Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

NRL
Norddeutsches
RealLabor

Arbeitspapier im Rahmen des
Norddeutschen Reallabors

Bedrohungsszenarien für Energieinfrastrukturen

Tom Petersen, Joshua Stock, Hannes Federrath

Universität Hamburg

Fachbereich Informatik

Arbeitsbereich SVS

28. Juli 2023

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Zusammenfassung

Gegenwärtig unterliegt der Energiesektor, wie viele andere Bereiche auch, einer zunehmenden Digitalisierung und Vernetzung, unter anderem vorangetrieben durch die Energiewende und zahlreiche Projekte im Rahmen der Sektorenkopplung. Potenzielle Sicherheitsrisiken in Energieanlagen und -netzen, die durch die Umstellung auf digitale Prozesse entstehen können, sollten von vornherein minimiert werden. Ansonsten ergeben sich Bedrohungsszenarien, die im schlimmsten Fall auch Auswirkungen auf die Stabilität der Energieversorgung haben können.

Ziel dieses Arbeitspapiers ist es, einen Überblick über aktuelle Bedrohungsszenarien im Kontext von Sicherheit für Information Technology (IT) und Operational Technology (OT) in Energieinfrastrukturen zu geben. Hierzu werden existierenden Forschungsarbeiten und Empfehlungen, bekannt gewordene Angriffe auf Energieinfrastrukturen und Erkenntnisse, die im Rahmen von Umfragen im Projekt Norddeutsches Reallabor gewonnen wurden, aufgearbeitet und eingeordnet.

Über das Norddeutsche Reallabor

Das Projekt Norddeutsches Reallabor (NRL) ist ein innovatives Verbundprojekt, das neue Wege zur Klimaneutralität aufzeigt. Dazu werden Produktions- und Lebensbereiche mit besonders hohem Energieverbrauch schrittweise defossilisiert – insbesondere in der Industrie, aber auch in der Wärmeversorgung und dem Mobilitätssektor. Hinter dem im April 2021 gestarteten Projekt steht eine wachsende Energiewende-Allianz mit mehr als 50 Partnern aus Wirtschaft, Wissenschaft und Politik. Das Großprojekt hat eine Laufzeit von fünf Jahren (04/2021-03/2026). Dabei beträgt das Investitionsvolumen der beteiligten Partner rund 405 Mio. Euro. Als Teil der Förderinitiative „Reallabore der Energiewende“ wird das Projekt mit rund 55 Mio. Euro durch das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert. Weitere Fördermittel werden durch das Bundesministerium für Digitales und Verkehr (BMDV) bereitgestellt. Das NRL versteht sich als ausbaufähige Plattform für weitere Projekte. www.norddeutsches-reallabor.de

Über den Arbeitsbereich Sicherheit in verteilten Systemen

Der Arbeitsbereich Sicherheit in verteilten Systemen (SVS) am Fachbereich Informatik der Universität Hamburg (UHH) unter der Leitung von Prof. Dr. Hannes Federrath verfügt über umfangreiche Erfahrungen in der Konstruktion sicherer und datenschutzgerechter IT-Systeme. Die am Lehrstuhl vorhandene Kompetenz im Bereich Informationssicherheit deckt sowohl übergreifende Aspekte der IT-Sicherheit wie Sicherheitsmanagement und wirtschaftliche Aspekte der Informationssicherheit als auch Techniken der IT-Sicherheit ab. Einen Schwerpunkt bildet dabei Grundlagenforschung zu datenschutzfreundlichen Techniken und deren Einsatz in verschiedenen Anwendungskontexten.

Innerhalb des NRL-Projektes widmet sich SVS in Teilvorhaben 2.2 der Sicherheit von IT- und OT-Systemen im Rahmen der Sektorenkopplung.

Inhaltsverzeichnis

Akronyme

AMI Advanced Metering Infrastructure 9

APT Advanced Persistent Threat 9, 19

BMDV Bundesministerium für Digitales und Verkehr 2

BMWK Bundesministerium für Wirtschaft und Klimaschutz 2, 33

BSI Bundesamt für Sicherheit in der Informationstechnik 12–14, 29, 31

DDoS Distributed Denial of Service 13, 15, 24, 30

DER Distributed Energy Resources 9

DGM Distribution Grid Management 9, 10

DR Demand Response 10

DSO Distribution System Operator 9

EE Erneuerbare Energien 6, 10

EECSP Energy Expert Cyber Security Platform 11

ET Electric Transportation 10

EWS Engineering Workstation 15

GEN Generation 10

GPS Global Positioning System 14

ICS Industrial Control System 6, 8, 12–20

IDS Intrusion Detection System 8

IEA International Energy Agency 14

IKT Informations- und Kommunikationstechnik 26, 29

IoT Internet of Things 14, 24

IT Information Technology 2, 6–8, 11, 12, 14–16, 19–21, 26, 27, 29, 30

NESCOR National Electric Sector Cybersecurity Organization Resource 9, 11

NIST National Institute of Standards and Technology 14

NRL Norddeutsches Reallabor 2, 7, 26, 30

OT Operational Technology 2, 6–8, 11, 16, 19, 26–30

PLC Programmable Logic Controller 6

SCADA Supervisory Control and Data Acquisition 6, 9, 18, 19, 23

SIDATE Sichere Informationsnetze bei kleinen und mittleren Energieversorgern 12

SVS Sicherheit in verteilten Systemen 2

UHH Universität Hamburg 2

UP-KRITIS Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland 29

USB Universal Serial Bus 19, 28

VoIP Voice over IP 28

VPN Virtual Private Network 25, 27

WAMPAC Wide Area Monitoring, Protection, and Control 9, 10

1 Einleitung/Hintergrund

Im Rahmen der Energiewende und mit der Umstellung von mit fossilen Energieträgern betriebenen Großkraftwerken hin zu kleineren, häufig dezentralen Anlagen aus dem Bereich der Erneuerbare Energien (EE) und Energiespeichern kommt der Digitalisierung und Vernetzung der Anlagen zum Zweck der Überwachung und Steuerung der Energieinfrastruktur eine immer größere Rolle zu, um durch bedarfsgerechte Energiebereitstellung und -verbrauch die Netzstabilität sicherzustellen [MRS22]. Die damit verbundene verstärkte Nutzung digitaler Technologien birgt jedoch auch eine steigende Gefahr von Angriffen auf die digitale Infrastruktur mit sich, die im schlimmsten Fall auch Auswirkungen auf die Stabilität der Energieversorgung haben können. Die Bandbreite der Angreifer reicht dabei von Script-Kiddies über eigene Mitarbeiter bis hin zu professionellen Hackergruppen oder sogar staatlichen Akteuren [Cou16].

Der Einsatz von Digitalisierungstechnologie in Energieinfrastrukturen – von Kraftwerken bis hin zu Pipelines – lässt sich grundsätzlich in die zwei Bereiche Information Technology (IT) (im Deutschen *Informationstechnik*) und Operational Technology (OT) (im Deutschen *Betriebstechnik*) einteilen. IT bezeichnet hierbei Hardware und Software, die für die Speicherung, Übertragung und Verwendung von Informationen für Zwecke des Geschäftsbetriebs genutzt wird. OT hingegen beschreibt Hardware und Software, die mit Komponenten gekoppelt sind, die Veränderungen in der physikalischen Welt hervorrufen können, etwa für die Prozessautomatisierung [Cyb20]. Hierunter fallen auch Industrial Control Systems (ICSs) – Systeme wie Supervisory Control and Data Acquisition (SCADA) und Programmable Logic Controllers (PLCs), die geschäftskritische Industrieprozesse überwachen und steuern. Die beiden Technologiearten unterscheiden sich im Allgemeinen stark in ihren Eigenschaften [AHT17], unter anderem bezüglich Echtzeit- und Verfügbarbarkeitsanforderungen, Ressourcenverfügbarkeit, Sicherheitsmechanismen und Lebensdauer. Mit der eingangs beschriebenen stärkeren Vernetzung und Fernsteuerbarkeit von Anlagen wird die auch externe Steuerbarkeit von OT-Komponenten immer häufiger notwendig, die meist über einen Zugriff aus dem IT-Bereich des Anlagenbetrei-

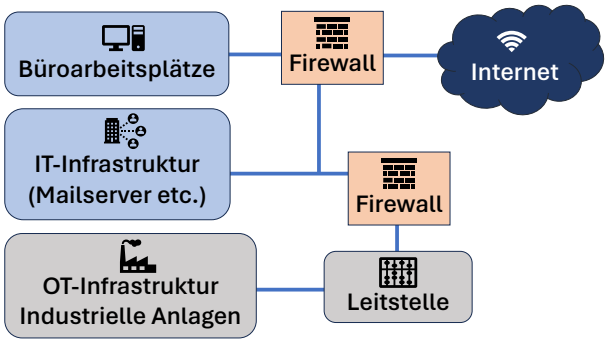

Abbildung 1.1: Beispielhafte Netzwerkstruktur für ein Unternehmen mit Energieanlagen.

bers stattfindet. Eine typische Architektur für die IT-/OT-Infrastruktur einer Anlage ist in Abbildung 1.1 dargestellt.

In diesem Arbeitspapier werden Bedrohungsszenarien für Energieanlagen betrachtet, die sich auf die IT und OT der Anlagen beziehen. Dazu wird in Kapitel 2 eine Übersicht über verwandte Arbeiten aus Forschung und Praxis bereitgestellt. Kapitel 3 bietet eine Übersicht über bekannt gewordene Angriffe im Energiebereich. In Kapitel 4 stellen wir die wichtigsten Erkenntnisse aus Interviews vor, die mit Partnern im Rahmen des Norddeutsches Reallabor (NRL)-Projekts geführt wurden.

2 Wichtige Vorarbeiten

In diesem Kapitel werden existierende Arbeiten aus Forschung und Praxis zu Bedrohungen in Energieinfrastrukturen vorgestellt. Einige Arbeiten befassen sich auch allgemeiner mit der Sicherheit industrieller Steueranlagen (ICS), die eine der zentralen Komponente in Energieanlagen und -netzen darstellen und deshalb ebenfalls betrachtet werden.

2.1 Studie zu Risiken von IT/OT-Sicherheitsvorfällen im Energiesektor

Eine 2018 veröffentlichte Studie von Fischer u. a. [Fis+18] befasst sich mit der IT/OT-Sicherheit im europäischen Energiesystem. Neben dem im Folgenden fokussierten Abschnitt zu Bedrohungen werden weiterhin geeignete Maßnahmen und Regelwerke sowie Ansätze für die Risikoanalyse, Wirtschaftlichkeitsbetrachtungen für IT-Sicherheit und Regulierungsempfehlungen betrachtet.

In einem ersten Abschnitt werden Trends im Energiesektor und ihre Auswirkungen auf die IT/OT-Sicherheit betrachtet. Hier erwähnen die Autoren zu Beginn eine zunehmende Digitalisierung im Energiesektor und eine damit einhergehende stärkere Verbindung von IT- und OT-Komponenten. Für viele dieser OT-Komponenten war ursprünglich keine Vernetzung vorgesehen. Spezifische Risiken, die hier auftreten, liegen auch darin begründet, dass ICS während Wartung, Updatevorgängen und anderen Ausnahmesituationen teilweise erreichbar bleiben müssen, um das Energiesystem in einem operativen Zustand zu halten. Weiterhin sind lange Lebensdauern verwendeter Komponenten von 30 bis 50 Jahren keine Seltenheit, so dass geeignete Sicherheitsmaßnahmen veraltete, nicht leicht zu ersetzende, verwundbare und teilweise nicht mehr updatebare Systeme schützen müssen. Als weitere Besonderheit des Stromnetzes wird auch die spezifische Gefahr von Kaskadenabschaltungen erwähnt, die im schlimmsten Fall zu großflächigen und langanhaltenden Stromausfällen führen können.

In der Studie werden Bedrohungsszenarien exemplarisch herausgearbeitet, die entweder bereits in der Vergangenheit aufgetreten sind oder die aus Sicht der Autoren bisher nicht ausreichend bedacht wurden – gerade in Bezug auf neuartige Technologien. Genannt werden hier „mobile computing and remote access, security measures (intrusion detection and prevention systems used for zone protection), dynamic software updates, and finally cross-sector communication“. Die folgenden 11 Bedrohungsszenarien werden in dem Bericht detailliert betrachtet:

1. Infektionen mittels des Intrusion Detection System (IDS)
2. Virus- oder Trojanerinfektion von ICSs
3. Social Engineering: Phishing-Angriffe auf Unternehmensebene führen zu Manipulationen auf Feldebene
4. Kompromittierte Firmware-Updates, um einzelne Umspannwerke zu beeinflussen

5. Branchen- und grenzüberschreitende Überlastungsangriffe
6. Kompromittierung von Anlagen über die SCADA-App
7. Advanced Persistent Threat (APT)-Angriff gegen Distribution System Operator (DSO) Flexibilitätsmanagementsystem
8. Anlagenausfall durch Störung von Kommunikationsverbindung zu Geräten
9. Kompromittierung von Distribution Grid Management (DGM) durch Supply-Chain-Angriffe
10. Geschwächte Sicherheit während Katastrophen
11. Unbefugte massenhafte Trennung von Kommunikationsverbindungen durch Firmware-Updates

2.2 NESCOR-Störungsszenarien

Im Rahmen des National Electric Sector Cybersecurity Organization Resource (NESCOR)-Projekts wurde eine Übersicht über Bedrohungen im Energiesektor erstellt [Ins15b]. Die Autoren stellen Bedrohungsszenarien in acht Kategorien bereit, die verschiedenen Gebieten in dem Energiesystem entsprechen. Es werden sowohl böswillig hervorgerufene als auch unbeabsichtigte IT-Sicherheitsvorfälle betrachtet, u.a. Kompromittierung von Geräten, Angriffe auf Datenintegrität, Kommunikationsausfälle, menschliches Fehlverhalten und Naturkatastrophen. Es wird allerdings auch darauf hingewiesen, dass die Ausarbeitung keine vollständige Auflistung aller potentiellen Bedrohungsszenarien darstellt, sondern lediglich eine repräsentative Auswahl von Bedrohungen im Energiebereich darstellt.

- **Advanced Metering Infrastructure (AMI)**: Hierunter versteht man fortschrittliche Verbrauchsmesssyteme, die basierend auf von Smart Metern gemessenen Verbrauchsdaten etwa dynamische Strompreisgestaltung in Echtzeit ermöglichen. Diese Kategorie enthält 32 Bedrohungsszenarien, die Systeme in dieser Infrastruktur fokussieren.
  Beispiel AMI.24: Der Einsatz unsicherer kryptographischer Algorithmen erlaubt den Zugriff auf und die Veränderung von Daten oder Konfigurationen in AMI-Geräten.
- **Distributed Energy Resources (DER)**: Diese Kategorie beschreibt typischerweise kleinere Systeme, die Energie und Hilfsdienste für das Stromnetz bereitstellen, etwa kleine Solar- oder Windfarmen oder Batteriespeicher, die mit dem Stromnetz verbunden und typischerweise steuerbar sind. Sie enthält 26 Bedrohungsszenarien.
  Beispiel DER.14: Ein Angreifer fälscht SCADA-Steuerbefehle, um eine gleichzeitige Notabschaltung vieler DER-Systemen zu erreichen.
- **Wide Area Monitoring, Protection, and Control (WAMPAC)**: Unter diese Kategorie fallen verteilte Monitoring- und Steuersysteme, die es anhand einer Vielzahl verteilter Sensoren im Stromnetz ermöglichen, schnell auf lokale Ereignisse zu reagieren und zu einer verbesserten Netzstabilität beizutragen. Diese Kategorie enthält 12 Bedrohungsszenarien.

Beispiel WAMPAC.11: Ein böswilliger Insider verzögert den lokalen Austausch von Messdaten zwischen Umspannwerken, etwa indem er die WAMPAC-Kommunikationsverbindung mittels eines Flooding-Angriffs belastet.

- **Electric Transportation (ET)**: Diese Kategorie enthält 16 Bedrohungsszenarien, die den Bereich der E-Mobilität und elektrischer Ladesäulen fokussieren.
  Beispiel ET.2: Ein Angreifer kompromittiert ein Managementsystem für Schnellladestationen und modifiziert die Ladesäulern derart, dass das Schnellladen für alle Elektrofahrzeuge gleichzeitig beginnt, wodurch der Verteilertransformator überlastet wird und einen lokalen Ausfall verursacht.
- **Demand Response (DR)**: Diese Kategorie enthält 7 Bedrohungsszenarien, die die Interaktionen zwischen Strommärkten, Stromversorgern, Aggregatoren sowie Endverbrauchern fokussieren.
  Beispiel DR.2: Ein Angreifer belauscht den nicht ausreichend geschützten Netzwerkverkehr zwischen einem Demand Response Automation Server und einem Kundensystem und kann auf private Kundeninformationen zugreifen.
- **DGM**: Unter DGM versteht man die (automatisierte) Kontrolle von Einspeisungen und Übertragungen in Verteilnetzen (Smart Grids) zum Zweck von erhöhter Netzzuverlässigkeit, Verringerung von Lastspitzen und besserer Integration verteilter EE-Anlagen. In dieser Kategorie sind 16 Bedrohungsszenarien enthalten.
  Beispiel DGM.1: Ein Angreifer verwendet einen Störsender für drahtlose Signale, um drahtlose Kommunikationskanäle zu unterbrechen, die zur Überwachung und Steuerung von Verteilnetzen und Umspannwerken verwendet werden.
- **Generation (GEN)**: Diese Kategorie enthält 16 Bedrohungsszenarien, die Großanlagen der Energieerzeugung fokussieren und die von lokalen Einflüssen auf Geschäftsprozesse bis hin zu netzstabilitätsgefährdenden Szenarien reichen.
  Beispiel GEN.10: Ein Angreifer verschafft sich physischen Zugriff auf die Sprach- und Datenkommunikationsleitungen zwischen Übertragungsnetzbetreiber und Anlagenbetreiber und übt einen Man-in-the-Middle-Angriff aus. Der Angreifer sendet fehlerhafte Signale an die Anlage, um die Leistungsabgabe während einer Zeit hoher Netzlast schnell zu drosseln. Unzureichende Leistung und hohe Last führen zu Netzinstabilität.
- **Generic**: Diese Kategorie enthält 4 Bedrohungsszenarien, die übergreifende Aspekte abdecken.
  Beispiel Generic.2: Ein Angreifer kompromittiert über das Internet ein System im Büronetz, das auch Zugriff auf Steuerungssysteme besitzt. Diese Kompromittierung bietet dem Angreifer einen Dreh- und Angelpunkt, um die Kontrolle über Steuersysteme zu erlangen.

Für jedes dieser Bedrohungsszenarien werden eine detaillierte Beschreibung, relevante Schwachstellen, die Auswirkungen und mögliche Maßnahmen zur Reduzierung des Risikos angegeben. Weiterhin wurden die relevanten Schwachstellen analysiert und zur besseren Übersicht in Klassen eingeteilt. Dies ergab die am häufigsten betrachteten Schwachstellenklassen *Unzureichendes Änderungs- und Konfigurationsmanagement*, *nicht-notwendiger Systemzugriff*, *Schwächen im Authentifizierungsprozess oder in Authentifizierungsschlüsseln* und *Verwendung unsicherer Protokolle*.

Im Rahmen einer weiteren Veröffentlichung innerhalb des NESCOR-Projekts wurden einige der Bedrohungsszenarien noch detaillierter analysiert [Ins15a].

2.3 EECSP-Empfehlungen zur IT/OT-Sicherheit im Energiesektor

In [Eur17] arbeitet die Experten-Gruppe der Energy Expert Cyber Security Platform (EECSP) der europäischen Kommission Empfehlungen für einen strategischen Rahmen und gesetzliche Änderungen bezogen auf die IT/OT-Sicherheit für den europäischen Energiesektor vor. Im Rahmen der Veröffentlichung werden auch Trends im Energiesektor unter anderem bezüglich der IT/OT-Sicherheit betrachtet, von denen relevante Trends im Folgenden dargestellt werden sollen.

Im Gegensatz zu traditionellen Investitionszyklen im Energiebereich (Gerätelebensdauern von bis zu 40 Jahren), kommen vermehrt normale IT-Komponenten zum Einsatz, etwa zum Zweck erhöhter Verfügbarkeit und Resilienz des Energiesektors durch verbesserten Informationsaustausch und stärkere Automatisierung. Die Integration dieser Komponenten bringt jedoch nicht nur aus dem IT-Umfeld bekannte Schwachstellen mit, sondern setzt häufig auch Altsysteme neuen Bedrohungen aus, die zur Zeit der Herstellung dieser Geräte nicht in Erwägung gezogen wurden. Altsysteme sind häufig nicht mehr leicht an neue Sicherheitsstandards anzupassen. Weiterhin sind auch Anforderungen an die Verfügbarkeit, etwa keine verfügbaren Wartungsfenster im Dauerbetrieb, dafür verantwortlich, dass Schwachstellen in diesen Altsystemen nur schwer zu beheben sind. Hier besteht außerdem das Problem, dass gängige Sicherheitsmaßnahmen im IT-Bereich nicht mit diesen Verfügbarkeitsanforderungen kompatibel sein können.

Zusätzlich zu neuen Komponenten findet auch eine immer stärkere Vernetzung zwischen Strommarktteilnehmern und eine Automatisierung der Marktprozesse statt, um z.B. dynamischere Energiepreise zu ermöglichen. Diese gesteigerte Komplexität erhöht auch das inhärente Risiko für Störungen der Netzstabilität.

Ein weiterer Trend ist die immer stärkere Nutzung von externen Dienstleistern (etwa für Daten- oder Kommunikationsdienste). Problematisch kann hier die Abhängigkeit des Energiesektors von Sektoren sein, in denen Verfügbarkeits- und Integritätsanforderungen weniger stark ausgeprägt sind (siehe auch Abschnitt 3.3).

Aber nicht nur externe Dienstleister sondern auch externe Hersteller von Hard- und Software können eine Bedrohung darstellen. Die Verwendung von Komponenten, die durch einen böswilligen Hersteller oder durch eine dritte Partei korrumpiert wurden (etwa durch Einbringen von Backdoor-Funktionalität), kann Angreifern verschiedene Möglichkeiten bieten, Schäden hervorzurufen. Dies bezieht sich nicht nur auf Komponenten für die Industriesteuerung, sondern auch auf alle anderen Komponenten, etwa auch Sicherheitskomponenten, die eigentlich dem Schutz von Anlagen oder Netzen dienen sollen.

2.4 Umfrageergebnisse des SIDATE-Projekts

Im Rahmen des Projekts Sichere Informationsnetze bei kleinen und mittleren Energieversorgern (SIDATE) wurden 2016 deutsche Stromnetzbetreiber zum Stand der IT-Sicherheit befragt (881 kontaktiert, 61 Teilnehmer) [Dax+17]. Für dieses Arbeitspapier relevante Ergebnisse werden im Folgenden kurz zusammengefasst.

Der überwiegende Teil der befragten Unternehmen setzte unabhängige Dienstleister im Bereich der IT-Sicherheit ein. Dies zeigt, dass die Bedrohung durch Supply-Chain-Angriffe (siehe auch Abschnitt 3.3) auch in Bezug auf Dienstleister betrachtet werden muss. Gerade bei kleineren Betreibern kann so durch die Externalisierung von Sicherheitsdienstleistungen (aufgrund von nicht-existenter eigener Expertise) eine neue Angriffsfläche geschaffen werden. Fernzugriffe durch diese Dienstleister können in seltenen Fällen vollständig eigenständig erfolgen, zumeist jedoch erst nach vorheriger Authorisierung und im besten Fall nur mit zusätzlicher Überwachung des Zugriffs.

Bei einem kleinen Teil der befragten Unternehmen existieren keine Sicherheitsrichtlinien für die Büro-IT-Systeme oder die existierenden Sicherheitsrichtlinien werden nicht regelmäßig überprüft und ggf. angepasst. Im Vergleich dazu existieren lediglich bei der Hälfte der befragten Unternehmen Sicherheitsrichtlinien für den Bereich des Leitsystems.

Der überwiegende Teil der befragten Unternehmen verwendet das Leitsystem auch für die aktive Steuerung der Netze und nicht nur ihre Überwachung. Insbesondere vor diesem Hintergrund ist eine Trennung der Netzbereiche (Leitsystem, Büro-IT, ...) essentiell. Der größte Teil der Unternehmen gab an, dass dies mittels logischer Netztrennung durchgeführt wird, und ein kleinerer Teil nutzt hierfür echte physikalische Trennung. Die Leitsysteme selbst wurden jedoch nur von etwa der Hälfte der befragten Unternehmen (insbesondere der größeren Unternehmen) in verschiedene Sicherheitsbereiche unterteilt.

Ein großer Teil der Unternehmen gab an, dass verantwortliche Mitarbeiter sich regelmäßig über Schwachstellen eingesetzter Hard- und Software informieren. Im Vergleich dazu gaben jedoch nur etwa die Hälfte der Unternehmen an, dass regelmäßige Updates durchgeführt werden, ein weiteres Vierteil zumindest bei bekannten Schwachstellen.

Als zentraler Standard für das IT-Sicherheits-Management stellt sich der ISO/IEC-27001-Standard heraus, der in knapp der Hälfte der befragten Unternehmen verwendet wird.

Die Hälfte der Unternehmen führt Risikoanalysen für ihre Prozesse und Systeme durch, wobei in vielen Fällen nicht bekannt ist, wie häufig dies geschieht. Ein etwas geringerer Anteil führt ebenfalls Sicherheitsaudits oder Penetrationstests durch (häufig unter Mitarbeit oder exklusiv durch externe Dienstleister).

2.5 BSI-Veröffentlichungen zur Sicherheit industrieller Steueranlagen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt regelmäßig eine Übersicht zu der Sicherheit von ICS, also industriellen Steuersystemen, heraus [BSI22].

Hierin wird unterschieden zwischen *primären Angriffen*, mithilfe derer Angreifer in industrielle Anlagen und Unternehmen eindringen, und *Folgeangriffen*, die Angriffe auf

Bedrohung	Trend
Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme	unverändert
Infektion mit Schadsoftware über Internet und Intranet	stark gestiegen
Menschliches Fehlverhalten und Sabotage[a]	unverändert
Kompromittierung von Extranet und Cloud-Komponenten	leicht gestiegen
Social Engineering und Phishing	unverändert
Distributed Denial of Service (DDoS)-Angriffe	unverändert
Internet-verbundene Steuerungskomponenten	leicht gestiegen
Einbruch über Fernwartungszugänge	leicht gestiegen
Technisches Fehlverhalten und höhere Gewalt	unverändert
Soft- und Hardwareschwachstellen in der Lieferkette	stark gestiegen

Tabelle 2.1: Top-10-Bedrohungen für ICSs und Trend ggü. 2019. Entnommen aus [BSI22].

a. Zur Gefährdung von ICSs durch Innentäter existiert ein eigenes vom BSI herausgegebenes Dokument [BSI18].

weitere interne Systeme darstellen. Zu den Folgeangriffen zählen etwa die Erweiterung von Rechten, der unberechtigte Zugriff auf weitere interne Systeme, der Eingriff in die Kommunikation von Steuerungskomponenten, die Manipulation von Netzwerkkomponenten oder der Einsatz von Ransomware. Die Veröffentlichung konzentriert sich jedoch auf die primären Angriffe. Eine Übersicht der größten Bedrohungen ist in Tabelle 2.1 zu finden. Für jede dieser Bedrohungen werden in der Veröffentlichung Ursachen, mögliche Bedrohungsszenarien und auch potentielle Gegenmaßnahmen aufgeführt. Im Jahr 2022 ist in der Übersicht die Bedrohung durch Hard- und Softwareschwachstellen in Lieferketten hinzugekommen, der besondere Aufmerksamkeit gewidmet werden sollte.

Weiterhin werden kurz mögliche Schadensfolgen betrachtet:

- Das Auslösen oder die Manipulation von Safety-Prozeduren oder -Systemen, was zu Schaden an Mensch und Umwelt, Produktionseinbußen oder physischen Schäden an Anlagen führen kann.
- Die Störung der Verfügbarkeit des ICS mit der Folge potentieller Produktionseinbußen.
- Datenabfluss einhergehend mit dem Verlust von Know-how (Intellectual Property).
- Die Manipulation von Systemen oder Parametern, was zu einer Minderung der Qualität von Erzeugnissen führen kann.

Schlussendlich enthält die Veröffentlichung auch noch einen Test zur Selbsteinschätzung des Sicherheitsniveaus in Unternehmen.

2.6 Das ICS-Security-Kompendium des BSI

Im *ICS-Security-Kompendium* [BSI13] beschäftigt sich das BSI mit Sicherheitsaspekten von ICSs. Die Veröffentlichung des BSI soll nun als Grundlagenwerk[1] für die Sicherheit von ICSs dienen. Nach einer Einführung in die Grundlagen von ICSs und der IT-Sicherheit sowie in geltende Standards werden Best Practices für Betreiber erarbeitet und ein Konzept vorgestellt, das dem Audit von ICS-Installationen dienen soll.

Im Rahmen unserer Übersicht ist insbesondere eine Darstellung von Gefährdungen für ICSs von Interesse. Während ICSs früher im Normalfall entkoppelt von anderen Systemen betrieben wurden, werden sie heute vermehrt mit anderen Systemen auch über Netzgrenzen hinweg vernetzt, was zu mit klassischen IT-Systemen vergleichbaren Gefährdungen führt. Diesen Systemen gegenüber haben ICSs jedoch andere Anforderungen, etwa in Bezug auf Echtzeitanforderungen, längere Betriebszeiten oder kürzere und seltenere Wartungsfenster. Zusätzlich wird insbesondere auch darauf hingewiesen, dass veraltete Protokolle aus der Zeit unvernetzter Systeme häufig Aspekte der IT-Sicherheit nicht in ihren Anforderungen berücksichtigten. Daher lassen sich etablierte Schutzmaßnahmen in klassischen IT-Systemen nicht immer direkt übertragen.

Das BSI unterscheidet drei Arten von Gefährdungen: *organisatorische Gefährungen*, *menschliche Fehlhandlungen* und *vorsätzliche Handlungen*. Tabelle 2.2 stellt eine Übersicht über verschiedene Gefährungen bereit, die sich in diese Klassen einteilen lassen.

2.7 IEA: Resilienz in Energiesystemen

Die International Energy Agency (IEA) beschreibt in [Age21] Möglichkeiten dazu, die Resilienz von IT/OT-Komponenten in elektrischen Energiesystemen zu vergrößern. Hierbei geht ein Kapitel auch auf Bedrohungsszenarien und Vorfälle ein. Es wird darauf hingewiesen, dass über alle Wertschöpfungsketten (Erzeugung, Übertragung, Verbrauch) und Lieferketten im Energiesektor hinweg Bedrohungen und Schwachstellen existieren. Während alle Bereiche im Energiesektor potenziell von einer stärkeren Digitalisierung profitieren können, steigert dies auch die Bedeutung der Vermeidung entsprechender Bedrohungen.

Die Autoren weisen insbesondere auf einige Bedrohungen hin, die in der Zukunft vermutlich stärker im Fokus stehen werden:

- Die Übernahme von vielen vernetzten Internet of Things (IoT)-Geräten mit hohem Energiebedarf durch einen Angreifer: Hierdurch könnte ein Angreifer durch koordiniertes Vorgehen starke Schwankungen in den Energienetzen hervorrufen.
- Das Spoofen von Global Positioning System (GPS)-Signalen, die vermehrt für Funktionalitäten in der Erzeugung, Übertragung und Verteilung in Energienetzen eingesetzt werden.

1. Eine vergleichbare Publikation wurde auch durch das National Institute of Standards and Technology (NIST) erstellt [Sto+15]. Anhang C dieser Veröffentlichung beschäftigt sich mit konkreten Bedrohungen für ICS.

Organisatorische Gefährdungen	Menschliche Fehlhandlungen	Vorsätzliche Handlungen
Unzureichende Regelungen zur IT-Security	Unzureichende Absicherung oder zu weitreichende Vernetzung	Kommunikation von Mess- und Steuerwerten
Unzureichende Dokumentation	Mangelhafte Konfigurationen von Komponenten	Ermitteln von Zugangsdaten mittels Wörterbuch- und Brute-Force-Angriffen
Unvollständige Absicherung der Fernwartungszugänge	Fehlende Backups	Systematische Schwachstellensuche über das Netzwerk
Einsatz von Standard-IT-Komponenten mit bereits identifizierten Schwachstellen	Mobile Datenträger und Laptops	DDoS-Angriffe
Fehlende Überwachung der unterstützenden Infrastruktur	Unzureichende Validierung von Eingaben und Ausgaben	Man-in-the-Middle-Angriff
	Abhängigkeiten des ICS-Netzes von IT-Netzen	Phishing
	Mangelnde Awareness	Injection-Angriffe
		Cross-Site-Scripting
		Drive-By-Downloads
		Schadsoftware auf Engineering Workstation (EWS)
		Schadprogramme
		Replay-Angriff
		Physischer Angriff zur Provokation administrativer Eingriffe

Tabelle 2.2: Übersicht zu Gefährdungen für ICSs. Basiert auf [BSI13].

- Schwächen in den Lieferketten für Hard- und Software: Hier werden beispielhaft Backdoors in Hardwarekomponenten und die Kompromittierung von Übertragungskanälen für die Bereitstellung von Firmware-Updates genannt.
- Innentäterbedrohungen: Hierunter fallen sowohl unabsichtliches Fehlverhalten, etwa das Klicken auf einen Phishing-Link, als auch absichtliches Fehlverhalten, etwa die Weitergabe von Betriebsgeheimnissen. Neben Unternehmensangestellten sind hier auch Auftragsnehmer mit Zugriffsrechten zu beachten.

2.8 Sicherheitsbedrohungen für Kanadas Energiesystem

Das *Canadian Centre for Cyber Security* betrachtet in [Cyb20] im Jahr 2020 aktuelle Bedrohungen für den kanadischen Elektrische-Energie-Sektor. Es werden insbesondere Aktivitäten durch Kriminelle (häufig in Form von Ransomware-Angriffen) und durch staatliche Akteure (entweder zum Zweck der Informationsgewinnung oder mit dem Ziel durch Installation von geeigneten Tools den Zugriff für weitere Aktivitäten zu erhalten) beobachtet.

Zwei Bedrohungsfelder werden in dem Bericht hervorgehoben und detaillierter betrachtet. Das erste dieser Felder befasst sich mit Angriffen auf Lieferketten oder Dienstleister der Energieunternehmen. Diese Angriffe haben im Normalfall folgende Zwecke: Die Entwendung von geistigem Eigentum, die Beschaffung von Informationen über im Zielunternehmen zum Einsatz kommende Komponenten wie ICSs sowie die Schaffung einer Zugriffsmöglichkeit auf das Unternehmensnetz über den Zugang Dritter. Bei diesen Zugängen können entweder Hard- oder Softwarekomponenten, die dem Zielunternehmen durch Dritte bereitgestellt werden, kompromittiert werden (etwa durch die Änderung von Softwareupdates) oder bestehende Zugriffsrechte Dritter auf die Netze des Zielunternehmens ausgenutzt werden (etwa Fernwartungszugänge). Angriffe auf Lieferketten bieten Angreifern häufig auch die Möglichkeit, ihre Angriffe besser zu skalieren, da ein erfolgreicher Angriff auf eine Partei in der Lieferkette potenziell viele Zielunternehmen betreffen kann.

Das zweite Feld behandelt die steigende Verwundbarkeit von ICSs. Die steigende Einbindung früher autark betriebener OT-Komponenten in IT-Netze („OT/IT convergence“), etwa zum Zwecke vereinfachter Verwaltung oder Beobachtung dieser Komponenten, setzt sie vermehrt gängigen Bedrohungen etwa aus dem Internet aus. Insbesondere auch der Trend zu *Smart Grids*, die eine intelligente Echtzeit-Anpassung der Energienetze an aktuelle Bedarfe versprechen, verstärkt diesen Trend durch eine stärkere Vernetzung, höhere Komplexität und mehr Abhängigkeiten in den Lieferketten.

Eine zusammenfassende Übersicht über mögliche Angriffswege bietet Abbildung 2.1.

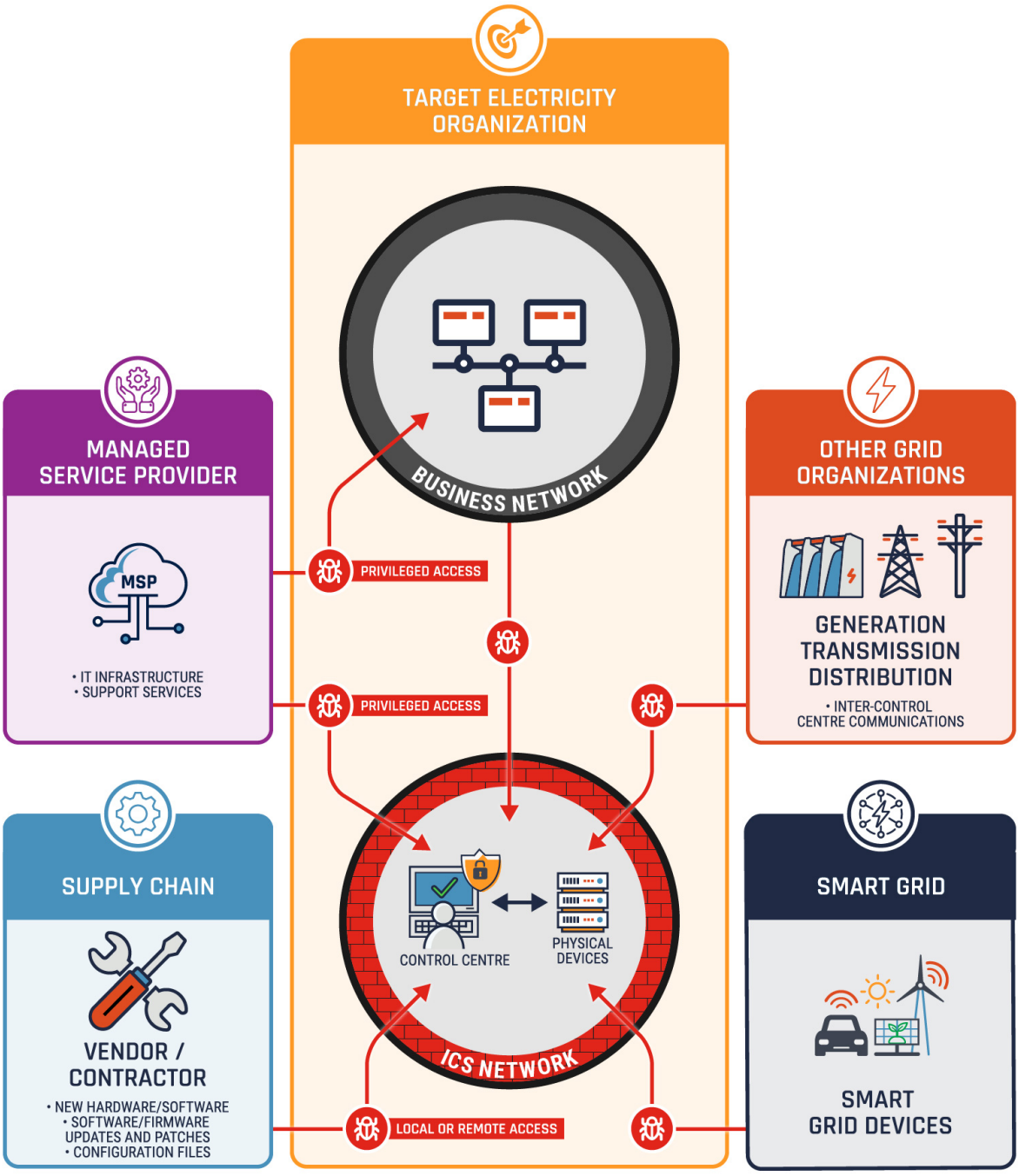

Abbildung 2.1: Potentielle Angriffswege auf das ICS-Netzwerk eines Unternehmens der Energiebranche. Entnommen aus [Cyb20].

3 Angriffsübersicht

In diesem Kapitel wird eine Übersicht zu Angriffen auf Energieinfrastrukturen bereitgestellt. Hierbei handelt es sich allerdings nur um Angriffe, die erstens überhaupt entdeckt und zweitens öffentlich geworden sind. Dass dies nur eine kleine Teilmenge aller Angriffe darstellen dürfte, zeigt eine Studie von Kaspersky [Kas19], wonach zwei Drittel aller betroffenen Unternehmen (entdeckte) Sicherheitsvorfälle nicht an Regulatoren melden, selbst wenn sie dazu gesetzlich verpflichtet sind. Als Gründe werden insbesondere die Vermeidung von Strafen und der potentielle öffentliche Vertrauensverlust im Falle der Veröffentlichung genannt.

Die folgende Übersicht teilt die Angriffe in sieben Kategorien nach ihrem Hauptangriffsvektor ein. Diese Kategorisierung ist keineswegs trennscharf zu verstehen. Etwa wurde 2015 im Rahmen eines Angriffs auf ukrainische Energieinfrastruktur letztlich eine ICS-Malware genutzt, die zum Ausfall der Stromversorgung führte. Für diesen finalen Schritt kamen jedoch weitere Angriffstechniken wie Spearfishing und mit Malware versehene Office-Dokumente zum Einsatz.

Weitere Übersichten zu Angriffen in Energieinfrastrukturen und im industriellen Bereich, die teilweise für dieses Kapitel herangezogen wurden, sind in [Fis+18; Age21; Cou16] zu finden.

3.1 ICS-Malware

Bei ICS-Malware handelt es sich um Schadsoftware, die sich explizit gegen industrielle Steueranlagen richtet. Angriffe dieser Kategorie erfordern im Normalfall vertieftes Angreiferwissen und eine lange Vorbereitung, da Spezifika der ICSs, verwendeter Kommunikationsprotokolle und ihrer Einsatzumgebung in Erfahrung gebracht werden müssen und Schadsoftware für diese Systeme entwickelt werden muss. Anschließend ist es notwendig diese Schadsoftware auf die Zielsysteme zu bringen, die häufig durch eine Vielzahl von Schutzmaßnahmen (etwa Netztrennung bis hin zu „airgapped“ Betrieb) gesichert sind.

3.1.1 Stuxnet

Stuxnet [FMC10] war eine Malware, die 2010 auf spezifische SCADA-Systeme der Firma Siemens abzielte, die u. a. in der iranischen Urananreicherungsanlage Natanz eingesetzt wurden. Ziel von Stuxnet war es, unentdeckt so in die Frequenzsteuerung der eingesetzten, mittels SCADA-Systemen gesteuerten Zentrifugen einzugreifen, dass die Zentrifugen langfristig beschädigt wurden. Mutmaßlich wurde Stuxnet von den USA und Israel entwickelt, um das iranische Atomprogramm zurückzuwerfen.

Da die Zielsysteme nicht mit dem Internet verbunden (*airgapped*) waren, kompromittierte Stuxnet Windows-Rechner, auf denen Software für die Programmierung der SCADA-Systeme installiert war. Hierbei wurden verschiedene Zero-Day-Exploits in Windows und auch eine Selbstverbreitung der Malware über lokale Netze und mittels Kompromittierung von Universal Serial Bus (USB)-Speichermedien genutzt. Anschließend infizierte Stuxnet existierende Installationen eines Siemens-Prozessvisualisierungssystems und schrieb für bestimmte Steuerungsgeräte Schadroutinen in die entsprechenden Steuerungsbausteine.

3.1.2 Havex/Dragonfly

Die Havex/Dragonfly-Kampagne [Nel16; Hen14] richtete sich zu Beginn gegen Unternehmen des Energiesektors in Europa und den USA, später auch gegen verschiedene andere Industriezweige. Sie begann vermutlich 2010, wurde jedoch erst erstmalig 2013 entdeckt. Für den Zugriff auf Unternehmen kamen sowohl Spearphising via E-Mail, die Nutzung von Malware als auch die Kompromittierung von ICS-Software-Herstellern und das Einbringen von Schadcode in deren Software zum Einsatz. Die Malware enthielt unter anderem eine Funktion zum Scannen des Netzwerks nach ICS-Systemen und das Senden der so erhaltenen Informationen an zentrale Command&Control-Server.

3.1.3 BlackEnergy

Im Dezember 2015 drangen Hacker in die IT- und OT-Systeme des ukrainischen Energieversorgers *Kyivoblenergo* ein und schalteten sieben 110-kV- und 23 35-kV-Umspannwerke ab, wodurch rund 80.000 Kunden drei Stunden lang unversorgt waren. Später wurde klar, dass Angriffe auf insgesamt drei Energieversorger stattgefunden hatten, was die Anzahl der betroffenen Kunden im ganzen Land auf 225.000 erhöhte. Im Rahmen einer Untersuchung [ICS16] wurde ein mehrstufiger Angriff aufgedeckt, bei dem sich Angreifer über einen längeren Zeitraum in den Systemen der Energieversorger bewegt hatten[1]. Von den Angreifern wurden hierbei verschiedene Techniken eingesetzt. Sie erhielten ersten Zugriff auf das IT-Netz mittels Spear-Phishing-Angriffen und mit Malware (BlackEnergy 3) verseuchten Office-Dokumenten. Dieser Zugriff wurde genutzt, um weitere Zugangsdaten zu entwenden und auf das OT-Netz zuzugreifen. Anschließend konnten über Remote-Access-Tools für industrielle Steuersysteme und individuell angepasste Firmware-Images für OT-Komponenten die Ausfälle hervorgerufen werden. Zusätzlich wurde während des finalen Schritts des Angriffs auch Call Center der Energieversorger mit Anrufen überflutet, um das Melden der Ausfälle zu verzögern.

Insgesamt kamen während des Angriffs eine große Bandbreite an Angriffstechniken von Social Engineering bis zu fortgeschrittenen ICS-Firmware-Modifikationen zum Einsatz, die zusammen mit der langen Aufenthaltszeit der Angreifer in den Unternehmensnetzen auf technisch versierte und koordinierte Angreifer vermutlich staatlichem Ursprungs hindeuten.

1. Diese Art von Angriff wird auch als APT bezeichnet

3.1.4 Crash Override

2016 wurde die Malware *Crash Override* (auch bekannt als *Industroyer*) entdeckt, die sich explizit gegen in Stromnetzen verwendete ICSs richtet [Dra17]. Eine Funktion der Malware erlaubte es, Trennschalter in Umspannwerken zu öffnen und ihr erneutes Schließen auf Softwareseite zu verhindern, wodurch die Umspannwerke vom Netz genommen werden konnten. Bei einem Einsatz der Malware führte diese Funktion zu einem etwa einstündigen Stromausfall im einem Bezirk von Kiew. Es wird davon ausgegangen, dass dieser Angriff als Testlauf für zukünftige Angriffe angesehen werden kann, wobei die konkrete Funtionalität der Malware anpassbar und erweiterbar ist.

3.1.5 Triton

Triton ist eine Malware, die sich gegen industrielle Sicherheitssysteme der Firma Triconex richtet und diese außer Kraft setzen kann [Joh+17]. Potentiell könnte die Malware größere Schäden hervorrufen und Menschenleben gefährden, wenn Sicherheitsprozesse ausgesetzt werden.

Triton wurde 2017 in einer saudi-arabischen petrochemischen Anlage entdeckt, weil ein Programmierfehler einen Fehler in einem Sicherheitssystem hervorrief. Die Angreifer verschafften sich zuerst Zugriff das IT-Netz der Anlage und schafften von dort den Übergang in einen geschützten Netzbereich, in dem sie über einen Ingenieursrechner Zugriff auf die Sicherheitssysteme erhielten und dort eine komprommitierte Version der System-Firmware einbringen konnten.

3.1.6 Incontroller/PipeDream

Incontroller [Bru+22] wurde 2022 entdeckt. Die Malware enthält Funktionen, die zum Scannen von Netzen nach ICSs dienen, und Funktionen, die sich gegen ICSs bestimmter Hersteller richten und potentiell auch physikalische Schäden hervorrufen können. Zum jetzigen Zeitpunkt ist allerdings noch kein Einsatz von Incontroller gegen Industrien bekannt geworden.

3.2 Ransomware

Bei Ransomware (im Deutschen auch *Verschlüsselungs-* oder *Erpressungstrojaner*) handelt es sich um Schadsoftware, die zugreifbare Benutzerdateien auf dem kompromittierten System verschlüsselt und eine Entschlüsselung der Dateien erst nach Lösegeldzahlung in Aussicht stellt. Viele Ransomware-Varianten verbreiten sich selbstständig von betroffenen Systemen aus auf weitere Systeme, inklusive Netzwerkspeicher und andere Server. Auf diese Weise kann eine Ransomware auch zum Ausfall ganzer Unternehmensnetze führen. Einige Vertreter gehen auch nach dem *Double-Extortion*-Prinzip vor und senden die Daten vor dem Verschlüsseln an den Angreifer, so dass zusätzlich mit einer Veröffentlichung sensibler extrahierter Daten gedroht werden kann. Dies ist vor allem

im Unternehmensumfeld eine relevante Bedrohung, wenn die Veröffentlichung von Kundendaten oder Unternehmensgeheimnissen droht.

Neben den im Folgenden dargestellten erfolgreichen Angriffen auf Energieinfrastrukturen, gibt es eine Vielzahl weiterer Beispiele für Ransomware-Varianten (z.B. *Locky*, *Hive*, *(Not-)Petya* oder *CryptoLocker*), die insbesondere in den letzten Jahren immer wieder zu großen Schäden für Privatpersonen und Unternehmen jeder Größe führten. Vermehrt stellen Dritte Angreifern auch die mietbare Infrastruktur für die Verbreitung und den Betrieb von Ransomwarekampagnen zur Verfügung (*Ransomware-as-a-service*).

3.2.1 Israels Energieministerium

2016 wurde Israels *Electricity Authority*, eine Abteilung des Energieministeriums, nach Angaben des Energieministers von einem schwerwiegenden Angriff getroffen. Im Nachhinein stellte sich dieser als einfacher Ransomwareangriff heraus, der über eine Phishing-E-Mail durchgeführt worden war [Reg16]. Das Stromnetz war nicht von dem Angriff betroffen.

3.2.2 WannaCry

2017 verbreitete sich die Ransomware *WannaCry* durch Ausnutzung einer *EternalBlue* genannten Sicherheitslücke in Microsoft Windows [Rep17]. Neben der Verschlüsselung zugreifbarer Daten verbreitete sich die Ransomware eigenständig über erreichbare Systeme im betroffenen Netz. Innerhalb weniger Tage waren tausende Organisationen in über 150 Ländern betroffen, darunter diverse Energieversorger und weitere kritische Infrastrukturen. Dies ist insbesondere vor dem Hintergrund kritisch zu betrachten, als dass bereits im Vorfeld ein Sicherheitsupdate existierte, das die ausgenutzte Lücke behob, jedoch in den betroffenen Systemen noch nicht installiert worden war. Es wird geschätzt, dass Wannacry weltweit Verluste in Höhe von 4 Milliarden US-Dollar verursacht haben könnte [Kas].

3.2.3 Elexon

2020 wurde *Elexon* Opfer eines Angriffs [Amb20], wobei auf interne IT-Systeme zugegriffen wurde. Das Unternehmen ist für die Verwaltung des englischen Strommarkts verantwortlich. Obwohl enge Verbindungen mit Übertragungsnetzbetreibern bestehen, wurden weitere Zugriffe und damit potentielle Auswirkungen auf die Netzstabilität verhindert. Unter Zuhilfenahme einer Malware wurden jedoch verschiedene sensible Daten extrahiert und später im Darknet zum Kauf angeboten [Mon20].

3.2.4 EDP (Ragnar Locker)

Angreifer nutzten 2020 die *Ragnar-Locker-Ransomware* für einen Angriff auf das portugiesische Energieunternehmen *EDP* [Gat20]. Nähere Details zum Ablauf des Angriffs

wurden nicht veröffentlicht, häufig wurde die Ransomware jedoch über einen initialen RDP-Zugriff, der mittels gestohlener Zugangsdaten oder per Brute-Force-Angriff erreicht wurde, und die anschließende Ausnutzung einer weiteren Sicherheitslücke in Unternehmen verbreitet [Acr21]. Während des Angriffs wurden große Mengen von nichtöffentlichen Unternehmensdaten extrahiert und verschlüsselt. Die Angreifer drohten mit einer Veröffentlichung der Daten, falls ein gefordertes Lösegeld nicht gezahlt werde. Auswirkungen auf die Stromversorgung hatte der Angriff laut Unternehmensangaben jedoch keine.

3.2.5 Colonial Pipeline (DarkSide)

2021 war die Betreibergesellschaft der *Colonial Pipeline* von der Ransomware *DarkSide* betroffen [Osb21]. Dies führte zu einer temporären Abschaltung des Pipelinebetriebes, wobei die eigentliche Pipelineinfrastruktur nicht von dem Angriff betroffen war. Grund war die Unfähigkeit, an Kunden geliefertes Gas abzurechnen, da das Rechnungswesen betroffen war. In der weiteren Folge kam es in einigen US-Staaten zu Benzinknappheit und Panikkäufen.

3.2.6 Nordex (Conti)

2022 wurde der deutsche Windradhersteller Nordex mit der Ransomware *Conti* angegriffen [Abr22]. In Folge des Angriffs wurden auch Fernwartungzugänge für Windräder des Betreibers abgeschaltet. Vermutet wird ein Eindringen der Angreifer mittels eines Phishingangriffs.

3.3 Supply-Chain-Angriffe

Bei *Supply-Chain-Angriffen* (Angriffe auf Lieferketten) wird das Zielunternehmen nicht direkt angegriffen. Stattdessen werden Unternehmen in der Lieferkette des Zielunternehmens angegriffen, um Zugriff auf das Netzwerk des Zielunternehmens zu erhalten. Hierbei können sowohl Dienstleister mit Zugriffsrechten auf das Zielunternehmen, als auch Zulieferer für Hardware oder Software als Ziel in Frage kommen, insbesondere wenn sie geringere Sicherheitsstandards erfüllen als das Zielunternehmen selbst. Insoweit fallen Supply-Chain-Angriffe in die Kategorie der Angriffe mittels transitiver trojanischer Pferde. Potentiell können durch jene Angriffe auch viele Ziele gleichzeitig angegriffen werden, wenn ein Dienstleister mehrere Zielunternehmen beliefert, wie auch das folgende Beispiel zeigt.

SolarWind

Als Zulieferer von Netzwerkmonitoring- und Netzwerkmanagementsoftware war die Firma *SolarWind* im Jahre 2020 im Fokus eines großen Supply-Chain-Angriffs [Man20]. Hierzu wurde durch die Angreifer in einem Softwareupdate während des Kompilierungsvorgangs und vor der Signatur des Updates eine Hintertür (in Form einer *Sunburst*

genannten Malware) eingebracht, so dass die Veränderungen von vorgeschalteten Audits des Codes nicht entdeckt werden konnten [Tem21]. In den folgenden Monaten wurde das Update von etwa 18.000 SolarWind-Kunden in den USA, Europa und Asien installiert, darunter verschiedene Behörden, große Technologiefirmen wie Microsoft und auch kritische Infrastrukturen. Sunburst ermöglichte den Angreifern eine Ausbreitung in den Netzen der Kunden mittels weiterer Malware und in Erfahrung gebrachter Zugangsdaten. So konnten beispielsweise mehrere E-Mail-Konten von hochrangigen Mitarbeitern des amerikanischen *Department for Homeland Security* kompromittiert werden [Phi21]. Insgesamt handelt es sich um einen der weitreichendsten bekannt geworden Supply-Chain-Angriffe.

3.4 Insiderangriffe

Diese Angriffskategorie beschreibt die Gefahr, die von Personen innerhalb eines Unternehmen, also von *Insidern* bzw. Innentätern, ausgehen kann. Innentäter können dabei verschiedenen Personenkreisen zugehören [Ver19]:

- Angestellte, die dem eigenen Unternehmen aus Verärgerung, Nachlässigkeit oder Boshaftigkeit Schaden zufügen,
- Außenstehende, die – etwa zum Zwecke der Industriespionage – gezielt von Dritten in das Unternehmen geschleust werden oder
- dritte Parteien (Dienstleister, ...), deren Zugriff auf das Unternehmen zu (gewollten oder ungewollten) Fehlhandlungen führt.

Da in allen drei Fällen Vertrauensbeziehungen innerhalb des Unternehmens bestehen, fällt die Missachtung von Sicherheitskonzepten oft nicht unmittelbar auf.

Weitere Angriffe durch Innentäter im Energiesektor sind in [Kab10] dargestellt.

3.4.1 Texanisches Energieunternehmen

2009 nutzte ein entlassener Angestellter eines texanischen Energieunternehmens nicht entzogene Zugriffsrechte dazu, sensible Unternehmensdaten zu extrahieren und andere Daten zu verändern oder zu löschen [Pou09]. Einige der gelöschten Dateien waren für Betriebsabläufe in der Verwaltung zentral, sodass deren Fehlen dem Unternehmen auf dem Strommarkt Verluste einbrachte. Der Betrieb der Energieanlagen war von dem Innentäter-Angriff nicht betroffen.

3.4.2 Kalifornische Öl- und Gasunternehmen

Ein ehemaliger IT-Berater eines kalifornischen Öl- und Gasunternehmens manipulierte 2008 aus Frust über eine verwehrte Festanstellung die SCADA-Systeme des Unternehmens, die unter anderem für die Fernsteuerung von Ölplattformen und zur Erkennung von Gaslecks eingesetzt wurden [Boo09].

3.5 Angriffe auf Kommunikationsstrecken

Anstatt Systeme direkt anzugreifen, können ebenso Angriffe auf die Kommunikation zwischen Systemen zu Ausfällen des Gesamtsystems führen. Beispiele sind die Störung drahtloser Kommunikation durch Störsender oder die Störung kabelgebundener Kommunikation durch physische Zerstörung der Kommunikationsleitungen.

Viasat/ENERCON (AcidRain)

2022 wurde das Satellitennetz *KA-SAT* des Kommunikationsanbieters Viasat angegriffen, indem Modems des Satellitennetzes mit einer *AcidRain* getauften Wiper-Malware unbrauchbar gemacht worden waren [GA22]. Angenommen wird eine Verbreitung der Malware in Form eines Supply-Chain-Angriffs und unter Ausnutzung von existierenden KA-SAT-Management-Funktionen. AcidRain ist hier nur ein Beispiel für den Einsatz von Wiper-Malware im (zumindest) zeitlichen Zusammenhang mit dem Ukraine-Krieg, andere Beispiele stellen etwa die Malwares *DoubleZero*, *HermeticWiper* und *WhisperGate* dar [Gat22]. Durch den Ausfall des Kommunikationsnetzes verlor das deutsche Energieunternehmen ENERCON für mehrere Tage die Verbindung zu 5800 Windrädern, sodass ihr Monitoring und ihre Fernwartung nicht mehr möglich waren. ENERCON empfiehlt, in Folge des Angriffs bei zukünftigen Anlagen redundante Kommunikationsstrecken direkt bei der Planung zu beachten [ENE22].

3.6 DDoS

Ein Denial-of-Service-Angriff zielt darauf ab, die Funktionsfähigkeit eines Zielsystems zu stören, indem das System oder die Kommunikationswege mit Anfragen überlastet werden. Wird ein derartiger Angriff von mehreren Quellsystemen aus durchgeführt, etwa um die Effektivität zu steigern oder die Abwehr zu erschweren, so spricht man von einem DDoS-Angriff (Distributed Denial of Service). Bei den Quellsystemen kann es sich um kompromittierte IoT-Systeme handeln, die ein Botnetz bilden und von einem sogenannten *Command&Control*-Server ferngesteuert werden. DDoS-Angriffe, die nicht mit weiteren Angriffsarten kombininert werden, ermöglichen Angreifern zunächst keinen Zugang zu sensiblen (Anlagen-)Systemen. Dennoch können sie zu hohen Kosten führen können, etwa wenn Dienstleistungen nicht erbracht werden können. Außerdem können DDoS-Angriffe als Vorbereitung für weitere Angriffswellen genutzt werden, bspw. um Verteidigungsmechanismen im Zielunternehmen abzuschalten.

50Hertz

Der deutsche Übertragungsnetzbetreiber *50Hertz* wurde 2012 Opfer eines DDoS-Angriffs, in dessen Folge extern angebotene Dienste wie die Internetseite, E-Mail-Server und Serviceportale nicht erreichbar waren [50H12]. Jedoch waren weder der Anlagenbetrieb, noch das operative Geschäft von dem Angriff betroffen.

3.7 Nicht ausreichend authentifizierter Zugriff auf Steuersysteme aus dem Internet

Industrielle Kontrollsysteme, die direkt oder nur durch schwache Authentifizierungsmaßnahmen (etwa der Nutzung von Standardpasswörtern) geschützt über das Internet erreichbar sind, können Angreifern die direkte Steuerung von Anlagen erlauben. Spezielle Suchmaschinen wie Shodan[2] erlauben die einfache und schnelle Suche nach ungeschützten Steuersystemen. Dieser Bedrohung kann oftmals durch einfache Gegenmaßnahmen (z.B. Nutzung von Virtual Private Network (VPN)-Lösungen) begegnet werden, dennoch ist sie auch heute noch in vielen Unternehmen anzutreffen [Sch16; Sch22].

Bowman Dam

Iranische Angreifer verschafften sich 2013 Zugriff auf die Steuerungssysteme des *Bowman Dam* in den USA [Kov16]. Als Einfallstor wurde dabei ein aus dem Internet zugreifbarer Windows XP-Rechner genutzt, der lediglich mit einem schwachen Zugangspasswort geschützt war. Die Angreifer konnten keinen Schaden verursachen, da die physikalischen Steuerungskomponenten des Damms gerade gewartet wurden und von dem System getrennt waren.

2. https://www.shodan.io/, zugegriffen am 11.04.2021.

4 Interviews

Um einen Überblick über die IT- und OT-Infrastruktur von Energieunternehmen im NRL-Konsortium zu erlangen und relevante Informations- und Kommunikationstechnik (IKT)-Sicherheitsherausforderungen aufgreifen zu können, wurden im Herbst 2022 Interviews mit Vertreterinnen und Vertretern von fünf Unternehmen aus dem NRL-Konsortium geführt. Die Unternehmen stammten aus den Bereichen Netzbetrieb und Kraftwerksbetrieb und unterschieden sich stark in Unternehmensgröße, eingesetzten Anlagen und dem Umgang mit Themen der IKT-Sicherheit. Gesprächspartner und -partnerinnen waren zumeist die Informationssicherheitsbeauftragten des Unternehmen. In einem weiteren Fall wurden mehrere Mitarbeiter der IT-Abteilung interviewt. Aufgrund der geringen Anzahl an Gesprächen wurde ein qualitativer Ansatz für die Interviews gewählt. Nachfolgend werden der Aufbau der Interviews und die wichtigsten gewonnenen Erkenntnisse vorgestellt.

4.1 Aufbau des Interviews

Inhaltlich standen in den Interviews die drei Themen *Infrastruktur*, *Bedrohungen* und *Sektorenkopplung* im Fokus. Der vollständige Interviewfragebogen befindet sich in Anhang A.

Im Themenfeld *Infrastruktur* wurden einerseits die im jeweiligen Unternehmen eingesetzten OT-Hardwarekomponenten thematisiert. Der Fokus lag hierbei auf Praktiken des Patchmanagements, der Fernsteuerbarkeit und physischen Zutrittsbeschränkungen zu den entsprechenden unternehmenseigenen Anlagen. Andererseits wurde auf Kommunikationspraktiken im Unternehmen eingegangen, mit Fragen zur Netztrennung, Schnittstellenabsicherung und organisationsübergreifenden Authentifizierung.

Im *Bedrohungen*-Teil des Interviews wurde über mögliche Auswirkungen gesprochen, die gezielte Angriffe auf die unternehmenseigene Infrastruktur haben könnten. Zudem wurde nach möglicherweise bereits erfolgten Angriffen im Kontext des eigenen Unternehmens gefragt.

Um auch zukünftige IKT-Sicherheitsthemen im Energiesektor antizipieren zu können, war der letzte Teil des Interviews der *Sektorenkopplung* und eventuellen zukünftigen Digitalisierungsprojekten gewidmet.

4.2 Wichtigste Erkenntnisse

In den Gesprächen mit den Unternehmensvertreterinnen und -vertretern wurden zahlreiche Erkenntnisse gesammelt, die in den folgenden Abschnitten kurz zusammengefasst werden.

4.2.1 Trennung von Netzen

Die konsequente Trennung von verschiedenen Netzbereichen trägt maßgeblich zum Schutz von IT- und OT-Infrastruktur bei. Sind beispielsweise Anlagenbereiche mit OT-Infrastruktur mit dem IT-Netzbereich und dem Internet verbunden, fällt es Angreifern deutlich leichter, unbefugte Kontrolle über Anlagen zu gewinnen. Da Angriffe grundsätzlich nicht ausgeschlossen werden können, können sie durch Netztrennung zumindest lokal beschränkt werden. Darüber hinaus sollten so wenige Geräte wie möglich mit dem Internet verbunden sein: Da jede Schnittstelle aus dem unternehmenseigene Netz ins Internet ein potenzielles Einfallstor für Angriffe jeglicher Art darstellt, sind insbesondere mit dem Internet verbundene sicherheitskritische Anlagen und Leitstellen als (vermeidbares) Sicherheitsrisiko anzusehen.

Im Rahmen der Interviews konnte festgestellt werden, dass insbesondere große Partnerunternehmen eine entsprechende Netztrennung weitestgehend umgesetzt haben. Vertreter von kleineren Unternehmen haben hier jedoch zum Teil Nachbesserungsbedarf angegeben.

4.2.2 Fernsteuerungsmöglichkeiten

Die Möglichkeit, eine Anlage aus der Ferne zu steuern, geht oft mit einer Anbindung an das Internet einher. Es ist deshalb individuell zu prüfen, ob der Nutzen dieser Funktion das Inkaufnehmen von Sicherheitsrisiken rechtfertigt. In jedem Fall sind Schutzmaßnahmen des aktuellen Stands der Technik zu ergreifen (beispielsweise VPN, 2-Faktor-Authentifizierung, sichere Passwörter, 4-Augen-Prinzip, ...).

Auch hierzu wurden in den Interviews verschiedene Angaben gemacht: Während einige Unternehmen Fernsteuerungsmöglichkeiten aus Sicherheitsgründen prinzipiell ablehnen, werden sie von anderen Unternehmen (in Verbindung mit entsprechenden Schutzmaßnahmen) regelmäßig genutzt.

4.2.3 Physische Sicherheit

Für einige Arten von Angriffen ist es für Angreifer zudem unerlässlich, physischen Zugriff zu den Anlagen zu erlangen. Das Erarbeiten und die konsequente Umsetzung von Sicherheitsrichtlinien können diesbezügliche Risiken minimieren. Dies kann das Einsetzen von Zugangskontrollen mit elektronischen Schlüsselkarten, aber auch nicht-elektronische Schließsysteme, gut gesicherte Zäune und viele weitere Maßnahmen einschließen. Die Maßnahmen sind allerdings erst dann wirksam, wenn allen Mitarbeitenden die Tragweite möglichen Fehlverhaltens bewusst sind: Wenn Fremden, die sich in blauer Kleidung als Wartungsarbeiter tarnen, aus Höflichkeit die Türen offen gehalten werden, gibt es Nachbesserungsbedarf in der Umsetzung von Sicherheitskonzepten. Stattdessen sollte es auch für Fremdfirmen Protokolle geben, etwa das Aushändigen von Besucherausweisen nach vorheriger Anmeldung bei Pförtnern.

4.2.4 Awareness-Schulungen

In den Interviews waren einige Gesprächspartner der Ansicht, dass ihr Unternehmen nicht besonders schützenswert sei. Wie in Kapitel 3 dargestellt, können potenziell alle Unternehmen mit größeren Anlagen Ziel eines Angriffs werden – und sei es nur, um die öffentlichen Ordnung zu stören (bspw. durch in Brand geratene Anlagen). Mitarbeitende dafür zu sensibilisieren, ist der erste wichtige Aspekt von Schulungen. Denn ein Bewusstsein für das Schützbedürfnis des eigenen Unternehmens motiviert einen sorgfältigen Umgang mit getroffenen Maßnahmen.

Die unternehmenseigenen Sicherheitsrichtlinien selbst sind der zweite Aspekt von Schulungen: Die verschiedenen Möglichkeiten, wie Angreifer Zugang zum Unternehmen erlangen können (USB-Sticks, Phishing-Mails, Social Engineering über Anrufe, Verkleidungen, etc.) sollten dabei ebenso thematisiert werden, wie Regeln, die zur Risikominimierung befolgt werden müssen.

4.2.5 Aktuelle Softwareversionen

Bei vielen der interviewten Partner kommen Hardwarekomponenten mit Software zum Einsatz, für die keine Updates mehr vom Hersteller bereitgestellt werden. Die Gefahr beim Einsatz derartiger Komponenten besteht darin, dass ggf. bekannt gewordene Sicherheitslücken nicht mehr geschlossen werden können. Können Angreifer ermitteln, dass Hardware mit Sicherheitslücken eingesetzt wird, kann sie als Einfallstor für Angriffe genutzt werden. Deshalb sollten OT-Komponenten, deren Software nicht mehr aktualisiert wird, möglichst durch neuere ausgetauscht werden. Für alle anderen Komponenten sollte das Patchmanagement (also das zeitnahe Einspielen neuer Updates) konsequent umgesetzt werden.

4.2.6 Authentifizierung anderer Organisationen

Die Kommunikation mit anderen Organisationen sollte umfassend geschützt werden, insbesondere wenn sicherheitskritische Informationen übertragen werden. In den Interviews wurde unter anderem angegeben, dass Personen authentifiziert werden, indem ihre Stimme in Telefonanrufen erkannt wird. Spätestens durch neuartige Stimmverzerrer ist dies nicht ausreichend. Idealerweise ist jegliche Kommunikation inner- und außerhalb des eigenen Unternehmens mit geeigneten Public-Key-Verschlüsselungssystemen geschützt, sodass nur dedizierte Empfänger die Inhalte entschlüsseln können. Die Authentifizierung sollte über geeignete Maßnahmen (2-Faktor-Authentifizierung, sichere Passwörter, etc.) stattfinden.

4.2.7 Redundante Kommunikationswege

In vielen Angriffsszenarien kann die primäre Kommunikationsinfrastruktur wie Voice over IP (VoIP), Telefon oder E-Mail ausfallen, siehe Abschnitt 3.5. Daher sollte sichergestellt werden, dass redundante Kommunikationsstrecken existieren – sowohl zu den Anlagen selbst als auch zu anderen relevanten Akteuren, innerhalb und außerhalb des

Unternehmens. Die Kommunikation selbst sollte bei Ausfall der primären Infrastruktur über dedizierte Wege und über vorher festgelegte Protokolle stattfinden. Die Annahme, dass Mitarbeitende sich im Störfall gegenseitig über ihre privaten Telefone erreichen können, reicht somit nicht aus – zumal auch Szenarien auftreten können, in denen der Mobilfunk nur eingeschränkt zur Verfügung steht. Zum Zeitpunkt der Interviews konnten uns die wenigsten Interviewpartnern von entsprechenden Plänen und Notfallprotokollen berichten.

4.2.8 Vorsicht bei Lieferketten

Wenn Aufträge an Dritte vergeben werden und diese Zugriff auf IT-/OT-Netze erhalten, kann dies die Übersicht über Bedrohungsszenarien und IKT-Sicherheitsmaßnahmen erheblich erschweren. Sämtliche Interviewpartner haben angegeben, Fremdkomponenten in Hard- oder Software einzusetzen. Darüber hinaus wurden bei einigen der Interviewpartner ganze IT-Abteilungen aus dem Unternehmen ausgegliedert. Außerdem wurde das Patchmanagement von einigen Hardwarekomponenten im Rahmen von Wartungsverträgen komplett von den Herstellern übernommen.

Wenngleich diese Maßnahmen wirtschaftlich sinnvoll und notwendig sein können, werden dadurch Schnittstellen aus dem Unternehmenskontext nach außen geschaffen. Da jede dieser Schnittstellen ein potenzielles Einfallstor für Angreifer ist (siehe Abschnitt 3.3), sollten beim Auslagern von Aufgaben und Infrastruktur Sicherheitsaspekte immer mitgedacht werden.

4.2.9 Informationen über Schwachstellen

Der Austausch über aktuelle Entwicklungen und neu gefundene Schwachstellen ist im sicherheitskritischen Bereich essenziell. Eine Möglichkeit hierzu ist die Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland (UP-KRITIS) vom BSI. Es wurde in den Interviews allerdings auch von kleineren Kreisen berichtet, in denen sich mit vergleichbaren Unternehmen ausgetauscht wird.

5 Fazit

In diesem Arbeitspapier wurden die aus IT-/OT-Sicherheitsperspektive aktuell relevantesten Bedrohungen für den Energiesektor zusammengefasst. Neben einer Übersicht der wichtigsten Angriffsarten inklusive Beispielen in Kapitel 3 und weiterführender Literatur in Kapitel 2 wurden die Ergebnisse einer Interviewreihe innerhalb des NRL-Konsortiums in Kapitel 4 präsentiert.

Obwohl die Angriffsmöglichkeiten in der heutigen stark vernetzten Welt vielfältig sind, kann durch die folgenden Ansätze bereits einigen große Bedrohungen vorgebeugt werden: Die **Trennung von Netzen**, insbesondere in einen gesonderten IT-Bereich (mit Internetzugang) und einen OT-Bereich (bestehend aus Anlagen ohne Internetzugriff), sowie ein **konsequentes Patchmanagement** inklusive des Austauschs veralteter Komponenten sind wichtige technische Maßnahmen, um die Angriffsfläche des eigenen Unternehmens klein zu halten. Weiterhin sollten **Lieferketten** von Hard- und Software genau überwacht werden, um auch die Angreifbarkeit von Schnittstellen aus dem Unternehmen heraus zu minimieren. Unternehmen sollten ihre Infrastruktur gegen relativ leicht zu verhindernde Angriffe wie (ungezielte) **Ransomwarekampagnen** oder **DDoS-Angriffe** selbstverständlich schützen – die Praxis zeigt jedoch auch, dass dies bei weitem noch nicht in allen Unternehmen geschieht. Ein oft unterschätzter Aspekt sind die eigenen **Mitarbeitenden**, die durch Schulungen für Sicherheitsthemen sensibilisiert und ausgebildet werden müssen, da ansonsten die Wirksamkeit von technischen und organisatorischen Maßnahmen schnell ausgehebelt werden kann.

Angesichts der Bedrohungslage werden Angriffe auf die Energieinfrastruktur in den nächsten Jahren eher noch zunehmen. Umso wichtiger ist es, allen Beteiligten in Unternehmen die Relevanz von die IT/OT-Sicherheit betreffenden Themen zu kommunizieren und Maßnahmen konsequent umzusetzen. Wir hoffen, mit diesem Arbeitspapier einen Beitrag dazu leisten zu können.

Danksagung

Die Autoren danken allen Projektpartnern, die sich für die Teilnahme an den Interviews bereit erklärt haben und uns mit ihrer Expertise zur Verfügung standen. Weiterhin möchten wir uns bei Christian Wolff bedanken, der die Interviews im Rahmen seiner Abschlussarbeit durchführte und eine erste Auswertung vornahm.

Literatur

[50H12] 50Hertz. *Geschäftsbericht 2012*. 2012. URL: https://docplayer.org/8440745-50hertz-geschaeftsbericht-2012.html (besucht am 29. 03. 2023).

[Abr22] Lawrence Abrams. *Wind turbine firm Nordex hit by Conti ransomware attack*. BleepingComputer. 2022. URL: https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/ (besucht am 28. 03. 2023).

[Acr21] Acronis. *Analysis of Ragnar Locker Ransomware*. 2021. URL: https://www.acronis.com/en-us/blog/posts/ragnar-locker/ (besucht am 21. 03. 2023).

[Age21] International Energy Agency. *Enhancing Cyber Resilience in Electricity Systems*. 2021. URL: https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (besucht am 13. 03. 2023).

[AHT17] Uchenna P. Daniel Ani, Hongmei (Mary) He und Ashutosh Tiwari. *Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective*. In: *Journal of Cyber Security Technology* 1.1 (2017), S. 32–74. DOI: 10.1080/23742917.2016.1252211. eprint: https://doi.org/10.1080/23742917.2016.1252211. URL: https://doi.org/10.1080/23742917.2016.1252211.

[Amb20] Jillian Ambrose. *Lights stay on despite cyber-attack on UK's electricity system*. The Guardian. 2020. URL: https://www.theguardian.com/business/2020/may/14/lights-stay-on-despite-cyber-attack-on-uks-electricity-system (besucht am 21. 03. 2023).

[Boo09] Dan Boodin. *(Former) IT consultant confesses to SCADA tampering*. The Register. 2009. URL: https://www.theregister.com/2009/09/24/scada_tampering_guilty_plea/ (besucht am 03. 02. 2023).

[Bru+22] Nathan Brubaker u. a. *INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems*. Mandiant. 2022. URL: https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (besucht am 03. 04. 2023).

[BSI13] BSI. *ICS-Security-Kompendium*. 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=3 (besucht am 18. 03. 2023).

[BSI18] BSI. *Industrial Control System Security: Innentäter*. 2018. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_061.html?nn=128768 (besucht am 18. 03. 2023).

[BSI22] BSI. *Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen 2022*. 2022. URL: https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html (besucht am 18. 03. 2023).

[Cou16] World Energy Council. *The road to resilience: Managing cyber risks*. 2016. URL: https://www.worldenergy.org/publications/entry/the-road-to-resilience-managing-cyber-risks (besucht am 18. 03. 2023).

[Cyb20] Canadian Centre for Cyber Security. *Cyber threat bulletin: The cyber threat to Canada's electricity sector*. 2020. URL: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector (besucht am 13. 03. 2023).

[Dax+17] Julian Dax u. a. *Stand zur IT-Sicherheit deutscher Stromnetzbetreiber : technischer Bericht*. 2017. URL: https://dspace.ub.uni-siegen.de/handle/ubsi/1185 (besucht am 13. 03. 2023).

[Dra17] Dragos. *CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids*. 2017. URL: https://www.dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/ (besucht am 27. 03. 2023).

[ENE22] ENERCON. *Over 95 per cent of WECs back online following disruption to satellite communication*. 2022. URL: https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/ (besucht am 29. 03. 2023).

[Eur17] Energy Expert Cyber Security Platform of the European Commission. *Cyber Security in the Energy Sector*. 2017. URL: https://energy.ec.europa.eu/system/files/2017-03/eecsp_report_final_0.pdf (besucht am 18. 03. 2023).

[Fis+18] Lars Fischer u. a. *Study on the Evaluation of Risks of Cyber-Incidents and on Costs of preventing Cyber-Incidents in the Energy Sector*. Okt. 2018. URL: https://energy.ec.europa.eu/study-evaluation-risks-cyber-incidents-and-costs-preventing-cyber-incidents-energy-sector_en (besucht am 13. 03. 2023).

[FMC10] Nicolas Falliere, Liam O Murchu und Eric Chien. *W32.Stuxnet Dossier*. Symantec. 2010. URL: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf (besucht am 21. 03. 2023).

[GA22] Juan Andres Guerrero-Saade und Max van Amerongen. *AcidRain | A Modem Wiper Rains Down on Europe*. SentinelLabs. 2022. URL: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (besucht am 29. 03. 2023).

[Gat20] Sergiu Gatlan. *RagnarLocker ransomware hits EDP energy giant, asks for €10M*. BleepingComputer. 2020. URL: https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/ (besucht am 21. 03. 2023).

[Gat22] Sergiu Gatlan. *Viasat confirms satellite modems were wiped with AcidRain malware*. BleepingComputer. 2022. URL: https://www.bleepingcomputer.com/news/security/viasat-confirms-satellite-modems-were-wiped-with-acidrain-malware/ (besucht am 21. 03. 2023).

[Hen14] Daavid Hentunen. *Havex Hunts For ICS/SCADA Systems*. F-Secure. 2014. URL: https://archive.f-secure.com/weblog/archives/00002718.html (besucht am 03. 04. 2023).

[ICS16] E-ISAC & SANS ICS. *Analysis of the cyber attack on the Ukrainian power grid*. 2016. URL: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (besucht am 20. 03. 2023).

[Ins15a] Electric Power Research Institute. *Analysis of Selected Electric Sector High Risk Failure Scenarios*. 2015. URL: https://smartgrid.epri.com/doc/NESCOR%20Detailed%20Failure%20Scenarios%20v2.pdf (besucht am 16. 03. 2023).

[Ins15b] Electric Power Research Institute. *Electric Sector Failure Scenarios and Impact Analyses*. 2015. URL: https://smartgrid.epri.com/doc/NESCOR%20Failure%20Scenarios%20v3%2012-11-15.pdf (besucht am 16. 03. 2023).

[Joh+17] Blake Johnson u. a. *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*. Mandiant. 2017. URL: https://www.mandiant.com/resources/blog/attackers-deploy-new-ics-attack-framework-triton (besucht am 21. 03. 2023).

[Kab10] M.E. Kabay. *Attacks on power systems: Data leakage, espionage, insider threats, sabotage*. Network World. 2010. URL: https://www.networkworld.com/article/2217680/attacks-on-power-systems--data-leakage--espionage--insider-threats--sabotage.html (besucht am 29. 03. 2023).

[Kas] Kaspersky. *What is WannaCry ransomware?* URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (besucht am 21. 03. 2023).

[Kas19] Kaspersky. *Quiet please: two-thirds of industrial organizations don't report cybersecurity incidents to regulators*. 2019. URL: https://www.kaspersky.com/about/press-releases/2019_two-thirds-of-industrial-organizations-dont-report-cybersecurity-incidents-to-regulators (besucht am 28. 03. 2023).

[Kov16] Eduard Kovacs. *Iranian Hacked Computer Controlling US Dam: Prosecutors*. SecurityWeek. 2016. URL: https://www.securityweek.com/iranian-hacked-computer-controlling-us-dam-prosecutors/ (besucht am 21. 03. 2023).

[Man20] Mandiant. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*. 2020. URL: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor (besucht am 27. 03. 2023).

[Mon20] Tech Monitor. *Internal Data Stolen, Leaked, in REvil Attack on Electricity Market's Elexon*. 2020. URL: https://techmonitor.ai/technology/cybersecurity/elexon-hack-ransomware-revil (besucht am 21. 03. 2023).

[MRS22] B. Munzel, M. Reiser und K. Steinbacher. *Flexibilitätspotenziale und Sektorkopplung. Synthesebericht 1 des SINTEG-Förderprogramms. Studie im Auftrag des Bundesministerium für Wirtschaft und Klimaschutz (BMWK)*. 2022. URL: https://www.bmwk.de/Redaktion/DE/Publikationen/Sinteg/synthesebericht-1-flexibilitatspotenziale-und-sektorkopplung.pdf?__blob=publicationFile&v=6 (besucht am 19. 03. 2023).

[Nel16] Nell Nelson. *The Impact of Dragonfly Malware on Industrial Control Systems*. SANS. 2016. URL: https://www.sans.org/white-papers/36672/ (besucht am 03. 04. 2023).

[Osb21] Charlie Osborne. *Colonial Pipeline ransomware attack: Everything you need to know*. ZDNET. 2021. URL: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/ (besucht am 21. 03. 2023).

[Phi21] Gavin Phillips. *SolarWinds Hackers Breached the Email Accounts of Top DHS Officials*. 2021. URL: https://www.makeuseof.com/solarwinds-hackers-breached-emails-top-dhs-officials/ (besucht am 25. 07. 2023).

[Pou09] Kevin Poulsen. *Ex-Employee Fingered in Texas Power Company Hack*. Wired. 2009. URL: https://www.wired.com/2009/05/efh/ (besucht am 03. 02. 2023).

[Reg16] The Register. *'Critical' Israel power grid attack was just boring ransomware*. 2016. URL: https://www.theregister.com/2016/01/28/israel_power_grid_attack_boring_ransomware/ (besucht am 27. 03. 2023).

[Rep17] Norton Rose Fulbright Data Protection Report. *WannaCry Ransomware Attack Summary*. 2017. URL: https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/ (besucht am 27. 03. 2023).

[Sch16] Jürgen Schmidt. *VNC-Roulette – was wollen Sie fernsteuern?* Heise. 2016. URL: https://www.heise.de/news/VNC-Roulette-was-wollen-Sie-fernsteuern-3159811.html (besucht am 03. 04. 2023).

[Sch22] Dennis Schirrmacher. *IT-Security-Anfängerfehler gefährden Stromver- und Abwasserentsorgung*. Heise. 2022. URL: https://www.heise.de/news/Bericht-IT-Security-Anfaengerfehler-gefaehrden-Strom-und-Abwasserversorgung-7146566.html (besucht am 03. 04. 2023).

[Sto+15] Keith Stouffer u. a. *NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security*. 2015. URL: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final (besucht am 18. 03. 2023).

[Tem21] Dina Temple-Raston. *A 'Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack*. NPR. 2021. URL: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (besucht am 27. 03. 2023).

[Ver19] Verizon. *Insider Threat Report*. 2019. URL: https://www.verizon.com/business/resources/Tea8/reports/insider-threat-report.pdf (besucht am 03. 04. 2023).

A Interviewfragebogen

Der verwendete Fragebogen ist in sechs Themenfelder untergliedert.

A.1 Einstieg

- In welchem Geschäftsfeld ist Ihr Unternehmen tätig?
- Welche Art von Anlagen/Infrastruktur betreut ihr Unternehmen?
- Unterliegen die Anlagen/unterliegt die Infrastruktur der KRITIS-Verordnung?
- Sind Ihre Anlagen oder Ihr Unternehmen als Betreiber gemäß ISO27001 oder BSI zertifiziert?
- Wie sieht Ihr persönliches Aufgabengebiet aus?
  - Auf welche Weise haben Sie Ihre Qualifikation/Kompetenz im Sicherheitsbereich erworben? (Studium, Weiterbildung, Selbststudium, ...)
- Gibt es innerhalb Ihrer Organisation bzw. Branche einen Informationsaustausch über Sicherheitsfragen? Wenn ja, welche?

A.2 IT/OT-Infrastruktur

OT-Komponenten

- Welche Arten von vernetzter Regelungstechnik und Sensorik (OT-Komponenten) kommen bei Ihnen zum Einsatz? Welchen Zweck erfüllen sie?
  - Welche Komponenten sind zu welchem Zweck fernsteuerbar?
  - Werden Standardkomponenten oder Eigenentwicklungen eingesetzt?
- Müssen die Komponenten regelmäßig geupdatet werden? Wenn ja, wie wird das Patchma- nagement umgesetzt?
  - Gibt es von Herstellerseite Informationen zu bekannten Verwundbarkeiten der Kom- ponenten?
- Sind die Komponenten redundant ausgelegt?
- Wie wird die physische Sicherheit der Anlagen gewährleistet? (Zugangskontrollen, Zäune, ...)?
- Wie und wo werden Warnungen zu fehlerhaften Komponenten in Anlagen/Steuergeräten/-Netzen erkannt und übermittelt?

  - Darstellungsformen in Leitstellen/Übertragungsnetzen -> „Rote Lampe“)

Kommunikation

- Welche Netzbereiche (z. B. OT-Netz(e), Büro-Netz, ...) gibt es im Unternehmen?
  - Wie werden die Netzbereiche separiert (physisch, DMZ, VLAN, ...)?
  - Gibt es jeweils Systeme, die gezielt zur Angriffserkennung genutzt werden (Host-basierte Sensoren z.B. Antivirus-SW, Applikations-spezifische Logging-Mechanismen oder Netz-basierte Sensoren, z.B. Bro/Zeek, oder Honeypots)?
- Welche Schnittstellen gibt es zwischen den Bereichen (Leitstellenzugriff, Fernwartung, Datenbanken, Messwerte, ...)?
  - Welche Protokolle/Standards kommen in den verschiedenen Bereichen zum Einsatz (IP, IEC 61850, ...)?
  - Wie sind die Schnittstellen und die Kommunikation abgesichert (Authentifizierung, Verschlüsselung, ...)?
  - Welche Benutzergruppen können auf diese Schnittstellen zugreifen (z. B. Leitstel- lenmitarbeiter kann Komponente X fernsteuern)?
- Welche Kommunikation erfolgt mit anderen Standorten/Organisationen und zu welchem Zweck (z. B. Kommunikation mit Übertragungsnetzbetreiber für Regelenergiezwecke)?
  - Welche Protokolle/Standards kommen zum Einsatz?
  - Wie wird die organisationsübergreifende Authentifizierung sichergestellt?
- Welche Kommunikationsstrecken sind redundant ausgelegt?

A.3 Bedrohungen und Vorfälle

- Welche Auswirkungen könnten im Energiesektor des Unternehmens auftreten, wenn gezielte Angriffe erfolgen oder technische Fehler in der IKT-Infrastruktur auftreten?
- Welche Bedrohungsszenarien werden in Ihrem Unternehmen betrachtet?
- Gab es in der Vergangenheit Angriffe auf die IKT-Infrastruktur Ihres Unternehmens?
- Begeben Sie sich in eine Angreiferperspektive: Wo sehen Sie die größten IKT-Sicherheits-Schwachstellen in Energieanlagen im Allgemeinen?

A.4 Sektorenkopplung und Ausblick in die Zukunft

- Welche Veränderungen erwarten Sie im Rahmen einer verstärkten Sektorenkopplung und der Energiewende in ihrem Energiesektor (insbesondere in Bezug auf Digitalisierung, Kommunikation, ...)?

A.5 Eigeninitiative, Wiederholung und Abschluss

- Dem Interviewpartner/Der Interviewpartnerin die Möglichkeit einräumen weitere, aus seiner Sicht wichtige Informationen einzubringen.
- ggf. abschnittsweise, bei komplexeren Themen: Antworten, die gegeben wurden, werden kurz wiedergegeben/wiederholt und das Interview kurz zusammengefasst, damit das richtige Verständnis vom Interviewpartner nochmal bestätigt werden kann.
- Verabschieden des Interviewpartners