung und Internationalisierung von Produkten und deren Lieferketten haben die Aspekte der IT-Sicherheit in diesem Bereich in den vergangenen Jahren einen erheblichen Bedeutungszuwachs erfahren. Aufgrund der zunehmenden Verwendung komplexer, digitaler Systeme sind Unternehmen, Anlagen und Organisationen oftmals auf die Bereitstellung von Produkten, Daten und Programmen wie zum Beispiel hoch-spezialisierte Hard- oder Softwaresysteme durch externe Zulieferer angewiesen, die in der Regel nicht oder nicht vollständig selbst auf ihre Integrität geprüft werden können. Der sichere Umgang mit den eigenen IT-Systemen und deren Schutz ist angesichts der stetig wachsenden Komplexität, Digitalisierung und Vernetzung der (IT-)Systeme für viele Unternehmen, Anlagen und Organisationen eine große Herausforderung.

Bei den Angriffen mit der Schadsoftware „NotPetya“ im Jahr 2017, welche weltweit große Beachtung fanden und global große finanzielle Schäden verursachten sowie gleichermaßen bei dem Vorfall der Schadsoftware „Stuxnet“ vor über 10 Jahren, bei welchem auch kerntechnische Anlagen betroffen waren, sind IT-Angriffe über die Lieferkette beobachtet worden. Zudem ist mit dem meldepflichtigen Ereignis 2016/025 im Kernkraftwerk Biblis bereits ein deutsches Kernkraftwerk von der Lieferkettenproblematik betroffen gewesen. Dabei wurde auf Rechnern der Anlagensicherung Schadsoftware gefunden, die sich mutmaßlich bereits bei der Installation der Systeme in der Anlage auf den betroffenen Komponenten befand. Neben diesen beispielhaften Vorfällen nahm die Anzahl von Lieferkettenangriffen national und international, darunter mehrere mit Bezug zu kerntechnischen Anlagen und Einrichtungen sowie Organisationen und Einrichtungen der kritischen Infrastruktur, in den letzten zehn Jahren beständig zu und beschäftigt daher Unternehmen und Aufsichtsbehörden.

4.2.5.1 Der Einwirkungspfad „Lieferkette“

Beim Einwirkungspfad „Lieferkette“ werden bereits mit Schadsoftware infizierte IT-Systeme – Hardware oder Software – geliefert und eingebaut bzw. es liegt eine Verletzung der Informationssicherheit bei einem Zulieferer zugrunde. Dabei gibt es neben der Manipulation von Hardware vor der Lieferung unterschiedliche Angriffsformen über die Lieferkette, wie beispielsweise das Einschleusen von schadhaftem Code in legitime Software, die Manipulation von Software-Updates oder die Kompromittierung von

IT-Dienstleistungen von Drittherstellern. Betroffen sind nicht nur Büro-Computer, sondern auch industrielle Steuerungssysteme einschließlich betrieblicher Leittechnik und Sicherheitsleittechnik sowie IoT (Internet of Things-) Geräte, die über das Internet verknüpft sind und Daten und Informationen austauschen.

Pfadeinleitung

Der Einwirkungspfad „Lieferkette“ beginnt außerhalb von kerntechnischen Anlagen und Einrichtungen beim Hersteller bzw. Entwickler von Geräten oder Software, die in den Anlagen verwendet werden. Der Schritt der Übermittlung vom Hersteller hin in die Anlage, erfolgt entweder auf dem Wege der Hardware in physischer Form oder über die Software, welche beispielsweise über das Internet geladen oder über mobile Datenträger übertragen werden kann. Für Hardware ergibt sich als einleitender Pfad zum Beispiel die Modernisierung von Komponenten, entweder weil es für die verbauten Komponenten keinen Ersatz mehr gibt oder eine Modernisierung beispielsweise aufgrund neuer Anforderungen oder Features gewünscht ist. Zudem kann eine Erweiterung eines Systems angestrebt werden oder auch die Anschaffung eines neuen Systems. Im Bereich der Anlagensicherung gibt es mit fortschreitender Digitalisierung stetig weiterentwickelte Systeme, die die Arbeit der Objektsicherung vor Ort signifikant erleichtern und zunehmend IT-Komponenten enthalten, die bei der Anschaffung ein Einfallstor für den Einwirkungspfad „Lieferkette“ darstellen können. Dieser Sachverhalt liegt dem meldepflichtigen Ereignis 2016/025 im Kernkraftwerk Biblis zugrunde, bei dem Schadsoftware auf Systemen der Anlagensicherung gefunden wurde, die mutmaßlich während der Einrichtung des Systems dorthin gelangte und sich über Jahre unbemerkt unter anderem über USB-Wechseldatenträger (siehe Einwirkungspfad „Wechseldatenträger“) verbreitete. Aber auch im Bereich der Anlagensicherheit gibt es eine stetige Weiterentwicklung, beispielsweise von leittechnischen Komponenten zur Prozesssteuerung.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Lieferkette“ einzuleiten, ist eine bzw. mehrere der folgenden Bedingungen zwingend notwendig:

- Einbau neuer Komponenten oder (Teil)-Systeme für sicherheits- oder sicherungstechnisch relevante Systeme und Funktionen einer kerntechnischen Anlage
- Updates von Komponenten oder (Teil)-Systemen für sicherheits- oder sicherungstechnisch relevante Systeme und Funktionen einer kerntechnischen Anlage

- Verbindung zu Diensten von Drittherstellern für sicherheits- oder sicherungstechnisch relevante Systeme und Funktionen einer kerntechnischen Anlage

Da eine externe datentechnische Verbindung eines sicherheits- oder sicherungsrelevanten Systems einer kerntechnischen Anlage in der Regel nicht bzw. zumindest nicht dauerhaft vorliegt, werden auch Softwareupdates typischerweise über Wechseldatenträger bzw. Servicegeräte durchgeführt. Dementsprechend weist der IT-Einwirkungspfad „Lieferkette“ unter diesen Umständen enge Verbindungen zu den IT-Einwirkungspfaden „Servicegeräte“ und „Wechseldatenträger“ auf. Bezüglich Hardware sind die notwendigen Bedingungen zur Pfadeinleitung, dass die in die Anlage installierten Komponenten, bereits vor Installation mit Schadsoftware infiziert sind oder sonstige IT-technische Schwachstellen aufweisen.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Unterstützend zur Einleitung des Einwirkungspfads „Lieferkette“ wirkt generell ein nicht sorgfältig durchgeführtes Update-Management in kerntechnischen Anlagen und Einrichtungen. Dazu zählt unter anderem beispielsweise die Auswahl vertrauenswürdiger direkter Quellen für Hard- und Software und die erweiterte Lieferkette. In vielen Fällen sind Komponenten und Geräte bzw. Software in der heutigen Zeit sehr komplex und setzen sich unter Umständen aus einzelnen Teilen unterschiedlicher Hersteller zusammen, was bei der Einschätzung der potenziellen Gefahr für die IT-Sicherheit über die Lieferkette entsprechend berücksichtigt werden muss. Dies gilt sowohl für physische Hardwarekomponenten als auch für Software, die möglicherweise auf externe Bibliotheken oder sonstige Komponenten zurückgreift.

Für den IT-Einwirkungspfad „Lieferkette“ kann außerdem ein weiterer Aspekt unterstützend zur Pfadeinleitung wirken, der in der Kommunikation zwischen der potenziell betroffenen kerntechnischen Anlage bzw. Einrichtung und dem Hersteller einer betroffenen Komponente liegt. Um mögliche Einwirkungen zu minimieren, sollten über den Kontakt zwischen Anlage und Hersteller mögliche Sicherheitslücken oder IT-Angriffe schnellstmöglich kommuniziert werden, um rechtzeitig eingreifen zu können. In der Vergangenheit kam es bei IT-Angriffen und IT-Sicherheitsvorfällen über die Lieferkette bereits zu Situationen, in denen die betroffenen Hersteller ihre Kunden nicht bzw. nicht rechtzeitig über das Problem informiert hatten oder in denen nicht klar war, wer genau möglicherweise betroffen ist.

Insgesamt wirkt jede Art von Softwareupdates oder die Installation von neuen Hardwarekomponenten unterstützend für diesen IT-Einwirkungspfad, da potenziell bei jeder Verbindung des Systems zur „Außenwelt“ – direkt oder indirekt – bzw. jeder neuen Komponente potenziell Schadsoftware in das möglicherweise ansonsten isolierte Netzwerk gelangen könnte. Hierbei ist eine unzureichende Überprüfung neuer Komponenten bzw. von Updates auf Schadsoftwarefreiheit durch die Anlage zusätzlich unterstützend zur Einleitung des IT-Einwirkungspfads.

Pfadzwischenschritte

Nach initialer Pfadeinleitung kann, je nach den genauen Umständen, die Einwirkung auf betroffene und weitere, verbundene IT-Systeme weiter eskaliert werden. Hierzu zählen die vollständige Systemkontrolle und die automatisierte Verbreitung auf weitere Systeme, Servicegeräte und Wechseldatenträger. Im Fall des meldepflichtigen Ereignisses 2016/026 im Kernkraftwerk Biblis waren Rechner der Anlagensicherung, zwei externe Sicherungsfestplatten und neun Teilsysteme des Personenkontrollsystems betroffen, darunter mehrere an verschiedenen Orten installierte Dialogstation PCs. Im Detail ist nicht bekannt, wo genau das Einfallstor für die Schadsoftware war bzw. ob nur eine Komponente oder mehrere/alle bei der Installation betroffen waren und inwieweit sich die Schadsoftware über das autarke Ethernet-Netzwerk des Personenkontrollsystems verbreitet hat. Falls die Systeme und Komponenten nicht nur für eine einzelne kerntechnische Anlage qualifiziert wurden, sondern beispielsweise für einen oder mehrere Betreiber mehrerer kerntechnischer Anlagen, können die betroffenen Systeme und Komponenten anlagenübergreifend verbreitet werden.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Lieferkette“ endet mit der Installation der neuen Komponente/des Updates in der Anlage. Potenzielle Schadsoftware kann in Folge entweder direkt auf die Komponente/das System, welches von der Modifizierung betroffen war, Einfluss nehmen oder sich im Netzwerk bzw. auf verbundene Systeme verbreiten. Dies können unter Umständen beispielsweise programmierbare Logikkontroller, (programmierbare) Steuerungen, Server oder ähnliches sein. Über Wechseldatenträger und Servicegeräte können zudem potenziell weitere Systeme betroffen werden, die vermeintlich durch das Air-Gap geschützt sind. Entsprechend sind die Pfadübergänge zu weiteren IT-Einwirkungspfaden abhängig von den bestehenden datentechnischen Verbindungen und der Art, wie die Einwirkung stattfand.

Es kann zu Interaktionen mit den IT-Einwirkungspfaden „Servicegeräte“, „Wechseldatenträger“ und ggf. weiteren kommen.

4.2.5.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfads „Lieferkette“ sind generell abhängig von den betroffenen Systemen und der Art der potenziellen Schadsoftware. Der wesentliche Aspekt dieses Einwirkungspfads ist eng mit der Fragestellung der generellen Sicherheit von Software- bzw. Hardwareupdates/Modernisierungen verknüpft. Handelt es sich bei betroffenen Komponenten um in mehreren Anlagen verwendete Systeme, kann ein IT-Angriff prinzipiell mehrere kerntechnische Anlagen und Einrichtungen betreffen.

Real beobachtete Auswirkungen

Im Fall des meldepflichtigen Ereignisses 2016/025 im Kernkraftwerk Biblis gab es keine Auswirkungen auf die Anlage, Personen oder die Umgebung. Die vom Schadsoftwarefund betroffenen Computer waren teilweise nicht im Betrieb und somit ausgeschaltet. Außerdem waren keine Computer betroffen, die elementare Funktionen der Anlagensicherung in der Peripherie erfüllen. Die Computer für Hauptfunktionen der Systeme waren schadsoftwarefrei. Insgesamt waren neben den Computern der Anlagensicherung und zwei externen Festplatten auch neun Teilsysteme des Personenkontrollsystems betroffen. Dabei handelt es sich um ein autarkes Ethernet-Netzwerk bestehend aus einem Hauptserver mit Datenbank, Dialogstationen, die beispielsweise als Bedienoberfläche zur Eingabe von Daten oder Ausweiserstellung dienen, sowie Stationen zur Personenidentifizierung und Zutrittsfreigabe. Eine forensische Analyse ergab, dass die Schadsoftware keine Funktionalitäten beinhaltete, die auf eine Manipulation von Zutrittskontroll- oder Steuerungssystemen hindeutete und generell ohne eine aktive externe Kommunikationsmöglichkeit keine Veränderungen an Daten vornehmen konnte.

Potenzielle Auswirkungen

IT-Einwirkungen über die Lieferkette können generell alle Systeme betreffen, die IT-Komponenten enthalten. Prinzipiell können IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein, die sicherheits- und sicherungstechnisch relevant sind, was schwerwiegende sicherheits- und sicherungstechnische Auswirkungen auf die Anlage haben kann. Wie das meldepflichtige Ereignis 2016/025 zeigt, war die Schadsoftware auf einem der IT-Schutzbedarfsklasse „Hoch“ zugeordneten System der Anlagensicherung über einen

langen Zeitraum unentdeckt vorhanden, wobei das System unter anderem durch ein Air-Gap geschützt ist, welches insbesondere im Fall der vorigen Schadsoftwareinfektion von Hardware über die Lieferkette einfach überwunden werden kann. Somit kann der Einwirkungspfad zur Überwindung von Air-Gaps genutzt werden und eine Manipulation von Systemen ermöglichen, deren Netzwerk keine Verbindungen zu weiteren Netzwerken bzw. zur Außenwelt haben oder deren Verbindungen durch Entkopplungs- oder andere Schutzmaßnahmen gesichert sind.

Im konkreten Fall des Personenkontrollsystems hätte speziell konfigurierte Schadsoftwäre unbemerkt das System teilweise oder vollständig stören, ausschalten oder manipulieren können, sodass der Zugang berechtigter Personen verhindert oder erschwert wird oder unberechtigte Personen Zugang zu sensiblen Bereichen erhalten, sodass es zu weiteren Einwirkungen kommen kann. Die Tatsache, dass die Schadsoftware zum Teil über Jahre hinweg bereits auf einigen der betroffenen Systeme ohne Entdeckung vorhanden war zeigt, dass bei entsprechendem zeitlichen Aufwand, Einflussnahmen durchaus möglich sind. Hierbei ist zudem ein dauerhafter oder regelmäßiger externer Datenverkehr zu potenziellen Angreifern nicht zwingend erforderlich.

Wird generell über die Lieferkette auf IT-Systeme eingewirkt, jedoch nicht pfadübergreifend direkt auf andere IT-Systeme, besteht eine große Anzahl an möglichen sicherheits- und sicherungstechnisch relevanten Auswirkungen. Einwirkende können unter anderem Informationen auslesen, was die Vertraulichkeit des ggf. direkt betroffenen Systems selbst und der damit verbundenen Systeme verletzt. Außerdem könnten Daten modifiziert oder gelöscht werden, sodass die Integrität verletzt ist. Eine Verletzung der Verfügbarkeit ist ebenfalls denkbar.

Die IT-Einwirkung über die Lieferkette ermöglicht somit insgesamt eine umfassende Einwirkung über das Gerät hinaus auf sicherheits- und sicherungsrelevante IT-Systeme. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Lieferkette“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen. Über Softwareupdates oder den Einsatz neuer manipulierter Hardware, kann Schadsoftware in kerntechnische Anlagen und Einrichtungen gelangen und insbesondere auch in Netzwerke eindringen, die durch Air-Gaps von der Außenwelt isoliert oder durch sonstige Maßnahmen geschützt sind. Der Einwirkungspfad „Lieferkette“ kann einleitend für bzw. übergreifend auf folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „**Servicegeräte**“: Servicegeräte können potenziell mit Geräten verbunden werden, die vom IT-Einwirkungspfad Lieferkette betroffen sind - beispielsweise im Rahmen eines Softwareupdates (auch eines potenziell manipulierten Softwareupdates selbst). Dadurch kann sich die Schadsoftware potenziell weiterverbreiten und je nach Einsatz des Servicegeräts weitere Systeme und Netzwerke infizieren.

- IT-Einwirkungspfad „**Wechseldatenträger**“: Wechseldatenträger können potenziell mit Geräten verbunden werden, die vom IT-Einwirkungspfad Lieferkette betroffen sind – beispielsweise im Rahmen der Erstellung eines Backups. Dadurch kann sich die Schadsoftware potenziell weiterverbreiten und je nach Einsatz des Wechseldatenträgers weitere Systeme und Netzwerke infizieren.

- IT-Einwirkungspfad „**Netzwerkverbindung**“: Bestehen für das vom IT-Einwirkungspfad „Lieferkette“ betroffene IT-System datentechnische Verbindungen zu weiteren Komponenten oder IT-Systemen, kann es zu weiteren Angriffsschritten über diese Verbindungen kommen. Der IT-Einwirkungspfad „Lieferkette“ kann somit einleitend für den IT-Einwirkungspfad „Netzwerkverbindung“ wirken.

- IT-Einwirkungspfad „**Überlastung von IT-Systemen**“: Vom IT-Einwirkungspfad „Lieferkette“ betroffene IT-Systeme können zur Einleitung des IT-Einwirkungspfads „Überlastung von IT-Systemen“ genutzt werden.

4.2.5.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Lieferkette“ verschiedene mögliche Pfadeinleitungen und kann außerdem zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung auf.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Im Fall von IT-Einwirkungen über die Lieferkette beinhaltet dies, möglichst wenige Softwareupdates durchzuführen, da diese möglicherweise kompromittiert sind und somit Schadsoftware aus vermeintlich seriöser Quelle auf das System gelangt. Demgegenüber müssen jedoch möglicherweise offene Sicherheitslücken, die möglicherweise auf Systemen die nicht mit Updates versorgt werden vorliegen, betrachtet werden. Außerdem wirkt die Sicherstellung der Integrität des Updates mitigativ, wobei ggf. nur eingeschränkt möglich ist, wenn beispielsweise die Updatedatei selbst, vom Hersteller unbemerkt manipuliert wurde. In dieser Hinsicht ist eine aufmerksame Beobachtung der IT-Sicherheitslage eingesetzter Komponenten erforderlich, um bei Bekanntwerden von kompromittierten Updates schnellstmöglich handeln zu können. Dies gilt auch für neu eingesetzte Hardware-Komponenten.

Aufgrund der Problematik, der möglicherweise nicht durch Virenscanner zu erkennenden manipulierten Updates könnte die Durchführung von Softwareupdates nicht für alle (getrennten) Systeme eines Typs/Redundanzen gleichzeitig durchgeführt werden, damit bei einem möglichen Angriff nicht alle Redundanzen bzw. Systeme betroffen sind. Zudem ist es möglich, Softwareupdates nicht direkt nach dem Erscheinen durchzuführen, sondern eine gewisse Zeitspanne abzuwarten, in der die Sicherheit des Updates beurteilt werden kann. Generell wirkt ein entsprechend umgesetztes IT-Sicherheitsmanagement und entsprechende administrative Regelungen ggf. mitigierend für diesen Einwirkungspfad, beispielsweise indem Systeme möglichst isoliert aufgebaut sind und somit die Verbreitung möglicher Schadsoftwarekomponenten behindert wird.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die Aufnahme von Gegenmaßnahmen und im Idealfall die sofortige Beendigung eines IT-Einwirkungspfades. Wird eine Einwirkung entdeckt, kann der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen werden. Im Fall von IT-Einwirkungen über die Lieferkette gibt es nur begrenzte Möglichkeiten der Aufdeckung. Virenscans von Softwareupdates, die vom Hersteller bereitgestellt wurden und vor der Verbreitung unbemerkt manipuliert wurden,

führen in der Regel nicht zur Detektion. Auch auf vom Hersteller eingebaut oder gelieferte Hardware lässt sich nur schwer überprüfen unter der Annahme, dass kein offensichtlicher Schadsoftwarebefall vorliegt, sondern eine gezielte Platzierung und Tarnung von Schadsoftwarekomponenten. Gegebenenfalls ist es möglich, Hardware über Boot-Integritäts-Checks zu überprüfen und Integritätsverletzungen zu erkennen, wobei dies von der Art der Überprüfung und der Art der Einwirkung abhängig ist.

Eine Möglichkeit zur Aufdeckung bietet unter Umständen die Beobachtung und Analyse (verdächtiger) Netzwerkkommunikation oder unregelmäßiger und verdächtiger Systemaktivitäten. Auch zur Aufdeckung ist der intensive Kontakt zum Hersteller hilfreich. Darüber hinaus können die Beobachtung der IT-Sicherheitslage genutzter Systeme und Komponenten und eine umfassende Kommunikation zwischen kerntechnischen Anlagen dazu beitragen, mögliche problematische Updates oder generell Einwirkungsmöglichkeiten über die Lieferkette aufzudecken und zu identifizieren.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Lieferkette“ nimmt seinen Ausgangspunkt außerhalb betroffener kerntechnischer Einrichtungen. Für softwarebasierte IT-Einwirkungen über den IT-Einwirkungspfad „Lieferkette“ ist die Durchführung eines nachfolgenden Updates ein unterbrechender Faktor, falls dadurch mögliche Schwachstellen, die ausgenutzt wurden, behoben werden. Zudem kann eine Einwirkung sowohl hardware- als auch softwarebasiert ggf. durch Air-Gaps unterbrochen werden. Ansonsten wird der IT-Einwirkungspfad Lieferkette unterbrochen, wenn eine Aufdeckung stattfindet und daraufhin anforderungsgerechte Maßnahmen eingeleitet werden.

4.2.5.4 Pfadzusammenfassung Lieferkette

Der IT-Einwirkungspfad „Lieferkette“ ist unter den beschriebenen Gesichtspunkten als schwerwiegender Einwirkungspfad mit zentralen Einwirkungsmöglichkeiten anzusehen, der auf verschiedenste Weise eingeleitet werden kann. Durch die oftmals auch durch Virenscanner oder sonstige Maßnahmen nicht bzw. nur schwer zu entdeckende Schadsoftwareinfektion von IT-Systemen, die über die Lieferkette erfolgt, ergeben sich zudem zahlreiche mögliche pfadübergreifende Auswirkungen und Möglichkeiten zur Verbreitung von Schadsoftware auch in isolierte Netzwerke und Systeme, indem beispielsweise schützende Air-Gaps überwunden werden.

Dies gilt insbesondere für die Anwendung von IT-Systemen in diversen Bereichen kerntechnischer Anlagen und Einrichtungen, da prinzipiell jedes IT-System betroffen sein kann, woraus sich für diverse sicherheits- und sicherungstechnisch relevante Systeme eine besondere Relevanz der Problematik ergibt. Die möglichen Auswirkungen des Einwirkungspfades sind potenziell schwerwiegend. Mit dem meldepflichtigen Ereignis 2016/025 kam es bereits zu einem IT-Sicherheitsvorfall in Zusammenhang mit einem Wechseldatenträger in einem deutschen Kernkraftwerk.

Durch die Reduzierung der Durchführung von Updates und der intensiven Kommunikation zwischen der Anlage und dem Hersteller können schadhafte Einwirkungen über die Lieferkette erschwert oder verhindert werden. Insbesondere für diesen IT-Einwirkungspfad sind aufdeckende Faktoren wie beispielsweise die Beobachtung von Netzwerkaktivitäten relevant, da andere Maßnahmen wie Virenscanner, die bei anderen IT-Einwirkungspfaden zur Aufdeckung und Unterbrechung des Einwirkungspfads führen können, im Fall des IT-Einwirkungspfads „Lieferkette“ ggf. unwirksam sind.

4.2.6 Wechseldatenträger

Mobile Datenträger werden weltweit in Unternehmen und Organisationen verschiedenster Sektoren regelmäßig eingesetzt. Dazu zählen auch kerntechnische Anlagen und Einrichtungen bzw. generell kritische Infrastrukturen. Als einfachstes Beispiele sind in diesem Zusammenhang USB-Sticks oder externe Festplatten zu nennen, die in der Regel unter anderem zum Datentransport oder Backup genutzt werden. Dies hat vor dem Hintergrund der angestrebten Minimierung von bzw. dem Verzicht auf Verbindungen eines Netzwerks zu weiteren Netzwerken oder zum Internet eine hervorzuhebende Bedeutung, da in diesem Fall mobile Datenträger möglicherweise die einzigen datentechnischen Verbindungen (ggf. abgesehen von Service- bzw. Programmiergeräten) zu isolierten (Insel)-Systemen darstellen. Mobile Datenträger stellen somit ein wirksames Werkzeug zur Überwindung sogenannter Air-Gaps dar, was in der Vergangenheit bereits durch diverse IT-Angriffe und IT-Sicherheitsvorfälle – überwiegend im nicht-nuklearen Bereich – gezeigt wurde.

Auch in Deutschland gab es mit dem meldepflichtigen Ereignis 2016/022 bereits einen IT-Sicherheitsvorfall im Zusammenhang mit mobilen Datenträgern.

In diesem konkreten Fall kam es zu einem Schadsoftwarefund auf einem Visualisierungsrechner der Brennelement-Lademaschine und weiteren acht Computern im Kernkraftwerk Gundremmingen, wobei die Schadsoftware über einen USB-Stick, der zuvor an einen Schulungsrechner mit Zugang zum Internet angeschlossen wurde, auf die betroffenen Systeme gelangte. Der USB-Stick war für diesen Einsatz nicht vorgesehen, da die Datenübertragung zwischen den IT-Systemen der BE-Lademaschine ausschließlich über einen dedizierten und nur dafür verwendeten USB-Stick erfolgen sollte, der außerdem unmittelbar vor dem Einsatz auf Schadsoftware überprüft werden soll, sodass in diesem Fall auch menschliche bzw. organisatorische Fehler für den IT-Sicherheitsvorfall relevant sind.

4.2.6.1 Der Einwirkungspfad „Wechseldatenträger“

Beim Einwirkungspfad „Wechseldatenträger“ gelangt Schadsoftware über mobile Datenträger wie USB-Sticks oder externe Festplatten in ansonsten nur sehr schwer oder gar nicht von außen zugängliche Netzwerke und Systeme. Potenziellen Angreifern ist es dadurch möglich beispielsweise, von einem Standort innerhalb oder außerhalb der Anlage schadhaften Einfluss auf IT-Systeme auszuüben, die durch Schutzmaßnahmen wie zum Beispiel Air-Gaps, geschützt sind. Prinzipiell können verschiedene IT-Systeme betroffen sein und insbesondere neben solchen mit einer für die mobilen Datenträger zugehörigen Schnittstelle auch Systeme, die keine entsprechende Schnittstelle besitzen, sich aber im selben (geschützten) Netzwerk wie IT-Systeme mit Schnittstellen befinden, über die eine Infektion dann erfolgen kann.

Pfadeinleitung

Für den Einwirkungspfad „Wechseldatenträger“ gibt es mehrere Einleitungsmöglichkeiten. Potenziellen Angreifern mit Zutritt zu kerntechnischen Anlagen und Einrichtungen ist es prinzipiell möglich, einen mit Schadsoftware präparierten USB-Stick oder eine externe Festplatte auf dem Anlagengelände zu platzieren. Je nach Sicherheitskonzept vor Ort für den Zutritt in verschiedene Bereiche mit erhöhtem Sicherheitsbedarf, ist der direkte Zugriff auf ein Zielsystem gegebenenfalls erschwert. Wie das Beispiel des meldepflichtigen Ereignisses 2016/022 aus dem Kernkraftwerk Gundremmingen zeigt, ist der direkte Zugriff unter Umständen jedoch nicht erforderlich, um Schadsoftware auf dem Zielsystem zu platzieren.

Vorstellbar wäre beispielsweise auch, dass ein potenzieller Angreifer einen präparierten Wechseldatenträger derartig platziert, dass er von anderen Personen verwendet wird. Prinzipiell ist außerdem denkbar, dass ein potenzieller Angreifer ohne Zutritt zu kerntechnischen Anlagen und Einrichtungen, sich zunächst über anderweitige Techniken wie Phishing oder Spear-Phishing Zugriff auf ein weniger kritisches (Büro)-Netzwerk verschafft, und bei entsprechendem Zeitaufwand darauf angewiesen ist, dass das Air-Gap zu sicherheits- bzw. sicherungsrelevanten Systemen mit Hilfe eines Wechseldatenträgers überwunden wird, der beispielsweise wie im Fall von Gundremmingen durch Personen fälschlicherweise verwendet wird. Schließlich kann darüber hinaus auch der Wechseldatenträger selbst bereits bei der Anschaffung Schadsoftware enthalten bzw. manipuliert worden sein. Diese Problematik schließt an den Einwirkungspfad „Lieferkette“ an, der separat diskutiert wird.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Wechseldatenträger“ einzuleiten, sind folgende Bedingungen zwingend notwendig:

- Existenz und/oder Nutzung von Wechseldatenträgern für sicherheits- oder sicherungstechnisch relevante Systeme und Funktionen einer kerntechnischen Anlage
- Existenz und/oder Nutzung von Wechseldatenträgern für Systeme mit Verbindung zu sicherheits- oder sicherungstechnisch relevanten Systemen einer kerntechnischen Anlage

Sobald ein oder mehrere Wechseldatenträger für sicherheits- und sicherungstechnisch relevante Funktionen verwendet werden, ist potenziell eine Einwirkungsmöglichkeit über diese mobilen Datenträger möglich. Zudem ist denkbar, dass Systeme betroffen sind, die selbst keinen direkten physischen Kontakt zu Wechseldatenträgern haben, netzwerktechnisch aber mit Systemen verbunden sind, bei denen Wechseldatenträger verwendet werden.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Die Möglichkeiten der Einleitung des IT-Einwirkungspfades „Wechseldatenträger“ werden durch die erweiterte Nutzungen von Wechseldatenträgern, Datenaustausch, erweiterte Zugriffsmöglichkeiten und die nicht Einhaltung bzw. das Fehlen von Sicherungsvorschriften erweitert bzw. vereinfacht. Im meldepflichtigen Ereignis 2016/022 wurden

Sicherheitsvorschriften nicht konsequent beachtet, die besagten, dass in Verwendung beim IT-System der BE-Lademaschine nur spezielle USB-Sticks verwendet werden sollten, die vor Verwendung außerdem auf Schadsoftware geprüft werden sollten.

Unterstützend wirken insbesondere jede Form von regelmäßigen und sporadischen Datentransfers bzw. generell die Verbindung von Wechseldatenträgern zu Systemen oder Netzwerken mit sicherheits- bzw. sicherungsrelevanten Funktionen. Jede Verbindung, ob diese betrieblich oder sicherheitstechnisch (z. B. aufgrund von Backups oder Patches/Updates) geboten ist, ist eine potenzielle Einleitung des IT-Einwirkungspfades. Werden generell bzw. zusätzlich Schutzmaßnahmen und Regeln nicht ausreichend beachtet, werden diese Einwirkungsmöglichkeiten noch weiter wahrscheinlich. Dies gilt insbesondere, wenn ein Wechseldatenträger in Verbindung mit mehreren IT-Systemen verwendet wird, sodass eine Schadsoftwareinfektion des mobilen Datenträgers sich potenziell auf mehrere Systeme auswirken kann.

Pfadzwischenschritte

Nach initialer Einwirkung auf Wechseldatenträger kann, je nach den genauen Umständen, die Schadsoftware eingebracht und die Einwirkung auf betroffene IT-Systeme weiter eskaliert werden. Hierzu zählt die vollständige Systemkontrolle und die automatisierte Verbreitung auf weitere Systeme und Wechseldatenträger. Im Fall des meldepflichtigen Ereignisses 2016/022 in Gundremmingen waren neben dem Visualisierungsrechner der BE-Lademaschine außerdem acht Computer in der Anlage infiziert, sowie 18 USB-Sticks und ein Notebook einer Fremdfirma.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Wechseldatenträger“ endet mit der IT-Einwirkung auf die mit den Wechseldatenträgern verbundenen IT-Systeme. Dies können z. B. programmierbare Logikkontroller, (programmierbare) Steuerungen, Server oder ähnliches sein. Bei der weiteren Verwendung des betroffenen Wechseldatenträgers können gegebenenfalls weitere Schadsoftwarekomponenten heruntergeladen oder Informationen übertragen werden, wenn eine Verbindung zu Systemen mit Internetanbindung bestehen sollte. Die Pfadübergänge zu weiteren IT-Einwirkungspfaden sind abhängig von den bestehenden datentechnischen Verbindungen und der Art, wie die Einwirkung stattfand. Es kann zu Interaktionen mit den IT-Einwirkungspfaden „Servicegeräte“, „Leittechnikverbreitung“ und weiteren kommen.

4.2.6.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfads „Wechseldatenträger“ sind generell abhängig von den betroffenen Systemen und der Art der potenziellen Schadsoftware. In erster Linie ist dieser Einwirkungspfad im Zusammenhang mit der Überwindung des Air-Gaps relevant, um Netzwerke und Systeme mit Schadsoftware zu infizieren, die keine Verbindung zu externen Systemen oder dem Internet haben oder anderweitig durch Schutzmaßnahmen isoliert sind.

Real beobachtete Auswirkungen

Im Fall des meldepflichtigen Ereignisses 2016/022 in Gundremmingen gab es keine Auswirkungen auf die Anlagen, Personen oder die Umgebung. Die auf dem Visualisierungsrechner der BE-Lademaschine gefundene Schadsoftware war auf Windows-Infrastrukturen ausgelegt und beinhaltete keine Funktionalitäten zur Manipulation von Steuerungssystemen. Das betroffene System hatte keine Internetverbindung. Die Konfiguration des Visualisierungsrechners zum Zeitpunkt des Vorfalls erlaubte zudem keine Änderungen der Betriebs- und Sicherheitssteuerungen der BE-Lademaschine. Es ist davon auszugehen, dass es sich nicht um einen gezielten IT-Angriff handelte, sondern um eine zufällige Infektion mit Schadsoftware, die nur aufgrund der Verwendung eines USB-Sticks in nicht vorgesehenen Rahmen, im Zusammenhang mit einem anderen IT-System (Schulungsrechner), erfolgen konnte. Neben dem Visualisierungsrechner der BE-Lademaschine wurden außerdem acht Computer der Anlage, ein Notebook einer Fremdfirma und 18 USB-Sticks infiziert. Eine forensische Analyse der Schadsoftware im betroffenen Fall ergab, dass diese nicht aktiv genutzt wurde und aufgrund der fehlenden externen Netzwerkverbindung keine weiteren IT-Angriffsschritte möglich gewesen wären.

Potenzielle Auswirkungen

Wechseldatenträger können vielfältig eingesetzt werden. In der Regel werden sie beispielsweise zur Datenübertragung oder Speicherung von Backups verwendet. In diesem Zuge ergeben sich je nach Nutzung der Wechseldatenträger für ein oder mehrere Systeme potenzielle Verbindungen zu diversen IT-Systemen. Wie das meldepflichtige Ereignis 2016/022 zeigt, können Wechseldatenträger zur Überwindung von Air-Gaps genutzt werden und eine Manipulation von Systemen ermöglichen, deren Netzwerk keine

Verbindungen zu weiteren Netzwerken bzw. zur Außenwelt haben oder deren Verbindungen durch Entkopplungs- oder andere Schutzmaßnahmen gesichert sind. Prinzipiell können IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein, die sicherheits- und sicherungstechnisch relevant sind, was schwerwiegende sicherheits- und sicherungstechnische Auswirkungen haben kann. Im konkreten Fall der BE-Lademaschine hätte speziell konfigurierte Schadsoftwäre unbemerkt über den Visualisierungsrechner im Laufe der Zeit Änderungen der Betriebs- und Sicherheitssteuerungen der BE-Lademaschine vornehmen können, auch wenn die zu dem Zeitpunkt vorliegende Konfiguration des Systems keine Änderung erlaubte. Die Tatsache, dass die Schadsoftware zum Teil über Jahre auf einigen der betroffenen Systeme ohne Entdeckung vorhanden war zeigt, dass bei entsprechend zeitlichem Aufwand Einflussnahmen möglich sind. Dabei ist außerdem ein dauerhafter oder regelmäßiger externer Datenverkehr nicht zwingend erforderlich.

Wird generell auf Wechseldatenträger eingewirkt, jedoch nicht pfadübergreifend direkt auf andere IT-Systeme, besteht eine große Anzahl an möglichen sicherheits- und sicherungstechnisch relevanten Auswirkungen. Einwirkende können unter anderem die auf dem Wechseldatenträger gespeicherten Informationen auslesen, was die Vertraulichkeit des Datenträgers selbst und der damit verbundenen Systeme verletzt. Außerdem könnten Daten modifiziert oder gelöscht werden, sodass die Integrität verletzt ist. Eine Verletzung der Verfügbarkeit ist ebenfalls denkbar, was insbesondere bei Backups relevant ist. Generell ist die Einflussnahme auf mit dem Wechseldatenträger verbundene Systeme bzw. Systeme mit netzwerktechnischer Verbindung dazu möglich.

Die Manipulation von Wechseldatenträgern ermöglicht somit insgesamt eine umfassende Einwirkung über das Gerät hinaus auf sicherheits- und sicherungsrelevante IT-Systeme. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Wechseldatenträger“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen. Wechseldatenträger an sich besitzen in kerntechnischen Anlagen und Einrichtungen in der Regel keine aktive bzw. steuernde Funktion, sondern werden mit entsprechenden Systemen verbunden, auf die dadurch Einflussnahmen möglich sind. Abgesehen von potenziellem Datendiebstahl oder vom Löschen gespeicherter Daten, dienen Wechseldatenträger somit in einem Angriffsszenario hauptsächlich dem Zweck,

Schadsoftware zu verbreiten und Netzwerke und Systeme zu infiltrieren und infizieren, die beispielsweise keine datentechnische Verbindung zur Außenwelt haben, sodass das in der Theorie schützende Air-Gap überwunden wird. Der Einwirkungspfad „Wechseldatenträger“ kann somit einleitend für bzw. übergreifend auf folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „Servicegeräte“: Servicegeräte können potenziell mit Wechseldatenträgern verbunden werden, beispielsweise im Rahmen eines Softwareupdates oder zur Backuperstellung. Die beiden IT-Einwirkungspfade „Servicegeräte“ und „Wechseldatenträger“ können daher gegenseitig einleitend wirken und einander beeinflussen.
- IT-Einwirkungspfad „Netzwerkverbindungen“: Wechseldatenträger können, wenn sie mit IT-Systemen mit datentechnischen bzw. Netzwerkverbindungen zu weiteren Komponenten oder anderen IT-Systemen verbunden werden, entsprechend weitere Angriffsschritte über diese Verbindungen ermöglichen. Sie können zur Einleitung des IT-Einwirkungspfads „Netzwerkverbindung“ eingesetzt werden.
- IT-Einwirkungspfad „Parametrierung und Konfiguration“: Die Parametrierung bzw. Konfiguration von IT-Systemen kann manipuliert werden, wenn Wechseldatenträger an parametrierbare bzw. konfigurierbare IT-Systeme angeschlossen werden.
- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Entsprechend präparierte bzw. manipulierte Wechseldatenträger können durch Anschluss an bestimmte IT-Systeme zu einer Überlastung dieser Systeme führen.

4.2.6.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Wechseldatenträger“ verschiedene mögliche Pfadeinleitungen und kann außerdem zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen Interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung ein.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Im Fall von Wechseldatenträgern beinhaltet dies insbesondere die Reduzierung der datentechnischen Verbindungen der Geräte zu IT-Systemen. Um eine weite Verbreitung von Schadsoftware zu

verhindern, ist eine beispielsweise durch administrative Regelungen implementierte exklusive Zuordnung spezifischer Wechseldatenträger zu einzelnen IT-Systemen bzw. IT-Sicherheitszonen denkbar. Außerdem können durch eine Deaktivierung nicht verwendeter Schnittstellen und eine Whitelist autorisierter Geräte für die verwendeten Schnittstellen, die Erfolgsaussichten des IT-Einwirkungspfads „Wechseldatenträger“ weiter reduziert werden.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die Aufnahme von Gegenmaßnahmen und im Idealfall die sofortige Beendigung eines IT-Einwirkungspfades. Wird eine Einwirkung entdeckt, kann der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen werden. Eine wirksame Maßnahme zur Aufdeckung ist im Fall von Wechseldatenträgern der Virenscan auf das Vorhandensein von Schadsoftware. Auf Wechseldatenträgern gespeicherte Daten oder Backups können zudem über Checksummenvergleiche bezüglich der Integrität überprüft werden, bevor die Wechseldatenträger mit den Zielsystemen verbunden werden. Eine Überwachung und Überprüfung des Datenverkehrs kann zudem Hinweise auf verdächtige Systemaktivitäten liefern und auf das Vorhandensein von Schadsoftware hindeuten; woraufhin weitere investigative Maßnahmen durchgeführt werden können.

Unterbrechende Faktoren

Abseits der Pfadunterbrechungen nach Aufdeckung, bestehen verschiedene Möglichkeiten den IT-Einwirkungspfad „Wechseldatenträger“ zu unterbrechen. Der Einwirkungspfad kann dadurch unterbrochen werden, dass nicht verwendete Schnittstellen des IT-Systems deaktiviert oder mechanisch verschlossen sind und bei aktivierten Schnittstellen nur auf einer Whitelist eingetragene Wechseldatenträger erlaubt sind. Außerdem bieten administrative Regelungen bezüglich des Umgangs mit diesen Systemen, Zugriffskontrollen, Unterbringungsschutz und datentechnische Untersuchungen vor und während Datenübertragungen, die Möglichkeit Einwirkungen zu unterbrechen, bevor sie den IT-Einwirkungspfad „Wechseldatenträger“ einleiten können oder aber von Wechseldatenträgern ausgehend weitere Einwirkungen ermöglichen. Die unterbrechenden Faktoren enthalten generell allgemeine Aspekte, die auch für andere IT-Einwirkungspfade und in diesem Fall speziell für den Pfad „Servicegeräte“ gültig sind.

4.2.6.4 Pfadzusammenfassung Wechseldatenträger

Der IT-Einwirkungspfad „Wechseldatenträger“ ist unter den beschriebenen Gesichtspunkten als schwerwiegender Einwirkungspfad mit zentralen Einwirkungsmöglichkeiten anzusehen, der auf verschiedenste Weise eingeleitet werden kann. Durch die Mobilität und Anwendungsvielfalt von Wechseldatenträgern ergeben sich zudem zahlreiche mögliche pfadübergreifende Auswirkungen und Möglichkeiten zur Verbreitung von Schadsoftware auch in isolierte Netzwerke und Systeme, indem beispielsweise schützende Air-Gaps überwunden werden. Die allgemeine Anwendung von Wechseldatenträgern in kerntechnischen Anlagen und Einrichtungen ist nicht auf einen Bereich eingeschränkt, sondern relevant für diverse sicherheits- und sicherungstechnisch relevante Systeme. Die möglichen Auswirkungen des Einwirkungspfades sind potenziell schwerwiegend. Mit dem meldepflichtigen Ereignis 2016/022, kam es bereits zu einem IT-Sicherheitsvorfall in Zusammenhang mit einem Wechseldatenträger in einem deutschen Kernkraftwerk. Durch die Reduzierung von Kontakten von Wechseldatenträgern zu IT-Systemen, der festen Zuordnung der Geräte zueinander und der Deaktivierung nicht verwendeter Schnittstellen bzw. der Verwendung von Whitelists bei aktivierten Schnittstellen und mit entsprechend administrativen Regelungen – vorausgesetzt, diese werden eingehalten - können schadhafte Einwirkungen mit Hilfe von Wechseldatenträgern erschwert oder verhindert werden.

4.2.7 Versionenmanagement

Digitale Systeme bilden eine Einheit aus Software und Hardware, wobei einzig die Software nach der Herstellung noch nachträglich verändert werden kann. Die eingesetzte Software, sei es Firmware, installierbare Software für Betriebssysteme oder kleinere Betriebssysteme, wie Echtzeitbetriebssysteme, werden komplexer und damit anfälliger für Schwachstellen. Zusätzlich ist die Entwicklung einer Software mit dem Verkaufsbeginn des Produktes im Gegensatz zur Hardware nicht beendet, neue Funktionen und Optionen können einer Software auch beim Einsatz beim Endkunden weiterhin hinzugefügt werden.

Zur Schließung von Schwachstellen und zur Erweiterung der Funktionen, werden daher regelmäßig Updates für die eingesetzte Software digitaler Systeme, wie z. B. leittechnischen Steuerungssystemen, seitens der Herstellern veröffentlicht. Um die Versionen bzw. Updates auf die einzelnen betroffenen Systeme aufzuspielen, ist ein Versionsmanagement zu betreiben, um zu gewährleisten, dass nicht unterschiedliche Versionen zum Einsatz kommen und zu unerwartetem Verhalten der Systeme führen.

Mit dem Ereignis 2016/044 ist 2016 ein meldepflichtiges Ereignis bekannt geworden, in welchem der Versionsunterschied baugleicher Systeme eine Rolle spielte. Es kam zur Abschaltung von betroffenen Systemen und unerwartetem Verhalten der baugleichen, jedoch nicht versionsgleichen Systeme. Auch vermeintlich geringe Versionsunterschiede können untereinander, insbesondere bei redundanten Systemen, zu Abweichungen im Verhalten führen oder die Änderung bestehender Parameter notwendig machen. Abweichend vom Einwirkungspfad über die Lieferkette, bei welchem z. B. die Versionsupdates selbst betroffen sind, werden die Einwirkungen über das Versionenmanagement direkt vor Ort in der Anlage durchgeführt. Hierbei werden nicht die Versionen selbst oder die Updates manipuliert, sondern das Versionenmanagement wird in einer Weise beeinflusst, dass nicht kompatible Versionen gleichzeitig in Betrieb genommen werden.

4.2.7.1 Der Einwirkungspfad „Versionenmanagement“

Der Einwirkungspfad beginnt im Rahmen der Managementtätigkeiten von Update- und Versionierungsprozessen. Er unterscheidet sich hierbei vom Einwirkungspfad über die Lieferkette insofern, als nicht die eigentlichen Updates oder Versionen selbst manipuliert werden, sondern deren Zusammenwirken nach Anwendung. Zum Einwirkungspfad über die Parametrierung unterscheidet er sich insofern, dass keine Einwirkung auf betroffene IT-Systeme über den Update-Prozess hinaus, durchgeführt werden. Einwirkende müssen bei dem Aufspielen der Updates nicht anwesend sein, es muss in irgendeiner Form auf die Versionierung bzw. auf das Management von Updates zugegriffen werden können. Hierzu werden Pläne zum Bezug und zur Installation von Updates durchgeführt. Eine direkte Manipulation der Liste der zu updatenden Systeme führt z. B. zu einem Versionsunterschied dieser Systeme, aus welchem sich dann potenziell schadhafte Konsequenzen ergeben. Hierzu reicht ein Zugriff auf das Betriebsführungssystem sowie eine mangelhafte Prüfung von Arbeitsaufträgen aus. Bei der Ausführung der Updates kann direkt zugegriffen werden.

Pfadeinleitung

Der Einwirkungspfad „Versionenmanagement“ beginnt nach dem Eingang von Updates für im Betrieb befindliche digitale Systeme von Kernkraftwerken. Um den Pfad einzuleiten, ist die Einwirkung auf den Arbeitsprozess zum Aufspielen von Versionsupdates in der Weise zu beeinflussen, dass nach Abschluss der Arbeiten zwei oder mehr verschiedene Versionen auf redundanten oder zusammenwirkenden IT-Systemen aufgespielt sind. Eine solche Einwirkung auf den Arbeitsprozess kann zum einen beginnend beim Arbeitsmanagement einwirken. Hierbei wird entweder auf ein Betriebsführungssystem über einen vorherigen Einwirkungspfad wie „USB-Sticks“ eingewirkt, sodass die Dokumentation des Arbeitsprozesses manipuliert wird. Alternativ kann Vor-Ort direkt auf den Arbeitsprozess eingewirkt werden, z. B. in dem die Ausführung manipuliert wurde. Werden nun verschiedene Versionen auf redundante oder innerhalb eines Netzwerks gemeinsam arbeitende baugleiche IT-Systeme aufgespielt, kann es zu unerwartetem Verhalten der Systeme kommen. Im Anforderungsfall können die Systemeigenschaften dann möglicherweise gar nicht, nicht wie erwartet oder sporadisch nicht zur Verfügung stehen.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Versionsmanagement“ einzuleiten, ist eine bzw. mehrere der folgenden Bedingungen zwingend notwendig:

- Updates für bestehende oder zukünftig einzubauende Systeme sind vorgesehen
- Zugriff auf den Arbeitsprozess oder das Arbeitsprozessmanagement
- Potenziell schadhafte Wechselwirkung unterschiedlich versionierter IT-Systeme

Um über das Versionenmanagement auf IT-Systeme einzuwirken, muss mindestens eine neue Version via Update für die betroffenen IT-Systeme bereitstehen und deren Installation muss langfristig vorgesehen sein. Um einen Versionenunterschied zwischen den IT-Systemen sicherzustellen, ist ein wie auch immer gearteter Zugriff auf den Arbeitsprozess oder das Arbeitsprozessmanagement notwendig. Weiterhin müssen die daraufhin unterschiedlichen Versionen der Software bzw. Firmware der betroffenen IT-Systeme, ein Potenzial zur schadhaften Wechselwirkung haben.

Hierzu sind mehrere IT-Systeme gleichen Typs notwendig, die zusätzlich in irgendeiner Form miteinander in Verbindung stehen bzw. deren gegenläufige Signale unerwünschte Auswirkungen haben können.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Unterstützend zur Einleitung des Einwirkungspfads „Versionenmanagement“ wirkt generell ein nicht sorgfältiges geplantes und durchgeführtes Versionenmanagement in kerntechnischen Anlagen und Einrichtungen. Hierzu zählen unübersichtliche Verfahren der Versionenspeicherung, des Arbeitsauftragswesens und der Installationsroutinen.

Pfadzwischenschritte

Der Pfad wird zu dem Zeitpunkt eingeleitet, in dem eine neue Version für ein mehrfach installiertes IT-System bereitsteht und von der Anlage in irgendeiner Form bezogen wurde, um langfristig eingesetzt zu werden. In Zwischenschritten kann über die folgenden Verfahren zur Verteilung der neuen Version eben diese Verteilung in einer Form optimiert werden, welche eine schadhafte Wechselwirkung zwischen den gleichen IT-Systemen mit dann unterschiedlichen Versionen erzeugt.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Versionenmanagement“ endet, wenn gleiche IT-Systeme nach Ende von Installations- bzw. Wartungsarbeiten verschiedene Software- (oder seltener) Hardwareversionen besitzen.

Im Rahmen des Einwirkungspfades kann es zu umfassenden Überschneidungen und Übergängen zu weiteren Pfaden kommen. Hierzu zählt Einfluss auf die Parametrisierung im Rahmen der Versionierung und des Arbeitsprozesses sowie der Zugriff auf den Arbeitsprozess selbst. Servicegeräte, welche die Versionen auf IT-Systeme aufspielen, können als Zwischenschritt ebenfalls betroffen sein. Auch die bezogenen Versionen können bereits bei Bezug durch andere Einwirkungen manipuliert werden. Es bestehen also Pfadübergangsmöglichkeiten zu den Einwirkungspfaden „Lieferkette“, „Parametrisierung“ und „Servicegeräte“.

4.2.7.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfads „Versionenmanagement“ sind generell abhängig von den betroffenen Systemen und dem sich aus dem Wechselspiel verschiedener Versionen ergebenden Schadpotenzial. Der wesentliche Aspekt dieses Einwirkungspfads ist eng mit der Frage der generellen Sicherheit von Software- bzw. Hardware-Updates/Modernisierungen bzw. deren Arbeitsprozessen verknüpft.

Real beobachtete Auswirkungen

Im Fall des meldepflichtigen Ereignisses 2016/044 im Kernkraftwerk Biblis gab es keine Auswirkungen auf die Anlage, Personen oder die Umgebung. Die dortige Brandmeldeanlage des Typs Siemens Sigmasys für das Kühlwasserpumpenhaus und das Hilfskesselgebäude wurde im Rahmen der WKP geprüft, hierbei wurde festgestellt, dass insgesamt sieben Brandmeldeleitungen Signale nicht weiterleiteten. Ähnliches wurde bei der Brandmeldeanlage im Verwaltungsgebäude festgestellt. Die betroffenen Baugruppen wurden ausgetauscht, das Problem behoben. Die Untersuchung ergab, dass verschiedene Baugruppen mit verschiedenen Firmwareversionen und sogar Elektronikkomponenten verbaut wurden. Jedoch war dies nicht die Ursache für den Ausfall der Systeme. Vielmehr war ursächlich eine fehlerhafte Programmierung beider Versionsstände, welche unter gewissen Umständen zu fehlerhaften Zuständen der Baugruppen bei Handbefehlen führte.

Potenzielle Auswirkungen

Die potenziellen Auswirkungen des Einwirkungspfades sind abhängig von der Ausgestaltung der betroffenen Systeme. Da über das Versionenmanagement teilweise oder vollständige neue Versionen bestehender Software auf IT-Systeme verteilt werden, sind umfassende Einflussnahmen durch den IT-Einwirkungspfad denkbar. Dazu zählt grundsätzlich jede unerwünschte Handlung eines IT-Systems, dessen Version mittels eines Versionierungs-Systems oder -Verfahrens verwaltet wird.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Versionenmanagement“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen.

Mittels übertragenden Versionen können zum einen falsche Handlungen und Befehle, aber auch Schwachstellen, Softwarefehler sowie Schadsoftware auf betroffene IT-Systeme übertragen werden. Einleitend können hierdurch insbesondere solche IT-Einwirkungspfade angeregt werden, welche grundsätzlich IT-Systeme betreffen, die im Rahmen von Versionenmanagement verwaltet werden:

- IT-Einwirkungspfad „Servicegeräte“: Servicegeräte selbst besitzen einen bestimmten Versionsstand der genutzten Software auf diesen Systemen, dienen aber auch der Verteilung neuer Softwareversionen auf andere IT-Systeme. Hierdurch können Servicegeräte durch den IT-Einwirkungspfad „Versionenmanagement betroffen sein.
- IT-Einwirkungspfad „Wechseldatenträger“: Wechseldatenträger dienen der Speicherung und dem Transport von Daten und werden auch beim Transport von Softwareversionen in Verbindung mit Versionierungssystemen eingesetzt.
- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Der Einsatz neuer Softwareversionen oder gar manipulierter Softwareversionen über ein Versionierungssystem, kann auf betroffenen IT-Systemen bei Auslegungsüberschreitung der bestehenden Rechenkapazitäten der Hardware zu Überlastungen führen.

4.2.7.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Versionenmanagement“ verschiedene mögliche Pfadeinleitungen und kann außerdem zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung auf.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Im Fall von IT-Einwirkungen mittels Versionierungssystemen sind dies insbesondere solche Maßnahmen, welche den Roll-out von neuen Versionen einschränken. Hierzu zählen zeitlich gestaffelte Roll-outs neuer Versionen bei identischen oder quasi-identischen IT-Systemen sowie bei multiredundanten IT-Systemen.

Aufdeckende Faktoren

Versionierungssysteme, die im Rahmen des Versionenmanagement eingesetzt werden, bieten eine Vielzahl von internen Kontrollmöglichkeiten für Anwender an. Dazu gehören z. B. das Aufzeigen von Abweichungen zwischen Neu- und Altversionen und die Auswertung betroffener spezifischer Softwarebereiche. Hierdurch können Fehler innerhalb der Versionen wie auch unerwartete Änderungen identifiziert und damit aufgedeckt werden. In Bezug auf Schadsoftware, welche in Softwareversionen eingepflegt wird, bestehen Möglichkeiten zur Auswertung mittels externer Programme zur Schadsoftwareerkennung.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Versionenmanagement“ wird im Aufdeckungsfall unterbrochen, da bei Kenntnissen fehlerhafter oder manipulierter Softwareversionen ein Roll-out eingestellt wird. Darüber hinaus sind all jene Maßnahmen, die eine Einflussnahme auf die Versionierung blockieren geeignet, den IT-Einwirkungspfad zu unterbrechen bzw. zu unterbinden. Da jedoch neue Softwareversionen von außerhalb der Anlage bezogen werden, können solche Maßnahmen erst z. B. in Rahmen von Testumgebungen und anderen Prüfmaßnahmen wirken.

4.2.7.4 Pfadzusammenfassung Versionenmanagement

Eine der Kernfunktionen von programmierbarer Software ist die Variabilität und die nachträgliche Möglichkeit zur Änderung dieser Software über Updates und neue Versionen. Solche neuen Versionen dienen zum einen der Behebung von Softwarefehlern und Schwachstellen und sind daher essenziell für IT-Systeme, andererseits zur Einführung neuer Funktionen. Letztere sind für den Betrieb von IT-Systemen nicht grundlegend notwendig, neue Funktionen und die Behebung von Softwarefehlern und Schwachstellen werden jedoch häufig mit einem einzelnen Update gleichzeitig vermengt. Versionierungssysteme bieten umfangreiche Möglichkeiten zum Management der bestehenden Softwareversionen von eingesetzten IT-Systemen, zum Abgleich und Analyse neuer Versionen und für die Verbreitung der Versionen. Somit können solche Versionierungssysteme für IT-Eingriffe über das „Versionenmanagement“ als Ziel von schadhaften Einwirkungen dienen und haben, je nach bedienten IT-Systemen, eine potenziell hohe Schadwirkung.

4.2.8 Fernzugriffe

Auf Informationssystemen basierende Arbeiten können bei entsprechender Vernetzung von jedem Ort ausgeführt werden, solange keine aktive Einflussnahme auf die Hardware sondern ausschließlich auf die Software notwendig sind. Sogenannte Remotezugriffe auf IT-Systeme sind in vielen Branchen zum Standard geworden, in dem über weite Entfernungen auf IT-Systeme zugegriffen wird, z. B. für die Wartung, für die Möglichkeit der Heimarbeit oder auch um schnellen Zugriff zu erhalten, ohne den entsprechenden Arbeitsbereich zu betreten. Im kerntechnischen Bereich waren Fernzugriffe bisher entweder gar nicht verbreitet oder nur innerhalb der Anlagennetze möglich. Mit der Umwälzung der Arbeitswelt in Folge der globalen Ausbreitung des SARS-Cov-2 Virus, wurden in vielen Branchen und Bereichen die Möglichkeiten zum Fernzugriff massiv ausgebreitet, um die Ausbreitung des Virus zu stoppen und die Gefahr des Arbeitsausfalls bei Erkrankungen oder Quarantäne zu reduzieren. Diese Ausweitung betrifft auch kerntechnische Anlagen, da diese seit 2020 vermehrt bestimmte Aufgaben, welche als nicht sicherheits- oder sicherungsrelevant angesehen werden, auch über Fernzugriffe bearbeiten lassen.

Bisher liegt kein nationales oder internationales Ereignis vor, in welche Fernzugriffe eine anteilige oder hauptsächliche Rolle spielten. Die SARS-Cov-2 Ausbreitung führt jedoch zu schnellen Umwälzungen, deren Auswirkungen absehbar sind. Der Folgende IT-Einwirkungspfad „Fernzugriff“ basiert daher auf seit dem Jahr 2020 von der GRS gemachten Erfahrungen sowie Erfahrungsaustausche im nuklearen und konventionellen Anwendungsbereichen von Informationssystemen. Hierzu gehören insbesondere Eindrücke und Erfahrungen aus der von der GRS besuchten Konferenz „Cyber Defense Summit 2021“ des Unternehmens Mandiant, welches mit dem Kernthema „Defending the new Normal“ zentral die Risiken und Gefahren aus der stark verbreiteten Nutzung von Fernzugriffen in kritischen Infrastrukturen und Industrien darstellte.

4.2.8.1 Der Einwirkungspfad „Fernzugriffe“

Der IT-Einwirkungspfad „Fernzugriff“ beginnt außerhalb der Grenzen der betroffenen kerntechnischen Anlagen, Fernzugriffverbindungen werden im Normalfall über VPN-Verbindungen vom außerhalb des Netzwerkes befindlichen IT-System über das Internet zu den Servernetzwerken der betroffenen Anlage aufgebaut. Diese Verbindungen können durch unterschiedliche Maßnahmen gesichert werden.

Allerdings sind diese auch selbst potenzielle Angriffspunkte, da sie einerseits klassisch IT-technisch angegriffen werden können und andererseits durch Nutzung bestehender Zugänge und Passwörter ausgenutzt werden können. Wird durch den Fernzugriff eingedrungen, stehen den Angreifern zuerst diejenigen Systeme zur Verfügung, für welche sie mittels des genutzten Zugangs bereits Rechte besitzen. Daraufhin besteht die Möglichkeit innerhalb des bestehenden Netzwerks, weitere eigentlich nicht per Fernzugriff bedienbare IT-Systeme anzugreifen. Die Grenzen der Einwirkung sind erreicht, wenn die Grenzen des zugreifbaren Netzwerks erreicht wurden.

Pfadeinleitung

Der Einwirkungspfad „Fernzugriff“ beginnt außerhalb der kerntechnischen Anlage. Hierzu muss eine Fernzugriffsmöglichkeit innerhalb der kerntechnischen Anlage bestehen. Diese wird im Rahmen des Einwirkungspfades durch Dritte verwendet, um Zugriff auf IT-Systeme der Anlage zu erreichen. Hierzu muss eine Zugriffsmöglichkeit im Rahmen des Fernzugriffs bestehen, also eine Schwachstelle in den benutzten Programmen und Protokollen des Fernzugriffes, eine Schwachstelle im Übergang vom freien Internet zum internen Netzwerk oder aber ein Zugriff auf die genutzten Programme des Fernzugriffs über Passwörter und Benutzererkennungen. Zur Einleitung ist also ein Einfallspunkt notwendig. Verschiedene Einfallspunkte, Schwachstellen usw. erleichtern die Einleitung des Einwirkungspfades.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Fernzugriff“ einzuleiten, ist eine bzw. mehrere folgender Bedingungen zwingend notwendig:

- Die kerntechnische Anlage muss bereits eine Art von Fernzugriff besitzen.
- Es muss mindestens eine Möglichkeit geben, als Einwirkender den Fernzugriff auszunutzen.

Auf eine kerntechnische Anlage, welche keine Form von Fernzugriff ermöglicht, kann nicht über den IT-Einwirkungspfad „Fernzugriff“ zugegriffen werden. Absolut notwendig ist also eine Form von Fernzugriffsmöglichkeit oder zumindest eine Schnittstelle zwischen internen IT-Systemen und dem Internet, welche als Zugriffspunkt dient.

Um per Fernzugriff auf die Anlage zugreifen zu können, muss die regulär bestehende Fernzugriffsinfrastruktur der Anlage einen Schwachpunkt besitzen. Dies können schwach konfigurierte Firewalls sein, Schwachstellen bestehender Netzwerkzugriffssysteme, Schwachstellen eingesetzter Fernzugriffssoftware oder auch bereits bekannte Fernzugriffskonten und Passwörter.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Unterstützend wirkt alles, was die Sicherheit der regulären Fernzugriffe unterminiert. Neben den bereits genannten direkten Zugriffsstellen ist insbesondere das Verhalten der den Fernzugriff nutzenden Mitarbeiter entscheidend. Fernzugriffe über öffentliche oder nicht gesicherte WLANs, unsichere Konfiguration oder Handhabung der für den Fernzugriff gedachten IT-Systeme, wiederholte Nutzung von gleichen Passwörtern und Accountdetails, welche verloren gehen können oder anderweitig gefährdendes Verhalten führt zu einer größeren Angriffsfläche für IT-Einwirkungen über Fernzugriffe.

Pfadzwischenschritte

Nach erfolgreicher Einleitung des IT-Einwirkungspfades „Fernzugriff“ besitzen die Einwirkenden die Kontrolle über mindestens einen Fernzugriff auf IT-Systeme der betroffenen kerntechnischen Anlage. Von hier aus ist eine Verbreitung der Zugriffe erwartbar. Hierzu werden bestehende Netzwerkverbindungen und Schwachstellen genutzt, um mittels Rechteeskalation die Grenzen für Fernzugriffsmöglichkeiten auf einzelnen Systemen zu überwinden und mittels Netzwerkverbreitung auf weitere verbundene IT-Systeme überzugreifen.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Fernzugriffe“ endet mit der Etablierung von Zugriffen auf IT-Systeme der Anlage, unabhängig vom in diesem Zusammenhang genutzten Pfad des Fernzugriffs oder bei Abschluss der operativen Eingriffe durch die Einwirkenden. Hierdurch kann entweder ein langfristig gesicherter Zugriff auf IT-Systeme der Anlage etabliert werden oder aber Schadsoftware auf die betroffenen IT-Systeme übertragen werden. Direkt betroffene IT-Systeme sind zumeist schutzbedürftige verwaltende Systeme, wie generelle Management- und Bürosysteme sowie Betriebsführungssysteme. Von hier aus ist eine potenzielle Weiterverbreitung auf andere IT-Systeme möglich, welche über das Anlagennetzwerk temporär oder dauerhaft verbunden sind.

Entsprechend sind die Pfadübergängen zu weiteren IT-Einwirkungspfaden abhängig von den bestehenden datentechnischen Verbindungen und der Art, wie die Einwirkung stattfand. Es kann zu Interaktionen mit den IT-Einwirkungspfaden „Servicegeräte“, „Leittechnikverbreitung“, „Wechseldatenträger“ und ggf. weiteren kommen.

4.2.8.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfads „Fernwirkung“ sind generell abhängig von den betroffenen Systemen und der Art der potenziellen Schadsoftware. Der wesentliche Aspekt dieses Einwirkungspfads ist eng mit der Frage des generellen Einsatzes von Fernwartungen sowie Fernzugriffen verbunden. Fernzugriffe können und werden insbesondere für verwaltungsrevelante Tätigkeiten und Themen in Bezug auf kerntechnische Anlagen umgesetzt. Ein Einsatz von Fernzugriffen mit leittechnischem Bezug ist bisher nicht bekannt. Jedoch sind direkte und indirekte Verbindungen über das Anlagennetzwerk zu leittechnischen Systemen nicht auszuschließen. Die direktesten Auswirkungen sind daher ein Zugriff auf IT-Systeme im Verwaltungsbereich und damit einhergehender Einfluss auf die Vertraulichkeit von schutzbedürftigen Informationen sowie der Verfügbarkeit und Integrität der betroffenen IT-Systeme. Durch weitere Verbreitung sowie Übergänge auf andere IT-Angriffspfade lassen sich weitere IT-Systeme manipulieren.

Real beobachtete Auswirkungen

Bisher liegen keine Ereignisse bezüglich der Nutzung von Fernzugriffen für IT-Angriffe vor. Die Nutzung von Fernzugriffen hat sich aufgrund der COVID-19 Pandemie auch im Bereich kerntechnischer Anlagen verbreitet. Hierbei sind insbesondere Fernzugriffe auf sicherheitstechnisch weniger relevante Einrichtungen, wie die verwaltende Infrastruktur, bekannt geworden. Im Bereich der kritischen Infrastruktur kam es durch Fernzugriffe bereits zu erheblichen Einwirkungen auf betroffene Anlagen. Insbesondere mit der COVID-19 Pandemie wurden vermehrt Fernzugriffe auch dort etabliert, wo bis Anfang 2020 aufgrund von IT-Sicherheitsbedenken die Möglichkeiten von Fernzugriffen pauschal abgelehnt worden waren. Solche Fernzugriffe benötigen zur Funktionsweise Software zur Einwahl in Anlagennetzwerke oder aber direkten Steuerungszugriff über sogenannte Remote Access Protokolle, wie sie von verschiedenen Entwicklern angeboten werden. In den Jahren 2020 und 2021 sind hierbei mehrere Fälle bekannt geworden, in welchen IT-Angreifer erfolgreich Remote Access Protokolle durch bekannte Zugangsdaten oder Schwachstellen in der Software ausnutzen konnten um kritische Infrastruktur anzugreifen.

Ein Fall war z. B. der Fund eines russischen Remote Access Programms mit permanentem Kontakt auf einen wiederum russischen Server, auf einem Server eines Wasserwerks.

Potenzielle Auswirkungen

Grundsätzlich können IT-Einwirkungen über Fernzugriffe all jene IT-Systeme betreffen, für die die Möglichkeit des Fernzugriffes etabliert wurde. Dies betrifft hauptsächlich IT-Systeme mit verwaltenden Aufgaben. Solche IT-Systeme habe keinen direkten Zugriff auf schutzbedürftige IT-Systeme mit leittechnischen Funktionen, können aber schutzbedürftige Informationen verarbeiten oder über das Anlagennetzwerk mit weiteren schutzbedürftigen IT-Systemen verbunden sein. Mit der direkten Einwirkung kann somit eine gewisse Anzahl von sicherungs- und sicherheitsrelevanten IT-Systemen beeinflusst werden. Ein Beispiel ist z. B. das Betriebsführungssystem (BFS). So kann ein erhebliches Interesse bestehen das BFS mit Fernzugriffen für die Mitarbeiter auszustatten, um die notwendigen verwaltungstechnischen Aspekte der Betriebsführung von außerhalb der Anlage erledigen zu lassen, z. B. aus gesundheitstechnischen Gründen in der COVID-19 Pandemie oder aus Gründen des Komforts für die Arbeitnehmer. Über das BFS werden jedoch sicherheits- und sicherungsrelevante Tätigkeiten organisiert, sodass eine Manipulation des BFS Einwirkungen auf sicherheits- und sicherungstechnisch relevante Einrichtungen haben kann.

Generell bestehen durch die Vernetzungsmöglichkeiten IT-Systemeinwirkungen auf weitere IT-Systeme, welche nicht direkt durch die Fernwartung bzw. Fernzugriff betroffen sind. Da Updates und Daten teilweise aus dem freien Internet bezogen werden müssen, bestehen solche Verbindungen auch zu IT-Systemen, welche normalerweise nicht mit dem Anlagennetzwerk verbunden sind, z. B. über Wechseldatenträger oder Servicegeräte. Hier kommt es dann zu einem Pfadübergang. Die Einwirkung ermöglicht dabei Einfluss auf Verfügbarkeit, Vertraulichkeit und Integrität von betroffenen IT-Systemen.

Die IT-Einwirkung über Fernzugriffe ermöglicht somit insgesamt eine umfassende Einwirkung über das Gerät hinaus auf sicherheits- und sicherungsrelevante IT-Systeme. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Fernzugriffe“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen. Über Fernwartungen oder Fernzugriffe, die manipuliert wurden oder unter Kontrolle von Dritten gebracht wurden, kann Schadsoftware in kerntechnische Anlagen und Einrichtungen gelangen, insbesondere auf direkt mit der Außenwelt verbundene IT-Systeme sowie mit dem Anlagennetzwerk verbundene IT-Systeme. Air-Gaps können durch temporäre Verbindungen durch Wechseldatenträger oder Servicegeräte überbrückt werden. Der Einwirkungspfad „Fernzugriff“ kann einleitend für bzw. übergreifend auf folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „Servicegeräte“: Servicegeräte können potenziell mit Geräten verbunden werden, die vom IT-Einwirkungspfad Lieferkette betroffen sind - beispielsweise im Rahmen eines Softwareupdates (auch eines potenziell manipulierten Softwareupdates selbst). Dadurch kann sich die Schadsoftware potenziell weiterverbreiten und je nach Einsatz des Servicegeräts weitere Systeme und Netzwerke infizieren.
- IT-Einwirkungspfad „Wechseldatenträger“: Wechseldatenträger können potenziell mit Geräten verbunden werden, die vom IT-Einwirkungspfad Lieferkette betroffen sind – beispielsweise im Rahmen der Erstellung eines Backups. Dadurch kann sich die Schadsoftware potenziell weiterverbreiten und je nach Einsatz des Wechseldatenträgers weitere Systeme und Netzwerke infizieren.

4.2.8.3 Pfadblockierende Faktoren

Die zentralen Pfadeinleitungen für den IT-Einwirkungspfad „Fernwirkung“ sind zum einen die Möglichkeit der Nutzung von bekannten bzw. ausgespähten Anmeldeinformationen bestehender Fernwartungs- und Fernbedienungssysteme sowie die Ausnutzung von Schwachstellen dieser implementierten Systeme. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung auf.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Je geringer die Nutzung von Fernzugriffen, desto geringer ist die Möglichkeit der Nutzung von Fernzugriffen durch Dritte. Weiterhin können Mehrfaktor-Sicherungsmaßnahmen bei der Mitigation der maliziösen Nutzung von Fernzugriffen durch Dritte eine zentrale mitigierende Rolle spielen. Werden jedoch Schwachstellen innerhalb der eingesetzten Fernzugriffssoftware ausgenutzt, können solche Sicherungsmaßnahmen überwunden werden.

Aufdeckende Faktoren

IT-Einwirkungen über Fernzugriffe aufzudecken ist insbesondere möglich durch die Überwachung des sich aus den Fernzugriffen ergebenden Netzwerkverkehrs. Weicht dieser deutlich von bisher erfahrenem Netzwerkverkehr ab, z. B. durch ein stark erhöhtes Volumen oder gehäufte Zugriffe auf selten zugegriffene IT-Systeme bzw. Daten, dann kann dies automatisch oder manuell erkannt werden und entsprechende Untersuchungen eingeleitet werden. Dies gilt auch bei wechselndem Nutzerverhalten, z. B. entgegen den Gewohnheiten häufig wechselnden IP-Adressen der zugreifenden, Zuordnung der Nutzer-IP-Adressen zu anderen Regionen als dem typischen Standort des Nutzers und untypisches Nutzungsverhalten in Bezug auf Abfragen und Zugriffen.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Fernzugriffe“ kann insbesondere durch die Abschaltung bestimmter Fernzugriffsfunktionen direkt und aktiv unterbrochen werden. Hierzu zählt die Abschaltung sowohl allgemeiner Fernzugriffsmöglichkeiten wie auch die Abschaltung spezifischer verdächtiger Zugriffskonten und die Entziehung von Zugriffsberechtigungen auf spezifische IT-Systeme und Funktionen. Darüber hinaus kann die Behebung von Schwachstellen und fehlerhaften Konfigurationen mögliche IT-Einwirkungen über Fernzugriffe dauerhaft unterbinden.

4.2.8.4 Pfadzusammenfassung Fernzugriff

Der IT-Einwirkungspfad „Fernzugriff“ ist unter den beschriebenen Gesichtspunkten als mittelschwerer Einwirkungspfad mit insbesondere Einwirkungsmöglichkeiten im administrativen Bereich anzusehen.

Die Einwirkungen können bei Zugriff auf Anmeldedaten oder Zugriffspunkte für den etablierten Fernzugriff oftmals unentdeckt bleiben oder nur durch aufwendige Analyse des Netzwerkverkehrs aufgedeckt werden. Zusätzlich ergeben sich durch die direkten Zugriffe mittels Fernwirkung zahlreiche weitere Übergänge auf andere IT-Einwirkungspfade. Die möglichen Auswirkungen des Einwirkungspfades sind abhängig von den bestehenden Möglichkeiten des etablierten Fernzugriffes. Diese Möglichkeiten werden national und international insbesondere unter dem Hintergrund der COVID-19 Pandemie und der sich schnell ändernden Arbeitswelt kontinuierlich weiter erörtert und ausgebaut. Bisher ist kein meldepflichtiges Ereignis bezüglich Fernzugriffen bekannt geworden, jedoch kam es mit der COVID-19 Pandemie zu einer massiven Verschärfung von IT-Einwirkungen durch Fernzugriffe auf konventionelle Anlagen der kritischen Infrastruktur.

Durch erweiterte Sicherheitsmaßnahmen, umfassende Überwachung der Kommunikation, besondere Beachtung von Schwachstellen der eingesetzten Software und Nutzung von Mehrfaktor-Authentifizierungen können die Möglichkeiten zur Einwirkung über Fernzugriffe reduziert werden.

4.2.9 Parametrierung und Konfiguration

Analoge wie digitale Hardware sowie generell auch Software sind in der Regel parametrier- bzw. konfigurierbar, wobei die Parametrierung und Konfiguration im Herstellungsprozess erfolgen können, bei der (Erst-)Einrichtung oder auch im laufenden Betrieb, beispielsweise im Rahmen von Wartungsarbeiten oder Updates. Neben funktionalen Aspekten können auch sicherheitsrelevante Funktionen und Grenzwerte durch Parameterbeeinflussung oder eine bewusst oder unbewusst falsch gewählte Konfiguration manipuliert werden, sodass beispielsweise Abläufe oder Prozesse gestört, gestoppt, oder fehlerhaft ausgelöst werden können. Dabei können Eingaben von Parametern oder Konfigurationen prinzipiell am Gerät bzw. in der Software selbst ohne weitere Hilfsmittel einstellbar sein, oder mit zusätzlicher Hard- oder Software beispielsweise in Form von Service-Geräten vorgenommen werden.

In den vergangenen Jahren gab es sowohl national als auch international Vorfälle in kerntechnischen Anlagen und Einrichtungen, bei denen eine fehlerhafte Parametrierung oder Konfiguration vorlag und zu entsprechenden Ausfällen führte.

Die betroffenen Komponenten können prinzipiell in sämtlichen Systemen einer Anlage vorliegen, die konfigurier- bzw. parametrierbar sind. In deutschen Anlagen kam es durch fehlerhafte Konfigurationen bzw. Parametrierungen bereits zu Beeinträchtigungen in Systemen der Aktivitätsüberwachung, der Brandmeldeanlage und einer Krananlage. International waren bereits leittechnische Systeme betroffen. Bei den vorliegenden Fällen handelte es sich nach aktuellem Kenntnisstand um versehentliche bzw. unbeabsichtigte menschliche Fehler in der Konfiguration/Parametrierung und nicht um gezielte Manipulationen oder Einflussnahmen.

4.2.9.1 Der Einwirkungspfad „Parametrierung und Konfiguration“

Der Einwirkungspfad „Parametrierung und Konfiguration“ umfasst Parameter- bzw. Konfigurationseinstellungen, mit denen der Betrieb eines (Teil-)Systems eingeschränkt bzw. gestört, verhindert, außerplanmäßig eingesetzt oder anderweitig manipuliert werden kann. Der Einwirkungspfad kann alle Systeme und Bereiche betreffen, in denen parametrierbare oder konfigurierbare Systeme eingesetzt sind. Das umfasst sowohl reguläre Bürohardware wie auch sicherheits- und sicherungsrelevante Systeme, sodass die potenziellen Auswirkungen des Einwirkungspfades breit angelegt sind. Eine potenzielle Einflussnahme kann zudem prinzipiell bei der oder auch vor der (ersten) Installation eines Systems erfolgen oder aber im laufenden Betrieb bzw. bei Wartungsarbeiten.

Pfadeinleitung

Der Einwirkungspfad „Parametrierung und Konfiguration“ hat mehrere mögliche Ausgangspunkte. Ähnlich wie im Einwirkungspfad „Lieferkette“ ist es möglich, dass Hard- oder Softwarekomponenten bereits bei der Installation mit entsprechend eingestellten oder manipulierten Parametern konfiguriert werden oder bereits wurden. Modifizierungen eines bestehenden Systems in Form von Modernisierungen, Erweiterungen oder sonstigen Änderungen bieten zudem in diesem Zusammenhang pfadeinleitende Faktoren. Dies umfasst sowohl die Installation neuer Komponenten als auch mögliche schädliche Maßnahmen, die an der Parametrierung bzw. Konfiguration von bestehenden Komponenten vorgenommen werden, die aufgrund von Änderungen an Systemen vorgenommen werden müssen. Beispielsweise kam es beim meldepflichtigen Ereignis 2012/066 bei der Brandmeldeanlage zu Beeinträchtigungen, da aufgrund der Nachrüstung mehrerer Brandmelder eine Neuparametrierung des Systems erfolgte.

Hier führten menschliche Fehler während der Durchführung dazu, dass die Brandmeldeunterzentrale einzelne Melder nicht erkannte und es zu fehlerhaften Schließfunktionen von Brandschutztüren kam. Neben einer potenziellen Pfadeinleitung bei der Installation von (neuen) Komponenten kann der Einwirkungspfad „Parametrierung und Konfiguration“ auch bei seit längerem unverändert bestehenden Systemen eingeleitet werden. Beispielsweise, wenn im Rahmen von wiederkehrenden Prüfungen oder Funktionsprüfungen, Änderungen an der Parametrierung oder Konfiguration vorgenommen werden. Beim meldepflichtigen Ereignis 2015/007 kam es in diesem Zusammenhang beispielsweise aufgrund einer Fehlinterpretation und nicht ausreichender technischen Klärung bei einer wiederkehrenden Prüfung der Aerosolaktivitätsmessstellen zu einer fehlerhaften Änderung ursprünglich eingestellter Parameter und dadurch schließlich zu fehlerhaft bestimmten Konzentrationsberechnungen einer Aerosolmesstelle. Generell ist auch eine Pfadeinleitung ohne spezielle Ereignisse möglich, indem potenzielle Angreifer vor Ort oder über datentechnische Verbindungen von außerhalb Parameter bzw. Konfigurationen von Systemen beeinflussen.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Parametrierung und Konfiguration“ einzuleiten, sind eine bzw. mehrere folgender Bedingungen zwingend notwendig:

- Existenz einer möglichen Parametrierung oder Konfiguration für sicherheits- oder sicherungstechnisch relevante Systeme und Funktionen einer kerntechnischen Anlage
- Existenz einer möglichen Parametrierung oder Konfiguration für Systeme mit Verbindung zu sicherheits- oder sicherungstechnisch relevanten Systemen einer kerntechnischen Anlage

Sobald Systeme existieren, die parametrier- oder konfigurierbar sind, ist der der Einwirkungspfad „Parametrierung und Konfiguration“ für IT-Angriffe prinzipiell vorstellbar. Dabei kann es sich um Software und/oder Hardware handeln. Sollte die Parametrierung bzw. Konfiguration nicht direkt an der betroffenen Komponente selbst vorgenommen werden können, werden in der Regel Servicegeräte für die entsprechende Einrichtung benutzt. Dadurch ergibt sich eine enge Verbindung zum IT-Einwirkungspfad „Servicegeräte“. Zur Pfadeinleitung ist es nicht zwingend erforderlich, dass eine Änderung der Parametrierung oder Konfiguration vorgesehen ist.

Der Pfad kann auch durch eine getarnte oder unbemerkt vorgenommene Parametrierung/Konfiguration eingeleitet werden, die im Rahmen anderer Arbeiten an IT-Systemen vorgenommen wird oder gänzlich unabhängig davon.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Als unterstützende Faktoren zur Einleitung des Einwirkungspfades „Parametrierung und Konfiguration“ gelten generell das nicht Einhalten oder Fehlen von Sicherungsvorschriften, wozu auch mangelhafte Untersuchungen potenzieller Auswirkungen falscher Eingaben/Parametrierungen zählen. Zu diesem Aspekt wurden bereits Ereignisse gemeldet, in denen beispielsweise eine Fehlinterpretation vorlag und eine technische Klärung nicht ausreichend durchgeführt wurde. Wird die Einordnung möglicher Gefahren, die von einer geänderten Parametrierung und Konfiguration ausgehen, verglichen mit anderen Einwirkungspfaden wie dem Anschluss von Wechseldatenträgern oder Servicegeräten als geringer wahrgenommen, kann sich eine Sorglosigkeit einstellen, welche die unterstützenden Aspekte menschlicher Fehlhandlungen dieses Einwirkungspfades unterstreicht.

Zudem gelten erweiterte Zugriffsmöglichkeiten als unterstützender Faktor, beispielsweise in Form von vorhandenen Konfigurationsmöglichkeiten, die für den Betrieb nicht erforderlich sind oder darüber hinaus gehen. Dies kann beispielsweise bei serienmäßigen IT-Systemen der Fall sein, die nicht speziell für das Aufgabengebiet in den entsprechenden Anlagen konzipiert und entwickelt wurden und somit angepasst bzw. ggf. in ihrem Funktionsumfang eingeschränkt werden müssen. Dieses Beispiel geht einher mit möglichen mangelhaften Informationen eines Herstellers über Produkte oder Produktfunktionen, was eine Verbindung zum IT-Einwirkungspfad „Unerkannte IT-Komponente“ darstellen kann.

Unterstützend können außerdem Anschlüsse von Wechseldatenträgern oder Servicegeräten wirken, die potenziell Schadsoftware übertragen und somit die Gelegenheit bieten, Parametrierungen oder Konfigurationen von isolierten Systemen ohne datentechnische Verbindungen zur Außenwelt zu manipulieren.

Pfadzwischenschritte

Die weiteren Pfadzwischenschritte sind durch die direkten Auswirkungen von Manipulationen von Parametrierungen und Konfigurationen eher eingeschränkt, jedoch abhängig von den Verbindungen des Systems und der allgemeinen Architektur.

Auch der Ausgangspunkt der Einwirkung ist relevant für mögliche weitere Schritte. Im Beispiel der fehlerhaften Parametrierung innerhalb der Brandmeldeanlage ist die Beeinflussung einzelner Unterabschnitte oder zentraler Einheiten denkbar, sodass beispielsweise nur gewisse Teile oder weite Abschnitte betroffen sind. Durch Über- oder Unterschreitung von manipulativ gesetzten Grenzwerten können Systeme blockiert werden oder durch fehlerhafte Parametrierung gänzlich aus der Überwachung entfernt werden. Damit würde der Einwirkungspfad entsprechend enden. Dadurch könnten wiederum weitere Systeme oder Abschnitte betroffen sein, sodass weitere Schritte möglich sind.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Parametrierung und Konfiguration“ endet mit der Manipulation von Parametern oder der Konfiguration eines Systems. Dies kann, je nach den genauen Umständen mehrere Folgen haben. Einzelne Systeme können beispielsweise gezielt durch Unter- oder Überschreitung von Grenzwerten beeinflusst werden. Außerdem könnten Systeme oder Abschnitte aus der Überwachung entfernt werden oder die gesamte Funktionalität eingeschränkt werden, sodass ein Betrieb nicht mehr möglich ist. Die möglichen Pfadübergänge sind abhängig von den bestehenden datentechnischen Verbindungen. Obwohl durch die Eingabe falscher Parameter oder Konfigurationsdaten in der Regel eher das eigentliche System betroffen ist, bei dem dieser Eingriff stattfand, können auch weitere Systeme betroffen sein, die datentechnische Verbindungen haben oder beispielsweise über Wechseldatenträger verbunden sind. Es kann zu Interaktionen zu den IT-Einwirkungspfaden „Überlastung von IT-Systemen“ kommen, wenn beispielsweise ein System so konfiguriert wird, dass es eine Vielzahl an Meldungen oder Verbindungsversuchen durchführt. Weitere mögliche Pfadübergänge sind für die IT-Einwirkungspfade „Servicegeräte“ oder „Wechseldatenträger“ denkbar, beispielsweise in Form von einer schadsoftwarebehafteten Konfigurationsdatei.

4.2.9.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfads „Parametrierung und Konfiguration“ sind generell abhängig von den betroffenen Systemen und insbesondere deren Aufbau. Abhängig davon können einzelne Komponenten, (Teil-)Systeme oder auch mehrere Systeme betroffen sein. Die Auswirkungen können beispielsweise einzelne Ausfälle sein oder auch ein weiterer Betrieb betroffener Systeme mit eingeschränkter Funktionalität, die im ungünstigsten Fall nicht oder nicht direkt bemerkt wird.

Real beobachtete Auswirkungen

Es wurden bisher mehrere Ereignisse im Zusammenhang mit dem Einwirkungspfad „Parametrierung und Konfiguration“ gemeldet, bei denen unterschiedliche Auswirkungen beobachtet wurden.

Im Fall des meldepflichtigen Ereignisses 2012/066 kam es zur Unverfügbarkeit der automatischen Schließanregung von Brandschutztüren aufgrund einer fehlerhaften Parametrierung, bei der aufgrund einer Nachrüstung zusätzlicher Brandmelder die Brandmeldeunterzentrale neu parametriert werden sollte und durch menschliche Fehler die Parametrierung nicht korrekt durchgeführt wurde. Die real beobachtete Auswirkung war in diesem Fall der Ausfall der automatischen Schließfunktion der betroffenen Brandschutztüren über zugeordnete Brandmelder.

Beim meldepflichtigen Ereignis 2015/007 kam es, durch eine aufgrund einer Fehlinterpretation und nicht ausreichenden technischen Klärung bei wiederkehrenden Prüfungen der Aerosolaktivitätsmessstellen durch einen Techniker, zu einer fehlerhaften Änderung eines Parameters. Dadurch wurde ein Grenzwert eines Volumenstroms der Aerosolmesstelle fehlerhaft erhöht und der beobachtete Volumenstrom, der über dem früheren, korrekt eingestellten Messwert lag, verursachte keine Meldung, weil der Grenzwert fehlerhaft erhöht wurde. Die Aufgabe der Messeinrichtung ist die Anzeige, Protokollierung und Alarmierung bei Grenzwertüberschreitungen, was in diesem Fall nicht erfolgte. Dies hatte letztlich die Auswirkung, dass von den betroffenen Filterkanälen abgeleitete Werte für die Aerosolaktivitätskonzentration in der Kaminfortluft nicht verfügbar waren.

Das meldepflichtige Ereignis 2015-503 umfasst abweichende Parameter, die bei der wiederkehrenden Prüfung einer Krananlage entdeckt wurden und durch eine fehlerhafte Projektierung bzw. Umsetzung der Funktionen der Steuerung verursacht wurde. Betroffen waren Parameter und die Programmierung der Steuerung, die Bremszeiten und die Richtungsüberwachung des Haupthubwerkes sowie eine nicht umgesetzte Schlüsselschalter-Quittierung, wobei eine Untersuchung ergab, dass die festgestellten Abweichungen keinen direkten Einfluss auf die zurückliegenden Behälterhandhabungen aufwiesen.

Bei dem der IRS-Meldung 8671 zugrundeliegenden Ereignis kam es international zu einer Unverfügbarkeit der Bedienstationen der rechnerbasierten Informations- und Steuerungssysteme, was aufgrund eines fehlerhaft programmierten Parameters geschah. Die Unverfügbarkeit hielt wenige Minuten an.

Potenzielle Auswirkungen

Die potenziellen Auswirkungen des IT-Einwirkungspfades „Parametrierung und Konfiguration“ sind abhängig vom betroffenen System, der Art der Einwirkung und von potenziellen Verbindungen zu anderen Systemen. Da in der Regel sehr viele IT-Systeme in allen Anlagenbereichen parametrierbar bzw. konfigurierbar sind, gibt es eine Vielzahl möglicher potenzieller Einwirkungen auf verschiedenen Systeme. Prinzipiell können IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein, die sicherheits- und sicherungstechnisch relevant sind, was schwerwiegende sicherheits- und sicherungstechnische Auswirkungen haben kann.

Durch eine Manipulation der Parameter oder Konfiguration eines IT-Systems lassen sich beispielsweise bestimmte Teilsysteme oder Komponenten von IT-Systemen unbemerkt deaktivieren. Im Fall der betroffenen Brandmeldeanlage lassen sich unter Umständen durch eine absichtlich oder ungewollt falsche Parametrierung zentraler Einrichtungen einzelne Abschnitte deaktivieren, sodass es im Anforderungsfall nicht oder nur verzögert zu den nötigen automatisierten Brandschutzmaßnahmen (z B. Schließen von Brandschutztüren) kommt und sich ein mögliches Feuer auf weitere Bereiche ausbreitet. Die Manipulation von IT-Systemen über die Parametrierung oder Konfiguration kann auch die direkte Funktionsfähigkeit von Komponenten oder IT-Systemen beeinträchtigen, sodass eine Funktion unverfügbar ist oder nicht entsprechend der Auslegung ausgeführt werden kann. Dies kann prinzipiell alle konfigurierbaren Systeme betreffen, beispielsweise industrielle Steuerungssysteme.

Neben der Unverfügbarkeit einzelner Komponenten, Teilsysteme oder Systeme, können potenzielle Auswirkungen des IT-Einwirkungspfads „Parametrierung und Konfiguration“ auch Manipulationen von Prozessen oder Funktionen laufender Systeme umfassen. So können sicherheitsrelevante Prozesse bzw. Grenzwerte manipuliert werden, sodass entweder Schutzaktionen unbeabsichtigt ausgelöst werden, um den Betrieb von (Teil-)Systemen oder der Anlage zu stören, oder dass Schutzaktionen durch eine entsprechende Manipulation von Grenzwerten nicht oder erst später erreicht werden.

Bei Krananlagen könnten beispielsweise Grenzwerte für Geschwindigkeiten oder Bremszeiten manipuliert werden, sodass es zu schweren sicherheitstechnisch relevanten Vorfällen kommen kann. Dabei sind die betroffenen IT-Systeme weiterhin verfügbar und eine Manipulation geschieht möglicherweise unbemerkt, sodass ein potenzieller IT-Angriff zunächst unerkannt bleibt. So können beispielsweise auch Aktivitätsmessstellen oder Bilanzierungseinrichtungen manipuliert werden, sodass vermeintlich niedrigere Aktivitäten vorliegen. Eine Aufdeckung der Manipulation könnte in so einem Fall ggf. über den Vergleich mit redundanten Einrichtungen durchgeführt werden. Diese Art der Einwirkung kann entsprechend besonders schwer zu bemerken sein, weil beispielsweise Antiviren-Programme bei einer reinen manuellen Manipulation von Parametern keine verdächtigen Aktivitäten bemerken und auch Techniker gezielt einzelne Systeme prüfen müssten, da keine offensichtliche Fehlfunktion vorliegt. Radiologische Messeinrichtungen eines Kernkraftwerks gehören zu sicherheitstechnisch wichtigen Einrichtungen. Bei Überschreitungen von entsprechenden Grenzwerten werden in der Regel Alarme ausgelöst, die ein frühzeitiges Erkennen und Einleiten von Gegenmaßnahmen ermöglichen sollen, was im Fall von manipulierten Grenzwerten zu keinen Alarmen bzw. Alarmen bei höheren Werten führen würde. Potenziell ist somit bei der Veränderung derartiger Parameter der Aktivitätsmessung eine erhöhte Strahlenbelastung bzw. unbemerkte Kontamination denkbar.

Die Manipulation der Parametrierung bzw. Konfiguration ermöglicht somit insgesamt eine umfassende Einwirkung auf eine Vielzahl sicherheits- und sicherungsrelevanter IT-Systeme mit diversen potenziellen Auswirkungen. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Parametrierung und Konfiguration“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen. Da viele Systeme parametriert oder konfiguriert werden können, gibt es diverse potenzielle IT-Angriffsmöglichkeiten in verschiedenen Bereichen und Systemen. Die Einwirkung dieses IT-Einwirkungspfades kann entweder direkt am IT-System selbst erfolgen oder aber über externe Systeme bzw. Servicegeräte und Wechseldatenträger. Der Einwirkungspfad „Parametrierung und Konfiguration“ kann somit einleitend für bzw. übergreifend auf folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Eine Manipulation der Parametrierung oder Konfiguration eines IT-Systems kann zur Überlastung des betroffenen Systems oder verbundener Systeme führen, beispielsweise indem Grenzwerte so manipuliert werden, dass dauerhaft sehr viele Meldungen zur Unter- oder Überschreitung erzeugt werden und so das empfangende System überlastet wird.
- IT-Einwirkungspfad „Servicegeräte“: Die Parametrierung bzw. Konfiguration von IT-Systemen wird häufig mit Servicegeräten durchgeführt, die dazu mit einem IT-System verbunden werden. Umgekehrt kann über diese Verbindung auch die Manipulation der Parametrierung oder Konfiguration dazu genutzt werden, auf ein angeschlossenes Servicegerät einzuwirken. Wird das Servicegerät an mehreren IT-Systemen benutzt, besteht das Risiko der Einwirkung auf die entsprechenden Systeme.
- IT-Einwirkungspfad „Wechseldatenträger“: Wechseldatenträger können potenziell mit Geräten verbunden werden, die vom IT-Einwirkungspfad „Parametrierung und Konfiguration“ betroffen sind – beispielsweise im Rahmen der Erstellung eines Backups. Dadurch kann sich die Schadsoftware potenziell weiterverbreiten und je nach Einsatz des Wechseldatenträgers weitere Systeme und Netzwerke infizieren.
- IT-Einwirkungspfad „Netzwerkverbindung“: Über Netzwerkverbindungen lassen sich bei parametrierbaren bzw. konfigurierbaren IT-Systemen mit entsprechenden Verbindungen weitere Angriffsschritte durchführen.

4.2.9.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Parametrierung und Konfiguration“ verschiedene mögliche Pfadeinleitungen und kann außerdem zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung auf.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Im Falle des IT-Einwirkungspfades „Parametrierung und Konfiguration“ ist dazu zunächst die Einschränkung von Benutzer- und Zugriffsrechten bzgl. der Parametrierung und Konfiguration der betroffenen IT-Systeme zu nennen.

Idealerweise ist der Zugriff entsprechend durch technische Maßnahmen (z. B. Passwort) geschützt, sodass nur Benutzer mit Administratorrechten überhaupt Parameter ändern können. Außerdem kann zur Mitigation des IT-Einwirkungspfads „Parametrierung und Konfiguration“ bei der Beschaffung und Installation von Systemen und Komponenten bereits darauf geachtet werden, dass nur für den Betrieb notwendige Konfigurations- und Parametrierungsmöglichkeiten implementiert sind.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die Aufnahme von Gegenmaßnahmen und im Idealfall die sofortige Beendigung eines IT-Einwirkungspfades. Wird eine Einwirkung entdeckt, kann der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen werden. Im Fall des IT-Einwirkungspfads „Parametrierung und Konfiguration“ können gängige Maßnahmen zur Aufdeckung wie beispielsweise Virenscans nur bedingt erfolgreich durchgeführt werden. Sollten Konfigurationsdateien oder Ähnliches mit Schadsoftware behaftet sein, sind solche Virenscans geeignet, um die Einwirkung aufzudecken. Allerdings werden beispielsweise manuelle Manipulationen von Parametern oder Konfigurationen dadurch nicht erkannt. Solche Einwirkungen können durch einen Abgleich der aktuellen Parametrierung und Konfiguration mit dokumentierten Vergleichswerten bzw. Herstellerunterlagen erkannt werden. Außerdem kann die Überprüfung von Zugriffs- bzw. Logdateien zur Aufdeckung beitragen, indem (unbefugte) Zugriffe oder Änderungen erkannt werden. Zudem können regelmäßig durchgeführte wiederkehrende Funktionsprüfungen Beeinträchtigungen der Funktionalität in Folge von IT-Einwirkungen über die Parametrierung oder Konfiguration eines IT-Systems aufdecken.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Parametrierung und Konfiguration“ wird immer dann unterbrochen, wenn eine Aufdeckung stattfindet und darauf eine entsprechende anforderungsgemäße Reaktion veranlasst wird. Zudem findet eine Unterbrechung statt, wenn Änderungen der Parametrierung oder Konfiguration softwareseitig deaktiviert sind bzw. nicht vorgenommen werden können. Außerdem bieten administrative Regelungen bezüglich des Umgangs mit diesen Systemen, Zugriffskontrollen und ggf. Unterbringungsschutz, die Möglichkeit Einwirkungen zu unterbrechen.

4.2.9.4 Pfadzusammenfassung Parametrierung und Konfiguration

Der IT-Einwirkungspfad „Parametrierung und Konfiguration“ kann unter den beschriebenen Gesichtspunkten als mittelschwerer Einwirkungspfad angesehen werden. Es gibt national und international bereits einige gemeldete Ereignisse, die auf eine fehlerhafte Parametrierung/Konfiguration zurückzuführen sind. Die Pfadeinleitung kann sowohl direkt und manuell am IT-System beginnen oder in Kombination mit anderen IT-Einwirkungspfaden wie „Servicegeräte“ oder „Lieferkette“. Neben einer direkt ersichtlichen Einflussnahme sind auch zunächst unbemerkte Schritte oder Manipulationen denkbar, die zunächst unerkannt bleiben. Bei den bisher beobachteten Auswirkungen handelt es sich um die fehlerhafte Kalibrierung eines Systems zur Aktivitätsüberwachung, den Teilausfall von Komponenten einer Brandschutzanlage, eine fehlerhafte Parametrierung einer Krananlage und den Ausfall eines Steuerungssystems. Es handelte sich in diesen Fällen nach aktuellem Kenntnisstand nicht um gezielte Einwirkungen, sondern unbeabsichtigte menschliche Fehlhandlungen. Die potenziellen Pfadauswirkungen sind vielfältig, da in der Regel sehr viele IT-Systeme in allen Anlagenbereichen parametrierbar bzw. konfigurierbar sind, sodass prinzipiell IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein können, die sicherheits- und sicherungstechnisch relevant sind, was schwerwiegende sicherheits- und sicherungstechnische Auswirkungen haben kann. Folgen können sowohl unmittelbare Ausfälle oder Manipulationen von Komponenten oder Systemen sein, wie auch zunächst unbemerkte Einflussnahmen, die längerfristig einzelne Bereiche oder Funktionen manipulieren. Zu den pfadblockierenden Faktoren zählen hauptsächlich aufdeckende Faktoren wie beispielsweise die Überprüfung von Parametrierungen und Konfigurationen, die im Anschluss unterbrechende Maßnahmen zur Folge haben, aber auch mitigierende Faktoren wie beschränkte Zugriffs- und Benutzerrechte.

4.2.10 Netzwerkverbindungen

IT-Systeme in kerntechnischen Anlagen und Einrichtungen sind in der Regel derartig angelegt, dass es möglichst wenige oder keine Verbindungen zwischen verschiedenen Systemen gibt bzw. von einzelnen Systemen in die „Außenwelt“. Dies dient als Vorsichtsmaßnahme, um den möglichen Schaden bei der Kompromittierung eines Systems möglichst gering zu halten und entsprechend weitere Systeme nicht zu gefährden. Solche isolierten Systeme werden auch als „Inselsysteme“ bezeichnet, da sie möglichst keine Verbindungen außerhalb ihres Systems nach außen besitzen.

Dennoch ist für einige IT-Systeme eine Verbindung zu anderen Systemen erforderlich. Beispielsweise sind einige IT-Systeme der Anlagensicherung in bestimmten Bereichen (z. B. Gefahrenmeldeanlage) auf eine Verbindung zwischen Komponenten oder zu anderen IT-Systemen angewiesen. IT-Systeme können in Zonen zusammengefasst werden oder aber auch über Zonengrenzen hinweg kommunizieren. Zudem gibt es innerhalb eines einzelnen IT-Systems in der Regel auch datentechnische Verbindungen zwischen einzelnen Komponenten, wenn das IT-System nicht nur aus einer einzelnen, abgeschlossenen Komponente besteht. Netzwerkverbindungen bzw. datentechnische Verbindungen verbinden somit Komponenten oder IT-Systeme miteinander und können prinzipiell für IT-Einwirkungen missbraucht werden.

Es wurden bereits Ereignisse gemeldet, bei denen datentechnische bzw. Netzwerkverbindungen eine Rolle gespielt haben. In deutschen Kernkraftwerken kam es bereits zu IT-Sicherheitsvorfällen, bei denen IT-Systeme mutmaßlich über Netzwerkverbindungen mit Schadsoftware befallen bzw. der Schadsoftwarebefall ausgebreitet wurde, nachdem die IT-Systeme ursprünglich über andere IT-Einwirkungspfade (Lieferkette und Wechseldatenträger) infiziert wurden. Dabei beschränkte sich die Ausbreitung der Schadsoftware nach aktuellem Kenntnisstand auf die betroffenen IT-Systeme bzw. einzelne Komponenten, in diesen Fällen das Personenkontrollsystem als Teil der Anlagensicherung und die BE-Lademaschine. Zudem kam es in einem deutschen Versuchskraftwerk zu einem Ereignis, bei dem die Kommunikationskette der Gefahrenmeldeanlage unterbrochen wurde, in dem versehentlich fälschlicherweise ein Kabel getrennt wurde, sodass Störungsmeldungen nicht mehr angezeigt wurden.

4.2.10.1 Der Einwirkungspfad „Netzwerkverbindungen“

Der Einwirkungspfad „Netzwerkverbindung“ basiert auf datentechnischen bzw. Netzwerkverbindungen von IT-Systemen untereinander oder einzelnen Komponenten innerhalb von isolierten IT-Systemen. Liegen Verbindungen zu IT-Systemen vor, die permanent oder temporär Verbindungen zur Außenwelt haben, kann über diesen IT-Einwirkungspfad prinzipiell ein IT-Angriff auch von außerhalb durchgeführt werden (siehe IT-Einwirkungspfad „Fernzugriff“). Generell ermöglicht dieser IT-Einwirkungspfad weitere Manipulationen, auch wenn der ursprüngliche IT-Angriff mit einem anderen IT-Einwirkungspfad beginnt. Es gibt somit weitreichende Überschneidungen, weil bei jedem anderen IT-Einwirkungspfad weitere Angriffsschritte über Netzwerk- oder datentechnische Verbindungen durchgeführt werden können.

Prinzipiell können außerdem verschiedene IT-Systeme in diversen Anlagenteilen und mit unterschiedlichen Funktionen betroffen sein.

Pfadeinleitung

Der IT-Einwirkungspfad „Netzwerkverbindung“ beginnt mit dem Zugriff eines Angreifers auf ein IT-System einer kerntechnischen Anlage bzw. Einrichtung oder einem IT-System, welches eine permanente oder temporäre datentechnische Verbindung zu einem IT-System einer kerntechnischen Anlage oder Einrichtung besitzt. Dies kann je nach IT-System und genauen Umständen über Fernzugriffe möglich sein oder direkt vor Ort, beispielsweise durch einen Innentäter. Der Zugriff auf ein IT-System kann außerdem auch indirekt und über Sicherheitsmaßnahmen wie Air-Gaps hinweg erfolgen, beispielsweise über die Lieferkette oder Wechseldatenträger bzw. Servicegeräte, wobei keine direkte Verbindung für den Angreifer besteht, der IT-Angriff jedoch nach der Platzierung von Schadsoftware weitergeführt werden kann und weitere Komponenten oder IT-Systeme mit datentechnischen oder Netzwerkverbindungen zum ursprünglichen System betroffen sein können.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Um den Einwirkungspfad „Netzwerkverbindung“ einzuleiten, ist eine bzw. mehrere folgende Bedingungen zwingend notwendig:

- Zugriff eines Angreifers auf ein IT-System, welches permanente oder temporäre datentechnische Verbindungen zu anderen IT-Systemen besitzt
- Zugriff eines Angreifers auf ein IT-System, welches aus mehreren Komponenten besteht, die permanent oder temporär datentechnisch miteinander kommunizieren

Für die Einleitung des IT-Einwirkungspfades „Netzwerkverbindung“ ist generell eine Form der datentechnischen Kommunikation bzw. Netzwerkverbindung von einzelnen Komponenten eines IT-Systems oder zwischen IT-Systemen erforderlich. Zu diesen muss ein potenzieller Angreifer Zugriff haben, entweder in Form eines direkten Zugriffs, der temporär oder permanent sein kann, oder in Form eines indirekten Zugriffs, der vorherige IT-Angriffsschritte erfordert. Dementsprechend weist der IT-Einwirkungspfad „Netzwerkverbindung“ unter diesen Umständen enge Verbindungen zu anderen IT-Einwirkungspfaden wie beispielsweise „Servicegeräte“ und „Wechseldatenträger“ auf.

Die Einwirkung kann darauf ausgelegt sein, die (Netzwerk)Kommunikation von Komponenten bzw. IT-Systemen zu manipulieren oder als Übertragungsweg für Schadsoftware auszunutzen, aber es sind auch Einwirkungen in Form von Unterbrechungen von Kommunikationswegen denkbar.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Unterstützend zur Einleitung des Einwirkungspfads „Netzwerkverbindung“ wirken generell dauerhaft bestehende datentechnische Verbindungen bzw. Kommunikation. Außerdem erhöht die Anzahl solcher Verbindungen das mögliche Gefahrenpotenzial und wirkt unterstützend zur Einleitung des Einwirkungspfades. Wenn datentechnische Verbindungen erforderlich sind, diese für den Betrieb aber nur temporär und nicht dauerhaft bestehen müssen, jedoch aus praktischen Gründen dauerhaft installiert werden, unterstützt dies die Einleitung des Einwirkungspfades.

Zudem wirkt das Nicht-Einhalten oder Fehlen von Sicherungsvorschriften, wozu auch mangelhafte Untersuchungen potenzieller Auswirkungen oder übermäßige Sorglosigkeit zählen, unterstützend. Zu diesem Aspekt wurde bereits ein Ereignis gemeldet, bei dem aufgrund eines falschen Kenntnisstandes und dem Unterlassen des Hinzuziehens der Anlagendokumentation, fälschlicherweise eine datentechnische Verbindung unterbrochen wurde, sodass Meldungen der Gefahrenmeldeanlage nicht mehr an den dafür vorgesehenen Stellen angezeigt wurden.

Pfadzwischenschritte

Nach initialer Pfadeinleitung kann, je nach den genauen Umständen, die Einwirkung auf betroffene und weitere, verbundene IT-Systeme weiter eskaliert werden. Ist ein IT-System vom IT-Einwirkungspfad „Netzwerkverbindung“ betroffen, können prinzipiell davon ausgehend in folgenden Schritten weitere Komponenten oder IT-Systeme Ziele eines IT-Angriffs sein und zur Verbreitung von Schadsoftware oder Erlangung der (vollständigen) Kontrolle des Systems genutzt werden. Außerdem können isolierte Systeme über andere IT-Einwirkungspfade wie Wechseldatenträger oder Servicegeräte für einen Angriff erreichbar sein.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad „Netzwerkverbindung“ endet mit der Einwirkung auf ein IT-System, wenn keine weiteren datentechnischen Verbindungen bestehen. Dies kann für das Ursprungssystem oder bereits über Netzwerke oder sonstige Wege mit Schadsoftware infizierte IT-Systeme gelten. Zudem ist eine gezielte Unterbrechung von Netzwerkverbindungen möglich, um den Einwirkungspfad zu beenden. Die Pfadübergänge zu weiteren IT-Einwirkungspfaden sind abhängig von den bestehenden datentechnischen Verbindungen und der Art, wie die Einwirkung stattfand. Es kann zu Interaktionen mit den IT-Einwirkungspfaden „Servicegeräte“, „Wechseldatenträger“, Parametrierung und Konfiguration“ und ggf. weiteren kommen.

4.2.10.2 Pfadauswirkungen

Die Auswirkungen des Einwirkungspfades „Lieferkette“ sind generell abhängig von den betroffenen Systemen und der Art der potenziellen Schadsoftware. Dabei kann prinzipiell zwischen Netzwerkverbindungen mit (digitaler) Kommunikation im Sinne eines Netzwerks und datentechnischer Kommunikation (analog oder digital, beispielsweise von Komponenten innerhalb eines IT-Systems) unterschieden werden. Aufgrund der engen Verbindung des IT-Einwirkungspfades „Netzwerkverbindung“ – viele andere IT-Einwirkungspfade beruhen (teilweise) auf datentechnischen bzw. Netzwerkverbindungen oder haben entsprechende Pfadeinleitungen, -zwischenschritte und/oder -übergänge – gibt es eine Vielzahl möglicher Auswirkungen.

Real beobachtete Auswirkungen

Im Fall des meldepflichtigen Ereignisses 2016/025 im Kernkraftwerk Biblis gab es keine Auswirkungen auf die Anlage, Personen oder die Umgebung. Die vom Schadsoftwarefund betroffenen Computer waren teilweise nicht im Betrieb und somit ausgeschaltet. Außerdem waren keine Computer betroffen, die elementare Funktionen der Anlagensicherung in der Peripherie erfüllen. Die Computer für Hauptfunktionen der Systeme waren schadsoftwarefrei. Insgesamt waren neben den Computern der Anlagensicherung und zwei externen Festplatten auch neun Teilsysteme des Personenkontrollsystems betroffen. Dabei handelt es sich um ein autarkes Ethernet-Netzwerk bestehend aus einem Hauptserver mit Datenbank, Dialogstationen, die beispielsweise als Bedienoberfläche zur Eingabe von Daten oder Ausweiserstellung dienen, sowie Stationen zur Personenidentifizierung und Zutrittsfreigabe.

Eine forensische Analyse ergab, dass die Schadsoftware keine Funktionalitäten beinhaltete, die auf eine Manipulation von zutrittskontroll- oder Steuerungssystemen hindeutete und generell ohne eine aktive externe Kommunikationsmöglichkeit keine Veränderungen an Daten vornehmen konnte.

Im Fall des meldepflichtigen Ereignisses 2016/022 in Gundremmingen gab es keine Auswirkungen auf die Anlagen, Personen oder die Umgebung. Die auf dem Visualisierungsrechner der BE-Lademaschine gefundene Schadsoftware war auf Windows-Infrastrukturen ausgelegt und beinhaltete keine Funktionalitäten zur Manipulation von Steuerungssystemen. Das betroffene System hatte keine Internetverbindung. Die Konfiguration des Visualisierungsrechners zum Zeitpunkt des Vorfalls erlaubte zudem keine Änderungen der Betriebs- und Sicherheitssteuerungen der BE-Lademaschine. Es ist davon auszugehen, dass es sich nicht um einen gezielten IT-Angriff handelte, sondern um eine zufällige Infektion mit Schadsoftware, die nur aufgrund der Verwendung eines USB-Sticks im nicht vorgesehenen Rahmen im Zusammenhang mit einem anderen IT-System (Schulungsrechner) erfolgen konnte. Neben dem Visualisierungsrechner der BE-Lademaschine wurden außerdem acht Computer der Anlage, ein Notebook einer Fremdfirma und 18 USB-Sticks infiziert. Eine forensische Analyse der Schadsoftware im betroffenen Fall ergab, dass diese nicht aktiv genutzt wurde und aufgrund der fehlenden externen Netzwerkverbindung keine weiteren IT-Angriffsschritte möglich gewesen wären.

Beim meldepflichtigen Ereignis 2018/059 im Versuchskraftwerk Jülich wurden durch die fälschlicherweise durchgeführte Trennung eines Kabels, sämtliche Störmeldungen der Gefahrenmeldeanlage unterdrückt. Die auflaufenden Meldungen wurden nicht an den meldungsausgebenden Teil der Gefahrenmeldeanlage weitergegeben, sodass sämtliche Komponenten der Visualisierungssysteme der Gefahrenmeldeanlage am Bedienplatz der Warte keine Störungen mehr anzeigten. Die Anlage befand sich zum Ereigniszeitpunkt außerhalb des Regelbetriebs und während der Ausfallzeit sind keine sicherheitstechnisch relevanten Meldungen angefallen, wie eine nachträgliche Untersuchung ergab.

Potenzielle Auswirkungen

Die potenziellen Auswirkungen des IT-Einwirkungspfades „Netzwerkverbindung“ sind abhängig von dem bzw. den betroffenen Systemen, der Art der Einwirkung und entsprechend von potenziellen Verbindungen zu anderen Systemen.

Je nach Vernetzung und den genauen Umständen gibt es eine Vielzahl möglicher potenzieller Einwirkungen auf verschiedene Systeme. Prinzipiell können IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein, die sicherheits- und sicherungstechnisch relevant sind, was schwerwiegende sicherheits- und sicherungstechnische Auswirkungen haben kann. Hinsichtlich der Verbindung zu anderen IT-Systemen und den mit höherer IT-Schutzbedarfsklasse einhergehenden steigenden Anforderungen an die IT-Sicherheit insbesondere bezüglich Verbindungen zu anderen IT-Systemen und IT-Sicherheitszonen, fallen potenzielle Auswirkungen bei IT-Systemen niedrigerer IT-Schutzbedarfsklasse in der Regel entsprechend schwerwiegender aus. Insbesondere sicherungstechnische IT-Systeme, wie beispielsweise die Gefahrenmeldeanlage oder Systeme zur Zutrittskontrolle, sind auf einen gewissen Grad an Vernetzung angewiesen, sodass die potenziellen Auswirkungen einer Einwirkung auf diese Systeme über Netzwerkverbindung entsprechend weitreichend und sicherungsrelevant sind.

Die direkten potenziellen Auswirkungen des Einwirkungspfades bei IT-Systemen, die keine Netzwerkverbindungen zu anderen IT-Sicherheitszonen bzw. IT-Systeme haben, beschränken sich auf dieses IT-System. Konkret können durch die Manipulation oder Unterbrechung von datentechnischen oder Netzwerkverbindungen innerhalb eines IT-Systems die Verfügbarkeit, Integrität und Vertraulichkeit gestört werden. Durch die Unterbrechung von datentechnischen Verbindungen zwischen verschiedenen Komponenten eines IT-Systems können Teilsysteme oder auch das Gesamtsystem gestört werden, sodass Funktionen nicht mehr oder nicht vollumfänglich verfügbar sind. Zudem ist es vorstellbar, dass durch die Manipulation einer Verbindung Schutzaktionen verhindert oder fälschlicherweise ausgelöst werden, beispielsweise indem falsche Grenzwerte erzeugt werden oder wie im Fall des meldepflichtigen Ereignisses 2018/059 Signale bzw. Meldungen blockiert werden.

Besitzt ein IT-System datentechnische Verbindungen zu weiteren IT-Systemen innerhalb einer IT-Sicherheitszone bzw. in anderen IT-Sicherheitszonen, beschränken sich die potenziellen Auswirkungen des Einwirkungspfades nicht nur auf das betroffene IT-System, sondern auch auf die verbundenen IT-Systeme. Dabei kann die Kommunikation zwischen den IT-Systemen manipuliert werden, sodass analog die Verfügbarkeit, Integrität und Vertraulichkeit von Teilsystemen bzw. einem oder mehreren IT-Systemen beeinflusst werden kann. Über Verbindungen zu anderen IT-Systemen kann potenzielle Schadsoftware zudem möglicherweise weiterverbreitet und die Kontrolle oder Manipulation von Angreifern entsprechend ausgeweitet werden.

Insgesamt ergeben sich für die IT-Einwirkung über Netzwerkverbindungen je nach den genauen Umständen und Verbindungen vielfältige Angriffsmöglichkeiten, ggf. auch auf sicherheits- und sicherungsrelevante IT-Systeme.

Pfadübergreifende Auswirkungen

Der IT-Einwirkungspfad „Netzwerkverbindung“ eröffnet bei entsprechenden Umständen verschiedene weitere IT-Einwirkungspfade und besitzt außerdem pfadübergreifende Auswirkungen. Netzwerkverbindungen sind bei Überlegungen zur IT-Sicherheitsarchitektur oft der erste Punkt, der genannt wird, wenn es um mögliche Schwachstellen geht. Über derartige Verbindungen zwischen Komponenten oder IT-Systemen können innerhalb eines IT-Angriffs weitergehende Angriffsschritte durchgeführt und beispielsweise das Einflussgebiet eines potenziellen Angreifers erweitert werden. Der Einwirkungspfad „Netzwerkverbindung“ kann einleitend für bzw. übergreifend auf folgende IT-Einwirkungspfade wirken:

- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Über datentechnische bzw. Netzwerkverbindungen können IT-Systeme beispielsweise durch eine Vielzahl an Anfragen oder Daten oder die Übertragung bestimmter Daten überlastet werden.
- IT-Einwirkungspfad „Parametrierung und Konfiguration“: Die Parametrierung bzw. Konfiguration von IT-Systemen kann über Netzwerkverbindungen manipuliert werden, wenn parametrierbare bzw. konfigurierbare IT-Systeme an ein IT-Angreifern zugängliches IT-System datentechnisch angebunden sind.
- IT-Einwirkungspfad „Fernzugriffe“: Bestehen datentechnische Verbindungen von IT-Systemen zu einzelnen Komponenten oder anderen IT-Systemen lokal oder auch remote, können über diese Verbindungen Fernzugriffe durchgeführt und dadurch weitere Angriffsschritte unternommen werden. Netzwerkverbindungen können somit unter Umständen unbeabsichtigte Fernzugriffe ermöglichen oder beabsichtigte Fernzugriffe manipulieren.
- IT-Einwirkungspfad „Wechseldatenträger“: Über datentechnische bzw. Netzwerkverbindungen können Wechseldatenträger, welche mit (anderen) IT-Systemen verbunden sind, für weitere Angriffsschritte genutzt werden.
- IT-Einwirkungspfad „Servicegeräte“: Über datentechnische bzw. Netzwerkverbindungen können Servicegeräte, welche mit (anderen) IT-Systemen verbunden sind, für weitere Angriffsschritte genutzt werden.

4.2.10.3 Pfadblockierende Faktoren

Wie beschrieben besitzt der IT-Einwirkungspfad „Netzwerkverbindung“ verschiedene mögliche Pfadeinleitungen und kann außerdem zur Einleitung weiterer IT-Einwirkungspfade führen oder mit diesen interagieren. Pfadblockierende Faktoren teilen sich dabei in die Faktoren Mitigation, Aufdeckung und Unterbrechung ein.

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Im Fall von Netzwerkverbindungen stellt bereits die Netzwerkarchitektur einen wesentlichen Faktor zur Mitigation von IT-Einwirkungen über datentechnische Verbindungen dar. Durch die Beschränkung auf für den Betrieb essenzielle Verbindungen und ggf. auch nicht permanente Verbindungen lässt sich die Gefahr von Einwirkungen über das Netzwerk bereits reduzieren. Außerdem bieten entsprechend konfigurierte Firewalls, die nur autorisierte Kommunikation zulassen, Möglichkeiten, IT-Einwirkungen über diesen Einwirkungspfad zu verhindern.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die Aufnahme von Gegenmaßnahmen und im Idealfall die sofortige Beendigung eines IT-Einwirkungspfades. Wird eine Einwirkung entdeckt, kann der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen werden. IT-Einwirkungen über datentechnische bzw. Netzwerkverbindungen lassen sich durch die Überwachung bzw. Überprüfung des Datenverkehrs aufdecken. Bei ungewöhnlichen Aktivitäten können so Gegenmaßnahmen eingeleitet werden. Je nach Art der Einwirkung und Überwachung des Datenverkehrs sind solche Aufdeckungsmaßnahmen nur bedingt geeignet, IT-Einwirkungen über Netzwerkverbindungen aufzudecken und zu unterbrechen. Besteht die Überwachung bzw. Überprüfung des Datenverkehrs ausschließlich aus der (manuellen) Auswertung von Logfiles findet eine Aufdeckung möglicherweise erst verspätet statt. Automatisierte Überwachungsmaßnahmen, die z. B. verdächtige Verbindungen oder Verbindungen zu ungewöhnlichen Zeiten erkennen, ermöglichen eine schnellere Aufdeckung und Reaktion. Ansonsten sind wie bei anderen IT-Einwirkungspfaden Virenscans grundsätzlich dazu geeignet, IT-Einwirkungen über Netzwerkverbindungen aufzudecken.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Netzwerkverbindung“ kann unterbrochen werden, indem die datentechnische bzw. Netzwerkverbindung getrennt wird. Dies ist in der Regel die erste Maßnahme, die empfohlen wird, um beispielsweise die Ausbreitung von Schadsoftware über das Netzwerk zu verhindern. Neben einer physischen Trennung der Verbindung, die ggf. nicht oder nur mit erheblichem Aufwand möglich ist, können zunächst auch Schritte zur digitalen Trennung der Verbindung oder weiterer Verbindungen unternommen werden.

4.2.10.4 Pfadzusammenfassung Netzwerkverbindungen

Der IT-Einwirkungspfad „Netzwerkverbindung“ ist unter den beschriebenen Gesichtspunkten als schwerwiegender Einwirkungspfad mit zentralen Einwirkungsmöglichkeiten anzusehen, der auf verschiedenste Weise eingeleitet werden kann. Über datentechnische bzw. Netzwerkverbindungen innerhalb von IT-Systemen oder zwischen IT-Systemen besteht häufig die größte Gefahr für die Ausbreitung von Schadsoftware, die Erweiterung des Zugriffs von Angreifern oder weiteren IT-Angriffsschritten. Im Allgemeinen ist die Anwendung von datentechnischen bzw. Netzwerkverbindungen in kerntechnischen Anlagen und Einrichtungen in sämtlichen Bereichen bzw. auch in mehreren vernetzten Bereichen denkbar. Mit höheren IT-Schutzbedarfsklassen steigen dabei die Anforderung an die IT-Sicherheitsmaßnahmen der Verbindungen. Gerade im Bereich sicherungstechnischer Systeme, die oftmals einen gewissen Grad an datentechnischer Verbundenheit erfordern, stellt der Einwirkungspfad eine hohe Relevanz dar. Die möglichen Auswirkungen des Einwirkungspfades sind potenziell schwerwiegend. Der IT-Einwirkungspfad „Netzwerkverbindung“ ist eng mit anderen Einwirkungspfaden verbunden, was sich in den zahlreichen aufgeführten möglichen pfadübergreifenden Auswirkungen zeigt, andererseits jedoch auch bei den anderen Einwirkungspfaden, welche oftmals ebenfalls pfadübergreifende Auswirkungen auf diesen Einwirkungspfad haben können. Mitigierende und aufdeckende Faktoren im Zusammenhang mit diesem Einwirkungspfad sind neben der Reduzierung der entsprechenden Verbindungen auf das für den Betrieb nötigste, einerseits die Verwendung von Firewalls und außerdem die Überwachung und Auswertung der Kommunikation über Netzwerke.

4.2.11 Innentäter

Der Einsatz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen wird, aufgrund der fortschreitenden Digitalisierung immer bedeutsamer und es ergeben sich daraus neue Angriffsmöglichkeiten. Die Bedienung der betrieblichen IT-Systeme, sowie IT-Systeme mit sicherheits- und sicherungstechnischer Bedeutung erfolgt durch das Fachpersonal einer kerntechnischen Anlage bzw. Einrichtung. Für die Bedienung der IT-Systeme sind Zugriffs- und Zutrittsrechte notwendig, sowie entsprechende Schulungen des Personals, um einen störungsfreien Betrieb der Anlage zu gewährleisten.

Als Innentäter wird eine Person bezeichnet, die einzelne Zugangsberechtigungen besitzt. Im Falle eines Innentäters sind verschiedene Fälle zu unterscheiden, denn nicht jeder Innentäter handelt vorsätzlich oder mit dem Ziel eine Auswirkung auf die Anlage zu erreichen. Im ersten betrachteten Fall eines Innentäters wird ein klares Ziel verfolgt, welches durch bewusst ausgeführte Handlungen zu erreichen versucht wird. Unabhängig von der Art des Motivs, ist es grundsätzlich das Ziel, eine Auswirkung auf die kerntechnische Anlage zu erreichen. Dies können kleine Auswirkungen sein, aber auch Weitreichende, wie beispielsweise die Gefährdung von Gesundheit und Leben oder die Kontrolle über das betroffene IT-System. Bei den anderen beiden Fällen handelt es sich auch um Mitarbeiter, die nicht im Interesse der Anlage agieren, jedoch verfolgen diese nicht zwangsläufig das Ziel eine Auswirkung auf die kerntechnische Anlage oder Einrichtung zu erreichen. Ein Mitarbeiter kann bewusst Regelungen und Richtlinien missachten und somit als Innentäter agieren, jedoch aus Motiven heraus wie Arbeitsüberlastung oder Schwächen im Managementsystem. Regelungen und Richtlinien können aber auch aufgrund von Unwissenheit missachtet werden, was beispielsweise auf einen unzureichenden Ausbildungsstand, also fehlenden Kenntnissen und Fähigkeiten zurückzuführen ist. Dennoch werden diese Fälle im Einwirkungspfad „Innentäter“ mit einbezogen und diskutiert, da es sich um Handlungen des Personals von Innen heraus handelt und Auswirkungen auf die Anlage nicht vollständig auszuschließen sind.

Die Möglichkeiten für einen Innentäter auf ein IT-System einzuwirken, sind vielfältig und zahlreich. Die Auswirkungen eines solchen Verhaltens können weitreichend sein und sind abhängig von der Art des Eingriffs und von dem betroffenen IT-System. Ein Innentäter stellt daher ein sehr hohes Sicherheitsrisiko in einer kerntechnischen Anlage dar.

Auch in Deutschland gab es mit dem meldepflichtigen Ereignis 2016/010 bereits einen IT-Sicherheitsvorfall in Zusammenhang mit einem Innentäter bzw. mehreren Innentätern. In diesem konkreten Fall kam es zum Ausfall der Messung des Störfallmonitors für die Aktivitätskonzentration, aufgrund von Fehlern in den Kondensatoren der Netzteile. Diese Fehler wurden in den vorherigen wiederkehrenden Prüfungen (WKPen) nicht erkannt. Es wird hier von einem vorsätzlichen Verhalten ausgegangen und von vorgetäuschten WKPen, da die Protokolle zwar ausgefüllt wurden, aber keine Durchführungen mit einem Prüfpräparat erfolgt sind. Im Folgenden wird unter Betrachtung dieses und weiterer nationaler, sowie internationaler Ereignisse, in welchen IT-Einwirkungen aufgrund von menschlichem Fehlverhalten (beabsichtigt oder unbeabsichtigt) stattfanden, ein umfassender IT-Einwirkungspfad „Innentäter“ entwickelt und ausführlich dargelegt.

4.2.11.1 Der Einwirkungspfad „Innentäter“

Der Einwirkungspfad „Innentäter“ setzt Fehlverhalten des Personals einer kerntechnischen Anlage, also die Missachtung von Regelungen bzw. Richtlinien, voraus. Dieses Fehlverhalten kann aus den unterschiedlichsten Motiven heraus resultieren. Der Einwirkungspfad „Innentäter“ kann innerhalb, aber auch außerhalb von einer kerntechnischen Anlage beginnen und ist von besonderer sicherheits- und sicherungstechnischer Bedeutung. Eine Einleitung des Einwirkungspfades von außerhalb einer kerntechnischen Anlage wird mit einbezogen, da Eingriffe beispielsweise über Fernzugriffe oder durch den Eingriff in Prozesse der Lieferkette erfolgen können. Auch in diesen Fällen kann ein Mitarbeiter als Innentäter agieren, obwohl dieser sich nicht in der kerntechnischen Anlage befindet, handelt dieser von „Innen“ heraus. Befindet sich ein Innentäter in einer kerntechnischen Anlage, so sind die Möglichkeiten grundlegend unbegrenzt, seien es beispielsweise vorgetäuschte wiederkehrende Prüfungen, das Herstellen von unerlaubten Netzwerkverbindungen oder die Eingabe über Servicegeräte. Ein Innentäter besitzt zahlreiche Möglichkeiten diesen Pfad einzuleiten und auf ein IT-System einzuwirken. In den IT-Einwirkungspfad „Innentäter“ fallen nicht nur direkte Eingriffe bzw. Einwirkungen auf IT-Systeme, sondern auch die Weitergabe von geschützten und vertraulichen Informationen. Werden diese Informationen an Dritte weitergegeben, wird die Vertraulichkeit verletzt und es kann zu Auswirkungen führen. Es gibt demnach zahlreiche Überschneidungen mit anderen Einwirkungspfaden, jedoch werden hier die möglichen Einwirkungen aus Sicht eines Innentäters betrachtet. Prinzipiell können außerdem verschiedene IT-Systeme in diversen Anlagenteilen und mit unterschiedlichen Funktionen betroffen sein.

Pfadeinleitung

Der IT-Einwirkungspfad „Innentäter“ beginnt mit dem Zugriff eines Mitarbeiters auf ein IT-System und der anschließenden Missachtung von Regelungen bzw. Richtlinien bei der Bedienung eines IT-Systems einer kerntechnischen Anlage bzw. Einrichtung. Es existieren unterschiedliche Fälle von Innentätern, die sich in der Motivation unterscheiden und differenziert voneinander zu betrachten sind.

Notwendige Bedingungen zur Einleitung des Einwirkungspfades

Zur Einleitung des Einwirkungspfades „Innentäter“ ist eine der folgenden Bedingungen notwendig:

- Zugriff eines Mitarbeiters auf ein IT-System und den Willen auf dieses einzuwirken, sowie die Verfolgung eines bestimmten Ziels (Bsp.: Gefährdung von Gesundheit und Leben, Kontrolle der kerntechnischen Anlage)
- Zugriff eines Mitarbeiters auf ein IT-System und vorsätzliches missachten der Regelungen, aber aus anderen Motiven heraus (keine gewollten resultierenden Auswirkungen)
- Zugriff eines Mitarbeiters auf ein IT-System und Fehlverhalten des Mitarbeiters ohne vorsätzliches Missachten der Regelungen, sondern aus Motiven wie beispielsweise der Unwissenheit heraus

Sobald IT-Systeme existieren, ist der Einwirkungspfad „Innentäter“ für IT-Angriffe vorstellbar. Es ist lediglich der Zugriff auf ein IT-System notwendig, dabei kann es sich um Software und/oder Hardware handeln. Grundsätzlich ist kein IT-System, sei es betrieblich, sicherheits- oder sicherungstechnisch relevant, vollständig vor dem Zugriff eines Mitarbeiters der kerntechnischen Anlage geschützt. Eine Einleitung des IT-Einwirkungspfades „Innentäter“ kann aus dem Inneren einer Anlage direkt erfolgen oder aber auch von außerhalb über Fernzugriffe oder im Prozess der Lieferkette.

Unterstützende Bedingungen zur Einleitung des Einwirkungspfades

Durch erweiterte Nutzungen, Datenaustausch, erweiterte Zugriffsmöglichkeiten, nicht ausreichende Schulungen bzw. Ausbildungsstand und nicht Einhaltung von Sicherungsvorschriften bzw. dem Fehlen dieser, wird die Möglichkeit der Einleitung des IT-Einwirkungspfades „Innentäter“ erweitert bzw. vereinfacht.

Im meldepflichtigen Ereignis 2016/010 wurden beispielsweise die Regelungen, die für eine WKP gelten absichtlich ignoriert. Unterstützend wirken somit unzureichend geschultes Personal, sowie nicht ausreichende Sicherungsmaßnahmen in Bezug auf Zugriffs- und Zutrittsmöglichkeiten.

Pfadzwischenschritte

Nach einer Pfadeinleitung kann die Einwirkung auf das betroffene IT-System oder auch weitere, verbundene IT-Systeme weiter eskalieren. Ist ein IT-System vom Einwirkungspfad „Innentäter“ betroffen, so kann es grundlegend zum Angriff auf andere IT-Systeme kommen, beispielweise zur Verbreitung von Schadsoftware oder aber auch zur vollständigen Kontrolle des betroffenen IT-Systems. Ein Innentäter bildet zudem die Brücke zwischen isolierten IT-Systemen und kann beispielsweise mit Hilfe von Wechseldatenträgern, unerlaubten Netzwerkverbindungen oder Servicegeräten eine Einwirkung auf diese IT-Systeme ausüben.

Pfadende und Pfadübergänge

Der IT-Einwirkungspfad endet mit der Einwirkung von einem Mitarbeiter auf ein IT-System, soweit keine weiteren Netzwerkverbindungen zu anderen IT-Systemen bestehen und keine weiteren Handlungen des Mitarbeiters vollzogen werden, im Sinne von Datentransfers, beispielsweise über Wechseldatenträger oder Servicegeräte. Diese Art von Innentätern missachtet die Regelungen bewusst oder unwissentlich, jedoch sind Auswirkungen auf die Anlage zu erreichen hier nicht das beabsichtigte Ziel und der Mitarbeiter vollzieht grundlegend keine weiteren Handlungen.

Verfolgt ein Innentäter ein bestimmtes Ziel und seine Verhaltensweisen sind geplant, so endet der Einwirkungspfad mit hoher Wahrscheinlichkeit erst, sobald der Täter sein Ziel erreicht hat. Es sei denn, es kommt zu einer vorherigen Aufdeckung durch Sicherungsmaßnahmen.

Die Pfadübergänge sind abhängig von dem betroffenen IT-System und den Netzwerkverbindungen zu anderen IT-Systemen, aber es kann grundsätzlich zu Interaktionen mit zahlreichen anderen Einwirkungspfaden kommen, in allen betrachteten Fällen des Innentäters.

4.2.11.2 Pfadauswirkungen

Die Auswirkungen des IT-Einwirkungspfad „Innentäter“ sind grundlegend abhängig von dem betroffenen IT-System und der Art der Einwirkung auf das IT-System. Zudem sind die Auswirkungen von den Motiven des Innentäters abhängig. Handelt ein Innentäter gezielt, so kann es zu gravierenden Auswirkungen kommen. Im schlimmsten Fall zur Gefährdung von Leben und Gesundheit in der kerntechnischen Anlage oder durch Entwendung von radioaktivem Material an anderen Orten, sowie die Herstellung von kritischen Anordnungen. In diesem betrachtenden Fall ist unabhängig von dem IT-System eine Auswirkung zu erwarten, da der Innentäter mit hoher Wahrscheinlichkeit eine Einwirkung auf ein relevantes IT-System oder die Beschaffung und Weitergabe von geschützten Informationen geplant hat.

Missachtet ein Mitarbeiter bewusst oder unwissentlich die geltenden Regelungen oder Richtlinien, können auch hier je nach Auslegung der IT-Systeme weitreichende Folgen entstehen, jedoch sind die Motive bzw. Gründe für das Verhalten hier grundlegend andere, sodass die Auswirkungen aller Wahrscheinlichkeit nach geringer ausfallen oder es nicht zu Auswirkungen führt. Als Beispiel ist hier das Ereignis 2016/022 zu nennen, wo eine Schadsoftware auf viele IT-Systeme übertragen wurde, es aber dennoch keine Auswirkungen in dem Sinne auf die IT-Systeme gab und die Anlage weiterhin störungsfrei betrieben werden konnte.

Mit dem VERA-Ereignis 2016/010 ist ein Ereignis in kerntechnischen Anlagen bekannt geworden, bei dem der IT-Einwirkungspfad „Innentäter“ betroffen war. Zudem gibt es auch einige internationale IRS-Ereignisse, die in den Einwirkungspfad „Innentäter“ fallen.

Real beobachtete Auswirkungen

Es wurden bisher mehrere Ereignisse im Zusammenhang mit dem Einwirkungspfad „Innentäter“ gemeldet, bei denen unterschiedliche Auswirkungen beobachtet wurden und verschiedene Motive bzw. Handlungen der Mitarbeiter ursächlich waren.

Im Fall des meldepflichtigen Ereignisses 2016/010 in KKP-2 gab es keine Auswirkungen auf die kerntechnische Anlage, Personen oder die Umgebung. Im Zuge einer wiederkehrenden Prüfung der Strahlungs-/Aktivitätsüberwachung wurde der Messwertausfall des Messgasdurchsatzes erkannt.

Durch vorherige vorgetäuschte wiederkehrende Prüfungen wurde dieser Fehler zuvor nicht erkannt, da eine Überprüfung der Kalibrierung, Signalisierung und der Messelektronik nicht erfolgte. Die real beobachtete Auswirkung war die Unterbrechung des Durchsatzsignals, welche zu einem Ausfall der Messung der Aktivitätskonzentration durch den Störfallmonitor führte. Dieses Ereignis ist ein Beispiel für ein vorsätzliches Verhalten von Mitarbeitern mit geringen sicherheitstechnischen Auswirkungen auf die Systemfunktionen der Strahlungs-/Aktivitätsüberwachung. Das Verhalten des Personals ist hier ein Hinweis auf Schwächen im Managementsystem.

Bereits im meldepflichtigen Ereignis 01/2015 kam es zu Unregelmäßigkeiten bei wiederkehrenden Prüfungen der Strahlungs-/Aktivitätsüberwachung in der Anlage KKP-1. Es wurden fehlerhafte Parameter an 24 Messgeräten entdeckt, aber anschließend nicht alle von dem Prüfteam korrigiert. Bei der Aufarbeitung des ME 02/2016 wurden weitere Unstimmigkeiten bei der WKP von anderen Meseinrichtungen festgestellt. Insgesamt in neun Fällen. In einem Fall, in KKP-1, wurden WKP-Protokolle erstellt und die Prüfungen als befundfrei dokumentiert, obwohl keine WKPen durchgeführt wurden. Ein weiterer Täuschungsfall wurde in der Anlage KKP-2 entdeckt (ein falsch eingestellter Grenzsignalgeber). Hier war das gleiche Prüfteam involviert, wie im Ereignis ME 2016/010. Es ist in den genannten Fällen davon auszugehen, dass die technischen Funktionen der Überwachungseinrichtungen trotz der Täuschungen noch gegeben waren.

International kam es zu einigen IRS-Meldungen, die in Zusammenhang mit menschlichem Fehlverhalten stehen, welche aus unwissentlichen bzw. unbeabsichtigten Handlungen der Mitarbeiter resultierten. Es sind unterschiedliche Auswirkungen der Einwirkungen zu erkennen. Ursächlich waren in diesen Ereignissen beispielsweise Fehlinterpretationen der digitalen Anzeige (8297), das Versenden einer falschen Nachricht bei einer Notfallübung (8247), Fehlbedienung der Benutzeroberfläche (8714), falsche Konfiguration des IT-Systems (8658) oder Verdrahtungsfehler bei der Installation (8983).

Potenzielle Auswirkungen

Die potenziellen Auswirkungen des IT-Einwirkungspfades „Innentäter“ sind abhängig von dem betroffenen System, der Art der Einwirkung und von den potenziellen Verbindungen zu anderen Systemen. Grundlegend ist der Zugriff auf jedes IT-System, welches betrieblich, sicherheits- oder sicherungstechnisch relevant ist, unabhängig von der IT-Schutzbedarfsklasse, gegeben.

Die Zugriffe und Zutritte für Mitarbeiter einer Anlage sind grundsätzlich geregelt und es gelten verschiedene Sicherungsmaßnahmen. Missachtung dieser Regelungen, egal aus welchen Motiven heraus, können schwerwiegende sicherheits- und sicherungstechnische potenzielle Auswirkungen haben.

Bei Manipulationen beispielsweise über eine Schadsoftware, direkte manuelle Eingaben, über Wechseldatenträger oder Fernzugriffe können relevante und betriebsgeheime Informationen ausgelesen, weitergegeben oder verändert werden oder auch die Funktionalität der IT-Systeme beeinflusst werden. Grundlegend ist die Kontrolle des IT-Systems oder mehrerer IT-Systeme der Anlage möglich. Als Innentäter sind die Möglichkeiten der Einwirkungen und der daraus resultierenden potenziellen Auswirkungen grundsätzlich unbegrenzt. Zudem ist es vorstellbar, dass durch die Manipulation eines IT-Systems Schutzaktionen verhindert oder fälschlicherweise ausgelöst werden.

Prinzipiell können die Vertraulichkeit, Verfügbarkeit oder die Integrität des IT-Systems verletzt werden. Die Manipulation ausgeführt von einem Innentäter ermöglicht somit insgesamt eine umfassende Einwirkung auf sicherheits- und sicherungsrelevante IT-Systeme. Diese Einwirkungen können unerkannt erfolgen und eine erhebliche sicherheits- und sicherungstechnische Relevanz entwickeln.

Pfadübergreifende Auswirkungen

Besitzt ein Mitarbeiter Zugriff auf ein IT-System oder Zutrittsrechte zu bestimmten Räumlichkeiten, sind die Möglichkeiten einen anderen Einwirkungspfad einzuleiten zahlreich. Vom IT-Einwirkungspfad „Innentäter“ können somit andere Einwirkungspfade entspringen und pfadübergreifende Auswirkungen ausgehen. Innentäter spielen eine entscheidende Rolle in den Auswirkungen eines Eingriffs und im Übergang zu anderen Einwirkungspfaden. Dieser Pfad kann für folgende IT-Einwirkungspfade einleitend sein:

- IT-Einwirkungspfad „Wechseldatenträger“: Wechseldatenträger werden für Updates von IT-Systemen genutzt und können mit zahlreichen IT-Systemen verbunden werden. Agiert ein Innentäter und verbindet einen Wechseldatenträger mit einem IT-System, so kann der IT-Einwirkungspfad „Wechseldatenträger“ ausgelöst werden. Ein Innentäter kann auch als Brücke zwischen sogenannten Inselsystemen dienen.

- IT-Einwirkungspfad „Servicegeräte“: Die Bedienung eines Servicegerätes erfolgt durch das Personal einer kerntechnischen Anlage und der Pfad kann durch direkte Eingaben in ein Servicegeräte oder die Herstellung von Verbindungen zu anderen IT-Systemen eingeleitet werden.
- IT-Einwirkungspfad „Parametrierung und Konfiguration“: Parameter und die Konfiguration von IT-Systemen können von einem Mitarbeiter manipuliert werden.
- IT-Einwirkungspfad „Fernzugriff“: Durch einen Innentäter können auf einige IT-Systeme über einen Fernzugriff zugegriffen werden und die Möglichkeit einer Manipulation besteht.
- IT-Einwirkungspfad „Lieferkette“: Mitarbeiter der kerntechnischen Anlage können in Prozesse der Lieferkette eingreifen.
- IT-Einwirkungspfad „Netzwerkverbindung“: Unerlaubte Netzwerkverbindungen können von Mitarbeitern hergestellt werden.
- IT-Einwirkungspfad „Überlastung von IT-Systemen“: Eine Überlastung von IT-Systemen kann durch häufige manuelle Anfragen oder durch den Aufbau einer Netzwerkverbindung, sowie den Anschluss eines Wechseldatenträgers oder Servicegerätes hervorgerufen werden.
- IT-Einwirkungspfad „Versionenmanagement“: Das Versionenmanagement kann durch einen Innentäter manipuliert werden.

4.2.11.3 Pfadblockierende Faktoren

Mitigierende Faktoren

Mitigierende Faktoren beinhalten jede Art von Maßnahme, welche potenzielle Auswirkungen des IT-Einwirkungspfades reduzieren oder aufheben. Mitigierend wirken insbesondere klare Regelungen der Zutritts- und Zugriffsrechte, Einschränkungen von Benutzer- und Zugriffsrechten, sowie administrative Regelungen bzw. Sicherungsmaßnahmen. Zudem werden die Möglichkeiten eines Innentäters, durch eine Reduzierung von datentechnischen Verbindungen, sowie der Deaktivierung nicht verwendeter Schnittstellen eingeschränkt.

Aufdeckende Faktoren

Die Aufdeckung von Einwirkungen ermöglicht die Aufnahme von Gegenmaßnahmen und im Idealfall die sofortige Beendigung eines IT-Einwirkungspfades. Wird eine Einwirkung entdeckt, kann der IT-Einwirkungspfad aufgrund der darauffolgenden Reaktion unterbrochen werden. Im Einwirkungspfad „Innentäter“ ist die Aufdeckung abhängig von der Art der Einwirkung, die von einem Innentäter ausgeübt wird. Für jede Einleitung eines anderen Einwirkungspfades ist der Zugriff auf das entsprechende IT-System notwendig. Sei dies direkt aus dem Inneren der kerntechnischen Anlage oder über einen Fernzugriff von außerhalb (aber auch auf einen Prozess innerhalb der Lieferkette). Eine frühzeitige Aufdeckung kann durch die Überprüfung von Zugriffs- bzw. Logdateien erfolgen. So können Zugriffe, befugte oder unbefugte, sowie Änderungen erkannt werden. Eine Überwachung und Überprüfung des Datenverkehrs kann zudem Hinweise auf verdächtige Systemaktivitäten und das Vorhandensein von Schadsoftware hindeuten, woraufhin weitere investigative Maßnahmen durchgeführt werden können. Regelmäßige durchgeführte wiederkehrende Prüfungen können IT-Einwirkungen auf ein IT-System aufdecken.

Allerdings können beispielsweise manuelle Manipulationen von Parametern oder Konfigurationen dadurch nicht aufgedeckt werden. Es besteht aber die Möglichkeit Manipulationen dessen durch einen Abgleich der aktuellen Parametrierung und Konfiguration mit dokumentierten Vergleichswerten bzw. Herstellerunterlagen zu erkennen. Eine Überwachung des Netzwerkverkehrs und des Nutzerverhaltens kann auch zu einer Aufdeckung beitragen.

Unterbrechende Faktoren

Der IT-Einwirkungspfad „Innentäter“ wird immer dann unterbrochen, wenn eine Aufdeckung stattfindet und darauf eine entsprechende anforderungsgemäße Reaktion veranlasst wird. Außerdem bieten administrative Regelungen bezüglich des Umgangs mit diesen Systemen, Zugriffskontrollen und ggf. Unterbringungsschutz die Möglichkeit Einwirkungen zu unterbrechen.

Eine Unterbrechung des Einwirkungspfades „Innentäter“ ist abhängig von der Art des Eingriffs auf ein IT-System, beispielsweise können Überwachungen bzw. Überprüfungen des Datenverkehrs, Virenscans, Überprüfungen der Integrität, Zugriffsdokumentationen, Datenabgleiche oder Eingabeprotokolle aufdeckend sein.

4.2.11.4 Pfadzusammenfassung Innentäter

Der IT-Einwirkungspfad „Innentäter“ kann unter den beschriebenen Gesichtspunkten als schwerwiegender Einwirkungspfad angesehen werden. Es gibt national und international bereits gemeldete Ereignisse, die auf vorsätzliche oder unwissentliche Handlungen von Mitarbeitern, sogenannten Innentätern, zurückzuführen sind. Die Pfadeinleitung kann sowohl direkt und manuell am IT-System beginnen oder in Kombination mit anderen IT-Einwirkungspfaden wie Servicegeräte, Wechseldatenträger, Netzwerkverbindungen oder Fernzugriffe. Neben einer direkt ersichtlichen Einflussnahme sind auch zunächst unbemerkte Schritte oder Manipulationen denkbar, die zunächst unerkannt bleiben. Bei den bisher beobachteten Auswirkungen handelt es sich um keine gravierenden sicherheitstechnischen Auswirkungen, auch wenn sicherheitstechnische IT-Systeme unteranderem betroffen waren.

Es handelte sich in diesen Fällen nach aktuellem Kenntnisstand nicht um Einwirkungen die gezielte Auswirkungen verursachen sollten, sondern unbeabsichtigtes oder beabsichtigtes menschliches Fehlverhalten, welches beispielsweise auf einen unzureichenden Ausbildungsstand oder auf Schwächen im Managementsystem zurückzuführen ist. Die potenziellen Pfadauswirkungen sind vielfältig, da in der Regel auf jedes IT-System Zugriff besteht, um den Betrieb der Anlage zu gewährleisten. Dadurch können prinzipiell IT-Systeme jeder IT-Schutzbedarfsklasse betroffen sein, die sicherheits- und sicherungstechnisch relevant sind, was zu schwerwiegenden, sicherheits- und sicherungstechnische Auswirkungen führen kann. Die resultierenden Folgen können sowohl unmittelbare Ausfälle oder Manipulationen von Komponenten bzw. vollständigen IT-Systemen sein, sowie auch zunächst unbemerkte Einflussnahmen, die längerfristig einzelne Bereiche oder Funktionen manipulieren. Zu den pfadblockierenden Faktoren zählen hauptsächlich aufdeckende Faktoren wie beispielsweise die Überprüfung von Zugriffsrechten, die im Anschluss unterbrechende Maßnahmen zur Folge haben, aber auch mitigierende Faktoren wie beschränkte Zugriffs- und Benutzerrechte.

4.3 Zusammenfassung AP 2

Mit der detaillierten Auswertung gemeldeter Ereignisse mit IT-Bezügen wurde eine solide Grundlage für die hieraus abgeleitete Entwicklung von IT-Einwirkungspfaden ermöglicht. Die Auswertung dieser Ereignisse zeigte hierbei in vielen Fällen potenzielle IT-Einwirkungen auf bzw. ermöglichte im nächsten Schritt die Ausarbeitung von detaillierten IT-Einwirkungspfaden. Durch Abstrahierung der ausgewerteten Ereignisse und der Ausarbeitung von allgemeinen Einflussmöglichkeiten, ergaben sich insgesamt 9 IT-Einwirkungspfade aus den ausgewerteten Ereignissen. Darüber hinaus wurde ein IT-Einwirkungspfad anhand der sich rapide ergebenden Nutzungsänderung in Bezug auf Fernzugriffe von IT-Systemen im industriellen Kontext entwickelt. Dieser lässt sich ebenso auf kerntechnische Anlagen übertragen, bei welchen Maßnahmen zur Etablierung von Fernzugriffen national wie international im begrenzten Kontext ergriffen werden.

5 Zusammenfassung und Ausblick

In kerntechnischen Anlagen eingesetzte IT-Systeme müssen entsprechend ihrer sicherheits- und sicherungstechnischen Bedeutung vor unerwünschten IT-Einwirkungen geschützt werden. Die Fähigkeiten und das Ausmaß von IT-Einwirkungen und der sich hieraus ergebenden 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, mit deren Umsetzung umfassende Sicherungsanforderungen für eingesetzte IT-Systeme festgeschrieben wurden. Um weiterhin die Effektivität der entsprechenden 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 der getroffenen IT-Sicherungsmaßnahmen durchzuführen.

Die Auswertung von IT-Einwirkungen auf IT-Systeme ermöglicht eine umfassende Auswertung des aktuellen Standes von Wissenschaft und Technik im Bereich der Informationssicherheit und ist damit ein wichtiger Pfeiler für die Fortschreibung bestehender Regelwerke. Bezüglich der nuklearen Sicherheit werden hierzu seit über 40 Jahren Ergebnisse in kerntechnische Anlagen national wie international berichtet und mittels einer vertieften Auswertung werden die wichtigsten Erkenntnisse aus der berichteten Betriebserfahrung bzw. Betriebsereignisse gewonnen. In der Informationssicherheit werden bisher hierzu insbesondere solche Ereignisse herangezogen, welche im nicht nuklearen Umfeld stattfinden. Hierzu zählen z. B. IT-Einwirkungen auf Pipelines, Raffinerien, Fabriken, Stromnetze und konventionelle Kraftwerke. Solche Ereignisse erfahren weltweite Beachtung, treten gehäuft auf und ermöglichen aufgrund einer zum Teil umfassenden Informationslage eine detaillierte Auswertung und damit Erfahrungsbildung. Demgegenüber ist die Anzahl der umfassend ausgewerteten IT-Ereignisse mit kerntechnischem Hintergrund deutlich reduziert. Neben dem Stuxnet Angriff im Jahr 2010 sind nur wenige IT-Ereignisse in kerntechnischen Anlagen bekannt geworden und noch weniger im Rahmen der bestehenden Reportingsysteme als Betriebserfahrung offiziell gemeldet worden.

Doch auch Ereignisse mit hauptsächlich sicherheitstechnischem Bezug aus kerntechnischen Anlagen und Einrichtungen können für die Informationssicherheit relevante Erkenntnisse liefern, wenn es sich bei den betroffenen Systemen der Anlagen um digitale

Systeme oder um Prozesse, welche typischerweise auch durch digitale Systeme in kerntechnischen Anlagen ausgeführt werden können. Daher wurden im vorliegenden Forschungsvorhaben sämtliche gemeldeten nationale und internationale betriebliche Ereignisse kerntechnischer Anlagen der Jahre 2011 bis 2021 auf solche Informationssicherheitsbezüge untersucht und entsprechend basierend auf dieser Untersuchung potenzielle IT-Einwirkungen ermittelt.

Im Arbeitspaket 1 wurden die vorliegenden Datenbanken für nationale und internationale kerntechnische Betriebsereignisse für den Zeitraum von 2011 bis 2021 auf potenzielle Bezüge zur Informationssicherheit und dem Einsatz digitaler Systeme untersucht. Hierzu wurden entsprechende wissenschaftliche Screeningmethoden angewendet. In ungefähr 4% der nationalen nach AtSMV gemeldeten Ereignisse und ca. 6% der mittels der IAEA IRS Plattform gemeldeten Betriebsereignisse wurden relevante Bezüge zur Informationssicherheit bzw. digitalen Systemen erkannt, wodurch ca. 80 Ereignisse zur Auswertung in den weiteren Arbeitspaketen vorlagen.

Im Arbeitspaket 2 wurden die 80 weiteren Ereignisse teilweise im Detail ausgewertet. Hierbei wurden insgesamt 27 weitere Detailauswertungen vorgenommen um die Ereignisse, die beteiligten digitalen Systeme, die dahinterliegenden Prozesse und die hierdurch naheliegenden IT-Einwirkungen auszuwerten. Die soweit ausgewerteten IT-Ereignisse dienten im Rahmen der Arbeiten am Arbeitspaket 2 der Ausarbeitung von insgesamt 9 IT-Einwirkungspfaden. Hierzu wurde eine Struktur für IT-Einwirkungspfade entwickelt, welche neben den für diese IT-Einwirkungspfade notwendigen und hinreichenden Bedingungen auch die Pfadanfänge, die Pfadzwischenschritte, Übergänge und Endpunkte der IT-Einwirkungspfade beschrieben. Darüber hinaus wurden potenzielle, generische Maßnahmen ausgearbeitet, welche die IT-Einwirkungspfade blockieren, detektieren und mitigieren können. Insgesamt wurden durch diese Arbeiten die folgenden 9 IT-Einwirkungspfade aus gemeldeten Ereignissen kerntechnischer Anlagen abgeleitet:

- Servicegeräte
- Unerkannte IT-Komponenten
- Überlastung von IT-Systemen
- Lieferkette
- Wechseldatenträger
- Versionenmanagement
- Parametrierung und Konfiguration
- Innentäter

Darüber hinaus wurde den schnellen Entwicklungen im modernen Arbeitsumfeld im Rahmen der COVID-19 Pandemie Rechnung getragen und sich vertieft mit den Auswirkungen der Etablierung von Fernzugriffen, Homeoffice und mobilen Arbeiten auf kerntechnische Anlagen beschäftigt. Hierzu wurde eine Cybersicherheitskonferenz im Rahmen des Vorhabens besucht und auf Basis der entsprechenden Erkenntnisse dieser ein zehnter IT-Einwirkungspfad „Fernzugriffe“ entwickelt, der den auch in kerntechnischen Anlagen stattfindenden Trend zur Fernarbeit in die Arbeiten des Vorhabens einfließen lässt.

Insgesamt zeigte sich im Rahmen des Vorhabens, dass mit der Auswertung von kerntechnischen Ereignissen aus Sicht der Informationssicherheit und der hieraus konsequent entwickelten IT-Einwirkungspfade eine Möglichkeit zur technisch-wissenschaftlichen Bewertung und Abgleich bestehender Informationssicherheitsanforderungen und Regelwerke entwickelt werden kann.

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/ BMU, Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen und sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)

/BMU13n04/ BMU, Lastannahmen zur Auslegung kerntechnischer Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter mittels IT-Angriffen (IT-Lastannahmen), VS-Vertraulich, 08.07.2013

/BMU13n05/ BMU, 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/ 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

Tabellenverzeichnis

Abbildungsverzeichnis

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

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

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

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

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

www.grs.de

ISBN 978-3-910548-95-4