TU WIEN Informatics

Cybersicherheit in der Stromversorgung

Analyse von Bedrohungen und regulatorischen Sicherheitsanforderungen

BACHELORARBEIT

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

033 526 Wirtschaftsinformatik

eingereicht von

Alexander Tschimben
Matrikelnummer 12122570

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Ao.Univ.Prof. Mag.iur. Dr.iur. Markus Haslinger

Wien, 16. Oktober 2025

Alexander Tschimben

Markus Haslinger

Erklärung zur Verfassung der Arbeit

Alexander Tschimben

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 16. Oktober 2025

Alexander Tschimben

Abstract

Die Stromversorgung ist eine zentrale kritische Infrastruktur moderner Gesellschaften und macht andere wesentliche Sektoren überhaupt erst funktionsfähig. Aus ehemals rein physischen Infrastrukturen hat sich ein komplexes cyber-physisches System entwickelt. Diese Entwicklung eröffnet neue Chancen, vergrößert jedoch zugleich die Angriffsfläche für Bedrohungen aus dem Cyberraum.

Vor diesem Hintergrund widmet sich die Arbeit der Analyse der aktuellen Bedrohungslage in der Stromversorgung. Im Mittelpunkt stehen ausgewählte Fallbeispiele bedeutender Cyberangriffe der Vergangenheit, anhand derer die verwendeten Angriffsvektoren und Vorgehensweisen genauer analysiert werden. Aus den gewonnenen Erkenntnissen der Analyse lässt sich die wachsende Bedeutung regulatorischer Mindestsicherheitsanforderungen ableiten. Entsprechend werden im weiteren Verlauf die rechtlichen und regulatorischen Rahmenbedingungen der Cybersicherheit im Bereich der Stromversorgung beleuchtet. Der Fokus liegt dabei insbesondere auf der Frage, welche Einrichtungsarten in den Geltungsbereich dieser Vorgaben fallen und welche präventiven sowie reaktiven Cybersicherheitsanforderungen von den betroffenen Einrichtungen umzusetzen sind.

Inhaltsverzeichnis

KAPITEL 1

Einleitung

1.1 Aufgabenstellung

Die Stromversorgung zählt zu den zentralen kritischen Infrastrukturen moderner Gesellschaften. Ohne eine verlässliche Energieversorgung wären essenzielle gesellschaftliche Funktionen wie medizinische Versorgung, Kommunikation, Verkehr, Verwaltung und Industrie nicht aufrechtzuerhalten.[1] Durch die zunehmende Digitalisierung und Vernetzung wandelt sich die Stromversorgung zu einem hochkomplexen cyber-physischen System, in dem physische Anlagen durch digitale Komponenten überwacht und gesteuert werden.[2] Dieser Transformationsprozess wird auch auf europäischer Ebene aktiv unterstützt: Die Europäische Kommission schätzt den Investitionsbedarf für das Stromnetz zwischen 2020 und 2030 auf rund 584 Milliarden Euro, wovon ein erheblicher Anteil in die Digitalisierung fließen soll.[3] Damit eröffnen sich zwar erhebliche Chancen im Hinblick auf Flexibilität, Effizienz und die Integration erneuerbarer Energien, gleichzeitig entstehen jedoch neue sicherheitstechnische Herausforderungen.[4] Dass diese Risiken nicht nur theoretischer Natur sind, belegen die koordinierten Cyberangriffe auf die ukrainische

[1] Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.

[2] Vgl. Alvarez-Alvarado et al. (2024): Cyber-physical power systems: A comprehensive review about technologies, drivers, standards, and future perspectives, S. 3; Hasan et al. (2023) *Review on cyber-physical and cyber-security system in smart grid*, S. 1.

[3] Vgl. Europäische Kommission (2022): *Digitalisierung des Energiesystems – EU-Aktionsplan*, Abschnitt 1.

[4] Vgl. Hasan et al. (2023) *Review on cyber-physical and cyber-security system in smart grid*, S. 3 f.

Stromversorgung in den Jahren 2015 und 2016.[5]

Vor diesem Hintergrund analysiert diese Arbeit die Bedrohungslage, die regulatorischen Mindestsicherheitsanforderungen sowie den Geltungsbereich der Stromversorgung. Ausgangspunkt ist die Analyse der technischen Grundlagen: Dabei wird ein Überblick über die Struktur der Stromversorgung gegeben, einschließlich der eingesetzten digitalen Komponenten sowie der klassischen internen Netzwerkinfrastruktur von Stromnetzbetreibern. Darauf aufbauend wird untersucht, wie sich die Bedrohungslage für Einrichtungen in der Stromversorgung entwickelt hat, welche Angriffsvektoren in der Vergangenheit identifiziert wurden und wie bestätigte Cyberangriffe die Stromversorgung unterbrechen konnten.

Aus der identifizierten zunehmenden Anzahl und Komplexität von Cyberbedrohungen ergibt sich die Notwendigkeit, regulatorisch verankerte Mindestsicherheitsanforderungen festzulegen, um ein einheitliches Schutzniveau zu gewährleisten. Daran anschließend folgt eine Analyse der geltenden rechtlichen und regulatorischen Rahmenbedingungen der Cybersicherheit im Bereich der Stromversorgung. Die Arbeit befasst sich insbesondere mit den präventiven und reaktiven Sicherheitsanforderungen auf Einrichtungsebene, ihrer Entwicklung und ihrem Geltungsbereich im Elektrizitätssektor. Ausgangspunkt bildet das unionsrechtliche Sekundärrecht, insbesondere die Richtlinie (EU) 2016/1148 (NIS1)[6], ihre Neufassung durch die Richtlinie (EU) 2022/2555 (NIS2)[7] sowie die delegierte Verordnung (EU) 2024/1366 (NCCS)[8]. Anschließend wird untersucht, wie diese Vorgaben in Österreich umgesetzt bzw. in Umsetzung sind und welche Pflichten sich daraus für Einrichtungen des Elektrizitätssektors ergeben.

Die Arbeit konzentriert sich dabei ausschließlich auf die Stromversorgung, während angrenzende Sektoren wie Gas- oder Wasserversorgung nicht berücksichtigt werden.

[5] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*; BBC News (2017): *Ukraine power cut 'was cyber-attack'*.

[6] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. L 194 vom 19.7.2016, S. 1.

[7] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, ABl. L 333 vom 27.12.2022, S. 80.

[8] Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 durch sektorspezifische Cybersicherheitsaspekte grenzüberschreitender Stromflüsse, ABl. L 141 vom 24.5.2024, S. 1.

1.2 Aufbau

Diese Arbeit gliedert sich in sechs Kapitel, die schrittweise von den technischen Grundlagen über die Analyse der Bedrohungslage bis hin zu rechtlichen Rahmenbedingungen führen.

Kapitel 2 vermittelt zunächst die technischen Grundlagen der Stromversorgung. Es wird ein Überblick über die Grundstruktur der Stromversorgung gegeben. Anschließend wird die zunehmende Digitalisierung der Stromnetze sowie deren Kommunikationsarchitektur näher erläutert. Ziel dieses Kapitels ist es, die technischen Grundlagen der Stromversorgung zu vermitteln, die für das Verständnis der nachfolgenden Analyse der Bedrohungslage erforderlich sind.

Kapitel 3 widmet sich der aktuellen Bedrohungslage in der Stromversorgung. Eingangs wird die Entwicklung der gemeldeten Cybervorfälle im Zeitraum zwischen 2020 und 2024 und deren mögliche Ursachen aufgezeigt. Im Mittelpunkt des Kapitels stehen die bedeutendsten öffentlich bekannten Cyberangriffe auf die Stromversorgung, aus denen die verwendeten Angriffsvektoren identifiziert und anschließend näher analysiert werden.

Kapitel 4 untersucht, welche rechtlichen Mindestanforderungen die Europäische Union zur Stärkung der Cybersicherheit eingeführt hat. Im Mittelpunkt stehen dabei die Richtlinie (EU) 2016/1148, ihre Neufassung durch die Richtlinie (EU) 2022/2555 sowie die delegierte Verordnung (EU) 2024/1366. Der Fokus liegt nicht auf einer vollständigen Analyse sämtlicher Regelungsinhalte, sondern auf dem Geltungsbereich im Elektrizitätssektor sowie auf den präventiven und reaktiven Cybersicherheitsanforderungen auf Einrichtungsebene.

Kapitel 5 widmet sich anschließend der Umsetzung der genannten EU-Richtlinien in das österreichische Recht. Analog zu Kapitel 4 werden dabei der Geltungsbereich im Elektrizitätssektor sowie die präventiven und reaktiven Cybersicherheitsanforderungen auf nationaler Ebene untersucht. Der Schwerpunkt liegt auf der Umsetzung der Richtlinie (EU) 2016/1148, die in Österreich bereits vollständig in nationales Recht überführt wurde. Darüber hinaus wird der aktuelle Stand der Umsetzung der Richtlinie (EU) 2022/2555 analysiert.

KAPITEL 2

Technische Grundlagen

Zur Einordnung der Bedrohungslage werden in diesem Kapitel die wesentlichen technischen Grundlagen der Stromversorgung erläutert. Dazu zählen sowohl der Aufbau und die Funktionsweise des Stromnetzes als auch die digitale Kommunikationsebene der Netzbetreiber. Abschließend werden die grundlegenden Konzepte der Cybersicherheit definiert.

2.1 Grundstruktur der Stromversorgung

Die Anfänge der Stromversorgung lassen sich bis an die Wende zum 19. Jahrhundert zurückverfolgen.[9] Zu dieser Zeit wurde Elektrizität noch dezentral erzeugt, meist unmittelbar an den Orten, an denen sie auch verbraucht wurde.[10] Der steigende Strombedarf in Haushalten und Industrie führte zur Entwicklung eines zentral organisierten Versorgungssystems für ganze Regionen.[11] Durch die Liberalisierung des Strommarkts wurden die zuvor zusammenhängenden Strukturen rechtlich entflechtet und in Erzeugung, Übertragung und Verteilung gegliedert (Unbundling).[12]

Da Strom nicht effizient gespeichert werden kann und in der Regel unmittelbar verbraucht werden muss, übernehmen große Kraftwerke die kontinuierliche Erzeu-

[9] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 9.

[10] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 9.

[11] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 10 f.

[12] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 13.

gung von Strom.[13] Für den Transport des Stroms über weite Entfernungen sind die Übertragungsnetzbetreiber (ÜNB) verantwortlich. Sie betreiben das überregionale Stromnetz, das insbesondere das Höchstspannungsniveau und Hochspannungsniveau abdeckt.[14] Die Verteilnetzbetreiber (VNB) übernehmen den Transport von Strom auf regionaler Ebene und leiten ihn über Mittelspannungsnetze und Niederspannungsnetze weiter zu den Endverbrauchern.[15] Um die Spannung zwischen diesen Netzebenen schrittweise zu reduzieren, kommen Umspannwerke zum Einsatz.[16] Sie wandeln die elektrische Spannung technisch so um, dass ein sicherer und verlustarmer Weitertransport innerhalb der jeweiligen Netzebene gewährleistet ist.[17]

Das europäische Stromnetz gilt laut dem Europäischen Rechnungshof als die größte und komplexeste technische Infrastruktur, die jemals in Europa geschaffen wurde. Innerhalb der Europäischen Union erstreckt es sich über mehr als 11,3 Millionen Kilometer.[18] In diesem Rahmen besteht das Netz aus einer vergleichsweise kleinen Zahl an ÜNB und einer deutlich größeren Zahl an VNB. So gibt es in der EU insgesamt 30 ÜNB und 2.589 VNB.[19] In Österreich sind derzeit zwei ÜNB für das Höchstspannungsnetz verantwortlich, die Austrian Power Grid AG und die Vorarlberger Übertragungsnetz GmbH, sowie rund 124 VNB, die den regionalen Betrieb sicherstellen.[20]

2.2 Digitale Kommunikationsebene

In der Fachliteratur werden moderne Stromnetze oft als cyber-physisches System (CPS) bzw. Smart Grid beschrieben. Es handelt sich dabei um ein verteiltes System,

[13] Dabrowski et al. (2017): *Grid Shock: Coordinated Load-Changing Attacks on Power Grids*, S. 312; Europäischer Rechnungshof (2025): *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*, S. 15 und 9.

[14] Vgl. Europäischer Rechnungshof (2025): *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*, S. 15 und 9.

[15] Vgl. Europäischer Rechnungshof (2025): *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*, S. 15 und 9.

[16] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 395.

[17] Vgl. Schwab (2022): *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*, S. 395.

[18] Vgl. Europäischer Rechnungshof (2025): *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*, S. 12.

[19] Vgl. Europäischer Rechnungshof (2025): *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*, S. 165 f.

[20] Vgl. Oesterreichs Energie (2020): *Netzberechnungen Österreich – Einfluss der Entwicklungen von Elektromobilität und Photovoltaik auf das österreichische Stromnetz*, S. 6.

in dem physische Prozesse durch digitale Komponenten überwacht und gesteuert werden.[21]

Zur besseren Veranschaulichung folgt im Weiteren ein vereinfachter Überblick über die digitale Kommunikationsebene eines einzelnen ÜNB oder VNB. Dabei erfolgt die Betrachtung bewusst auf Ebene eines einzelnen Netzbetreibers, um die Komplexität einzugrenzen und die Strukturen nachvollziehbar darzustellen.

2.2.1 Büronetzwerk und Prozesssteuerungsnetzwerk

Die Netzwerke eines Stromnetzbetreibers zeichnen sich klassischerweise durch eine Trennung von administrativen und betrieblichen Netzwerken aus.[22] Das Büronetzwerk ist typischerweise mit dem öffentlichen Internet verbunden, um Dienste wie die E-Mail-Kommunikation und andere klassische Unternehmensaufgaben zu ermöglichen.[23] Im Gegensatz dazu ist das Prozesssteuerungsnetzwerk für die direkte Anbindung und Steuerung der physischen Anlagen zuständig.[24]

Der Datenaustausch zwischen dem Büronetzwerk und dem Prozesssteuerungsnetzwerk sollte idealerweise streng über einen gesicherten Datenaustauschserver abgewickelt werden, jedoch gibt es in der Praxis oft zusätzliche Kommunikationswege.[25] Beispiele hierfür sind VPN-Verbindungen oder Fernwartungszugänge für Dienstleister, die eine direkte Kommunikation zwischen den Netzwerken ermöglichen.[26]

2.2.2 Prozesssteuerungsnetzwerk

Für die tatsächliche Steuerung und Überwachung des Stromnetzes betreiben Stromnetzbetreiber, wie bereits erwähnt, ein separates Kommunikationsnetz.[27] Dieses Netzwerk wird als Prozesssteuerungsnetzwerk (PCN) bezeichnet und besteht in der Regel aus einer Reihe von Teilnetzwerken.[28] Die Kommunikation zwischen den

[21] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3; Yohanandhan et al. (2020): *Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications*, S. 151020.

[22] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.

[23] Vgl. Van der Velde et al. (2020): *Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures*, S. 18.

[24] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.

[25] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.

[26] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.

[27] Vgl. Van der Velde et al. (2020): *Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures*, S. 18.

[28] Vgl. Van der Velde et al. (2020): *Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures*, S. 18.

Teilnetzwerken erfolgt dabei über etablierte industrielle Steuerungsprotokolle wie IEC 60870-5-104 oder DNP3.[29]

Ein wichtiger und zentraler Bestandteil des PCN ist das Kontrollzentrum, das ein Supervisory Control and Data Acquisition (SCADA)-System nutzt. Als überwachender und steuernder Bestandteil analysiert dieses SCADA-System Sensordaten, die überwiegend von Umspannwerken stammen, und kann darauf basierend Steuerbefehle zurücksenden.[30] Wie der Name SCADA bereits andeutet, erfolgt die Steuerung unter Aufsicht durch einen zuständigen Operator und ist somit nicht vollständig automatisiert, sondern manuell beeinflussbar.[31] So kann der Operator über eine Mensch-Maschine-Schnittstelle (HMI) Steuerbefehle erzeugen, die über ein Gateway an die Netzwerke der jeweiligen Umspannwerke übermittelt werden.[32] Um eine koordinierte Steuerung des Stromnetzes über regionale Grenzen hinweg sicherzustellen, können die SCADA-Systeme verschiedener ÜNB und VNB miteinander vernetzt werden.[33]

Aus einer abstrakten Perspektive handelt es sich im PCN um einen bidirektionalen Datenaustausch: Sensordaten werden von den Feldgeräten über verschiedene Netzwerke an das Kontrollzentrum übertragen, dort analysiert und gespeichert.[34] Basierend auf den Auswertungen der Daten sendet das Kontrollzentrum Steuerbefehle zurück an die Feldgeräte, um den Betrieb der physischen Anlagen zu regeln.[35]

Die Bedeutung der digitalen Steuerung im PCN wird in Zukunft noch weiter zunehmen. Das liegt vor allem daran, dass künftig immer mehr kleine und mittlere Kraftwerke, vor allem aus dem Bereich der erneuerbaren Energien, an das Verteilnetz angeschlossen werden.[36] Diese dezentrale Stromerzeugung stellt die Netzbetreiber vor neue Herausforderungen, da es dadurch unter anderem schwieriger wird, das Gleichgewicht zwischen Stromverbrauch und Stromerzeugung aufrechtzuerhalten.[37]

[29] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 4.
[30] Vgl. Geeta und Kolin (2021): *Architecture and security of SCADA systems: A review*, S. 3 f.
[31] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.
[32] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.
[33] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3.
[34] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 3; Hasan et al. (2023) *Review on cyber-physical and cyber-security system in smart grid*, S. 3 f.
[35] Vgl. Hasan et al. (2023) *Review on cyber-physical and cyber-security system in smart grid*, S. 3 f.
[36] Vgl. Oesterreichs Energie: *Digitalisierung: warum das Stromnetz intelligent werden muss.*
[37] Vgl. Oesterreichs Energie: *Digitalisierung: warum das Stromnetz intelligent werden muss.*

2.3 Definition und Abgrenzung von Cybersicherheit

Um den Begriff Cybersicherheit klar einordnen zu können, ist zunächst ein Überblick darüber notwendig, wie sie sich von anderen Sicherheitskonzepten abgrenzt. Zwar werden die Begriffe Informationssicherheit, IT-Sicherheit und Cybersicherheit häufig synonym verwendet, sie unterscheiden sich jedoch in ihrem jeweiligen Fokus und decken unterschiedliche, sich teilweise überschneidende Bereiche ab.[38]

2.3.1 Informationssicherheit

Informationssicherheit bezeichnet den Schutz von Informationen, unabhängig davon, ob sie digital verarbeitet, auf Papier festgehalten oder synaptisch gespeichert werden.[39] Die international anerkannte Norm ISO/IEC 27000:2018 definiert den Begriff Informationssicherheit als den Schutz dreier zentraler Aspekte, die als CIA-Triade bekannt sind:[40]

- **Vertraulichkeit**: Schutz von Informationen vor unautorisiertem Zugriff.[41]
- **Integrität**: Schutz von Informationen vor unbeabsichtigter oder unbefugter Veränderung.[42]
- **Verfügbarkeit**: Sicherstellung, dass Informationen für berechtigte Nutzer bei Bedarf zugänglich sind.[43]

2.3.2 IT-Sicherheit

Im Gegensatz zur Informationssicherheit, die den Schutz sämtlicher Informationen umfasst, konzentriert sich die IT-Sicherheit ausschließlich auf digitale Systeme und die darin gespeicherten oder verarbeiteten Daten.[44] Dabei umfasst die IT-Sicherheit nicht nur die klassischen Schutzziele der CIA-Triade, sondern erweitert

[38] Vgl. Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 2 f.
[39] Vgl. Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 4.
[40] Vgl. ISO/IEC (2018): ISO/IEC 27000:2018, Kl. 3.28.
[41] Vgl. ISO/IEC (2018): *ISO/IEC 27000:2018*, Kl. 3.10.
[42] Vgl. ISO/IEC (2018): *ISO/IEC 27000:2018*, Kl. 3.36.
[43] Vgl. ISO/IEC (2018): *ISO/IEC 27000:2018*, Kl. 3.7.
[44] Vgl. Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 3.

diese um zusätzliche Schutzziele.[45] Die IT-Sicherheit ist somit ein Teilbereich der umfassenderen Informationssicherheit.

2.3.3 Cybersicherheit

Cybersicherheit erweitert den traditionellen Fokus der IT-Sicherheit und stellt den Schutz des gesamten sogenannten Cyberraums in den Mittelpunkt. Die Definition des Begriffs Cyberraum ist vielschichtig und umfasst nach Pohlmann nicht nur die technischen Komponenten, also alle mit dem globalen Internet verbundenen IT-Systeme, Infrastrukturen sowie deren Kommunikationsprozesse, Anwendungen, Daten und Informationen, sondern auch die Akteure, die in diesem Raum agieren, einschließlich krimineller Organisationen und anderer Angreifer.[46] Dementsprechend kann Cybersicherheit als übergeordnete Disziplin verstanden werden, in der die IT-Sicherheit einen integralen Bestandteil bildet.[47]

Auf europäischer Ebene wird Cybersicherheit in verschiedenen Rechtsakten in den Begriffsbestimmungen definiert.[48] Dabei verweisen die Rechtsakte explizit auf die Definition in der Verordnung (EU) 2019/881:[49]

> *„Cybersicherheit“ bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen*[50]

[45] Vgl. Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 3.

[46] Vgl. Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 2 f.

[47] Vgl. Pohlmann 2019: *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 2.

[48] Vgl. Art. 6 Nr. 3 der RL (EU) 2022/2555; Art. 3 Nr. 12 der VO (EU) 2024/1366.

[49] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013, ABl. L 151 vom 7.6.2019, S. 15.

[50] Siehe Art. 2 Nr. 1 der VO (EU) 2019/881.

Aus der vorherigen Analyse der Begriffsabgrenzungen von Informationssicherheit, IT-Sicherheit und Cybersicherheit lässt sich die Abbildung 2.1 zur besseren Veranschaulichung der Zusammenhänge ableiten:

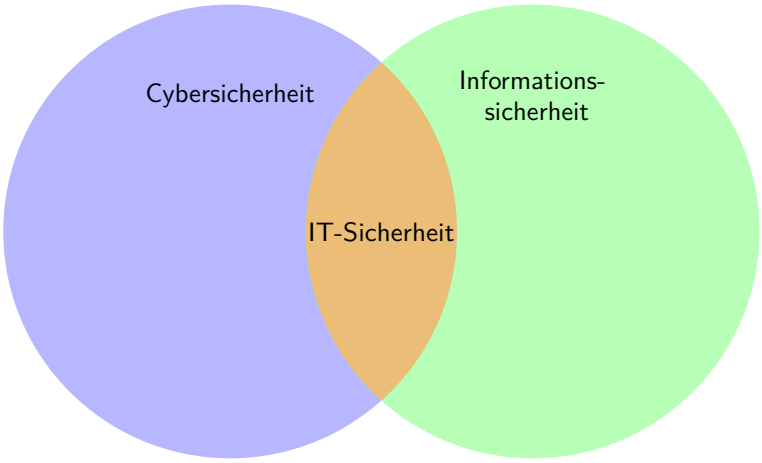

Abbildung 2.1: Begriffliche Einordnung von Cybersicherheit, Informationssicherheit und IT-Sicherheit[51]

[51] Eigene Darstellung in Anlehnung an Pohlmann (2019): *Cybersicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*, S. 5.

KAPITEL 3

Cyberbedrohungen für die Stromversorgung

Nachdem in Kapitel 2 die technischen Grundlagen und die begriffliche Einordnung der Cybersicherheit dargestellt wurden, richtet sich der Blick nun auf die praktische Ebene. In diesem Kapitel wird zunächst die aktuelle Bedrohungslage im Energiesektor dargestellt und ihre Entwicklung in den vergangenen Jahren aufgezeigt. Anschließend werden zentrale Angriffsvektoren analysiert, die bei den bekanntesten Cyberangriffen auf die Stromversorgung verwendet wurden. Darauf aufbauend erfolgt eine detaillierte Untersuchung dieser Angriffe, bei der sowohl das Vorgehen der Angreifer als auch die dabei ausgenutzten Schwachstellen betrachtet werden.

3.1 Entwicklung der Bedrohungslage

Die Abbildung 3.1 veranschaulicht die Entwicklung der gemeldeten Sicherheitsvorfälle im Energiesektor im Zeitraum von April 2020 bis Juni 2024, basierend auf den ENISA Threat Landscape (ETL) Reports des jeweiligen Berichtszeitraums.

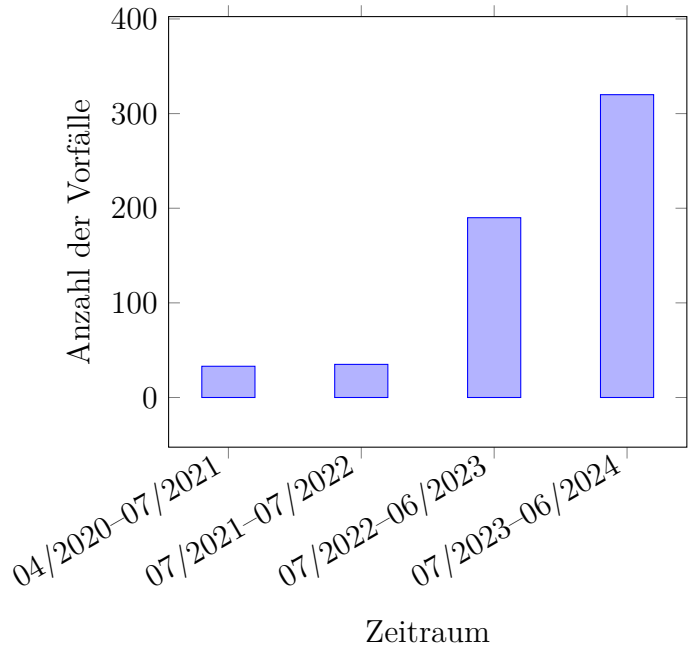

Abbildung 3.1: Anzahl gemeldeter Sicherheitsvorfälle im Energiesektor.[52]

Während die Anzahl der gemeldeten Sicherheitsvorfälle in den ersten beiden Berichtszeiträumen noch vergleichsweise gering bei um die 34 Vorfällen lag, zeigt sich ab Juli 2022 ein deutlicher Anstieg.[53] So wurden im Zeitraum von Juli 2022 bis Juni 2023 bereits 190 Sicherheitsvorfälle gemeldet, was einem Anstieg von etwa 459 % im Vergleich zum Vorjahr entspricht.[54] Im darauffolgenden Zeitraum stieg die Anzahl der gemeldeten Vorfälle weiter auf 320, was eine weitere Zunahme von etwa 68 % gegenüber dem Vorjahr entspricht.[55]

Ein wesentlicher Grund, warum der Energiesektor ins Visier von Cyberangriffen gerät, ist seine zentrale Rolle für eine funktionierende moderne Gesellschaft.[56] Ein Stromausfall kann kaskadenartige Störungen in anderen kritischen Bereichen verursachen, da viele weitere wesentliche Sektoren unmittelbar von einer stabilen

[52]Eigene Darstellung. Die Daten basieren auf: ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 14; ENISA et al. (2023): *ENISA threat landscape 2023 – July 2022 to June 2023*, S. 13; ENISA et al. (2022): *ENISA threat landscape 2022 – July 2021 to July 2022*, S. 15; ENISA et al. (2021): *ENISA threat landscape 2021 – April 2020 to mid-July 2021*, S. 12.

[53]Vgl. ENISA et al. (2022): *ENISA threat landscape 2022 – July 2021 to July 2022*, S. 15; ENISA et al (2021): *ENISA threat landscape 2021 – April 2020 to mid-July 2021*, S. 12.

[54]Vgl. ENISA et al. (2023): *ENISA threat landscape 2023 – July 2022 to June 2023*, S. 13.

[55]Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 14.

[56]Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.

Stromversorgung angewiesen sind.[57] Solche kaskadenartige Störungen können erhebliche wirtschaftliche und gesellschaftliche Folgen nach sich ziehen.[58] Wie real und folgenschwer ein großflächiger Stromausfall sein kann, zeigt das Beispiel Venezuela: Zwischen dem 7. und 14. März 2019 kam es dort zu einem landesweiten Blackout, dessen Folgen zahlreiche weitere wesentliche Sektoren betrafen.[59]

Betroffen waren unter anderem die Telekommunikation, die Ölindustrie, der Finanzsektor sowie die Versorgung mit Lebensmitteln, Wasser und medizinischen Leistungen.[60] Dabei fielen Fernsehsender, Mobilfunknetze und Internet weitgehend aus, Kartenzahlungen und Abhebungen waren nicht möglich, und Transaktionen erfolgten vielfach nur noch in US-Dollar.[61] Kühlketten brachen zusammen, ganze Städte blieben mehrere Tage ohne Wasser, und in Krankenhäusern führte Treibstoffmangel zu eingeschränktem Betrieb und Todesfällen.[62] Auch Förderplattformen in der Ölindustrie wurden stillgelegt, was die Produktion zeitweise halbierte.[63] Obwohl die Stromversorgung nach etwa sieben Tagen weitgehend wiederhergestellt wurde, führte die Regierung eine 30-tägige Stromrationierung ein.[64]

Das Beispiel zeigt, dass ein großflächiger und länger andauernder Ausfall der Stromversorgung weitreichende gesellschaftliche und wirtschaftliche Folgen haben kann. Vor diesem Hintergrund werden Cyberangriffe auf Energieinfrastrukturen zunehmend als strategisches Mittel hybrider Kriegsführung verstanden.[65] Der europäische Branchenverband Eurelectric warnt in diesem Zusammenhang ausdrücklich davor, dass solche Angriffe eingesetzt werden können, um ganze Regionen oder sogar Staaten zu destabilisieren.[66]

Diese Einschätzung wird durch die Cyberangriffe auf die ukrainische Stromversorgung in den Jahren 2015 und 2016 untermauert (siehe Abschnitt 3.4). Laut dem US-Justizministerium waren Mitglieder der russischen Militäreinheit GRU-Einheit 74455 für die Angriffe verantwortlich.[67] Im Jahr 2020 erhob das US-

[57] Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.
[58] Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.
[59] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 18.
[60] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 19 f.
[61] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 19.
[62] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 19.
[63] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 20.
[64] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 20.
[65] Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.
[66] Vgl. Eurelectric (2025): *Cybersecurity in the Power Sector*.
[67] Vgl. U.S. Department of Justice (2020): *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware*.

Justizministerium Anklage gegen sechs Angehörige dieser Einheit. Ihnen wird vorgeworfen, unter anderem die Schadsoftware BlackEnergy, Industroyer und KillDisk entwickelt und verbreitet zu haben, um die Stromversorgung der Ukraine zu sabotieren.[68]

Auch der Anstieg der gemeldeten Sicherheitsvorfälle im Jahr 2022 steht möglicherweise im Zusammenhang mit dem Konflikt zwischen Russland und der Ukraine.[69] Laut einem Bericht von Thales sind im Jahr 2022 rund 61% aller weltweit registrierten Angriffe auf russische Akteure zurückzuführen.[70] Besonders im Visier standen dabei Länder, die die Ukraine politisch und militärisch unterstützen.[71]

3.2 Angriffsvektoren für die Stromversorgung

In diesem Abschnitt werden die Angriffsvektoren bekannter Cyberangriffe (siehe Abschnitt 3.4) abgeleitet und genauer analysiert.

3.2.1 Social Engineering

Social Engineering bezeichnet einen Angriffsvektor, bei dem Angreifer in erster Linie das menschliche Fehlverhalten ausnutzen.[72] Grundsätzlich lassen sich solche Angriffe in zwei Hauptkategorien einteilen: menschlichbasierte und computerbasierte Ansätze.[73] Während bei menschlichbasierten Angriffen ein direkter Kontakt zwischen Täter und Opfer besteht, ist die Reichweite in der Regel auf eine begrenzte Zahl von Personen beschränkt.[74] Computerbasierte Angriffe dagegen erfolgen über digitale Endgeräte und können dadurch gleichzeitig eine große Zahl potenzieller Opfer erreichen.[75]

Zur Durchführung von Social-Engineering-Angriffen steht eine breite Methodenpalette zur Verfügung. Die Europäische Cybersicherheit Agentur ENISA nennt in ihrem ETL-Report 2024 die am häufigsten eingesetzten Typen.[76]

[68] Vgl. U.S. Department of Justice (2020): *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware.*
[69] Vgl. Vincent und Pietralunga (2023): *Cyberattacks on the rise in Europe amidst the war in Ukraine.*
[70] Vgl. Vincent und Pietralunga (2023): *Cyberattacks on the rise in Europe amidst the war in Ukraine.*
[71] Vgl. Vincent und Pietralunga (2023): *Cyberattacks on the rise in Europe amidst the war in Ukraine.*
[72] Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 7.
[73] Vgl. Salahdine et al. (2019): *Social Engineering Attacks: A Survey*, S. 3.
[74] Vgl. Salahdine et al. (2019): *Social Engineering Attacks: A Survey*, S. 3
[75] Vgl. Salahdine et al. (2019): *Social Engineering Attacks: A Survey*, S. 3
[76] Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 7.

- Phishing
- Spear-Phishing
- Whaling
- Smishing
- Vishing
- Watering-Hole-Attacken
- Baiting
- Pretexting
- Quid pro quo
- Honeytraps
- Scareware

Im Bereich der Stromversorgung werden Social-Engineering-Angriffe vor allem als initiale Schwachstelle genutzt, um einen ersten Zugriff auf das Büronetzwerk zu erlangen (siehe Abschnitt 3.4). Bei den Angriffen auf ukrainische Netzbetreiber in den Jahren 2015 und 2016 setzten die Täter täuschend echt gestaltete Phishing-E-Mails ein, um das Vertrauen der Mitarbeitenden zu gewinnen und sie dazu zu bringen, infizierte Anhänge zu öffnen.[77]

3.2.2 Denial-of-Service

Bei einem Denial-of-Service (DoS) handelt es sich um einen Angriffsvektor mit dem Hauptziel, legitimen Systemen den Zugriff auf wichtige Systemressourcen zu verwehren.[78] Ein Distributed-Denial-of-Service (DDoS)-Angriff ist eine koordinierte Variante des klassischen DoS-Angriffs, bei der eine große Zahl geografisch verteilter Systeme gleichzeitig auf ein Zielsystem einwirkt, um dessen Verfügbarkeit zu beeinträchtigen.[79] Die verteilten Systeme sind in der Regel mit Malware infiziert, die im Hintergrund agiert, sodass ihre Besitzer nicht wissen, dass ihr System

[77] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*; Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 4 f.
[78] Vgl. Srivastava et al. (2023): *A Review on Protecting SCADA Systems from DDOS Attacks*, S. 556.
[79] Vgl. Srivastava et al. (2023): *A Review on Protecting SCADA Systems from DDOS Attacks*, S. 557.

Teil des Angriffs sind.[80] DDoS-Angriffe sind deshalb so beliebt, da diese Art der Angriffskoordination nicht nur die Wirksamkeit des Angriffs verstärkt, sondern auch die Rückverfolgung des Angriffs erschwert.[81]

Abbildung 3.2 zeigt den typischen Ablauf eines DDoS-Angriffs. Ein Angreifer kontrolliert und koordiniert dabei mehrere kompromittierte Systeme (Botnetz).[82] Diese kompromittierten Systeme senden gleichzeitig eine große Anzahl an Anfragen an das Zielsystem, sodass dessen Ressourcen überlastet werden.[83] Dadurch wird der reguläre Zugriff auf den Dienst verhindert, was zu einem teilweisen oder vollständigen Ausfall führen kann.[84]

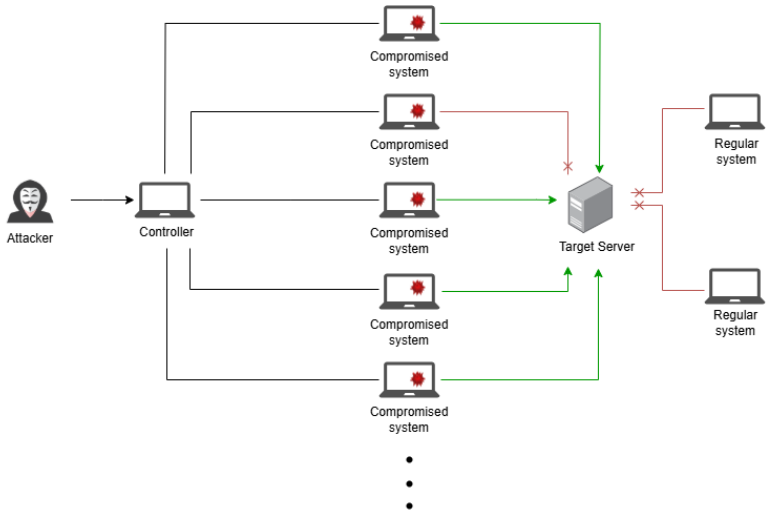

Abbildung 3.2: Ablauf eines Denial-of-Service-Angriffs.[85]

Im Bereich der Stromversorgung konnten mehrere DoS-Angriffe beobachtet werden. Beim Cyberangriff 2015 wurden unter anderem Callcenter und Websites der betroffenen Energieversorger durch DDoS-Angriffe zeitweise lahmgelegt. Infolgedessen konnten die betroffenen Kunden der Netzbetreiber keine Auskünfte über

[80] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 593.

[81] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 593.

[82] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 557.

[83] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 557.

[84] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 557.

[85] Eigene Darstellung nach Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 557.

die aktuelle Situation erhalten.[86] Beim Angriff im Jahr 2016 nutzten die Angreifer gezielt Schwachstellen in Schutzrelais von Umspannwerken aus und setzten diese mithilfe eines speziell entwickelten DoS-Tools außer Betrieb.[87] Betroffene Schutzrelais reagierten nicht mehr auf Steuerbefehle und mussten manuell neu gestartet werden.[88]

Gleichzeitig zeigt sich, dass Systeme von Energieversorgern nicht nur Ziel, sondern auch unbeabsichtigter Bestandteil eines Angriffs werden können. So wurden beim Angriff auf die dänische Energieinfrastruktur im Jahr 2023 kompromittierte Firewalls von mehreren Energieunternehmen selbst für DDoS-Angriffe missbraucht.[89]

DDoS-Angriffe stellen außerdem eine große Bedrohung für SCADA-Systeme dar, da SCADA-Systeme auf eine stabile Echtzeitkommunikation angewiesen sind.[90] Kalluri et al. konnten in einer Simulation zeigen, dass ein DDoS-Angriff auf die SCADA-Infrastruktur zu einer signifikanten CPU-Überlastung, erhöhtem Paketverlust und massiven Verzögerungen in der Datenverarbeitung führt.[91]

3.2.3 Lieferketten

Mit der Entscheidung, ein Produkt eines Dritten zu verwenden, vertraut ein Netzbetreiber zugleich darauf, dass dieser in gewissem Maße für die Sicherheit des Produkts verantwortlich ist. Potenzielle Angriffsvektoren betreffen daher nicht nur Sicherheitslücken in den eigenen Systemen, sondern erstrecken sich auch auf Drittparteien wie Zulieferer, Dienstleister oder Subunternehmen.[92] Die Ausnutzung solcher externen Schnittstellen stellt eine besonders kritische und schwer kontrollierbare Bedrohung dar, da Sicherheitslücken in der Lieferkette häufig weniger transparent und schwerer zu überwachen sind.[93]

Ein besonders gravierender Fall tritt ein, wenn Hersteller von Leitsystem-Software kompromittiert werden. Über bestehende Fernwartungsschnittstellen könnten An-

[86] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*.
[87] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 15.
[88] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 15.
[89] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 23-25.
[90] Vgl. Markovic-Petrovic et al. (2013): *Analysis of SCADA system vulnerabilities to DDoS attacks*, S. 593.
[91] Vgl. Kalluri et al. (2016): *Simulation and impact analysis of denial-of-service attacks on power SCADA*, S. 3 f.
[92] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 7.
[93] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 7.

greifer so gleichzeitig Zugriff auf die Systeme mehrerer Netzbetreiber erlangen.[94] Dieses Risiko steigt zusätzlich bei cloudbasierten Lösungen.[95]

Ein prominentes Beispiel ist die Dragonfly-Malware, die unter anderem Unternehmen in der Energieversorgung ins Visier nahm.[96] Dabei kompromittierten die Angreifer Softwareprodukte von drei verschiedenen Herstellern industrieller Steuerungssysteme und platzierten ihre Schadsoftware in öffentlich zugänglichen Softwarepaketen auf den Websites dieser Anbieter.[97]

Ein Sonderfall solcher Angriffe betrifft die Manipulation der Lieferkette bereits während der Produktion von Feldgeräten.[98] Solche Manipulationen sind besonders schwer zu erkennen, da sie tief in Hardware oder Firmware implementiert werden und es kompromittierten Geräten ermöglichen, heimlich zu kommunizieren oder externe Steuerbefehle zu empfangen.[99]

3.2.4 Man-in-the-Middle

Wie bereits im Abschnitt 2.2 erwähnt, nutzen Netzbetreiber einen bidirektionalen Datenaustausch im PCN. Durch diesen Datenaustausch stellen ungesicherte Kommunikationskanäle ein erhebliches Risiko dar.[100] Dabei ist insbesondere der sogenannte Man-in-the-Middle (MitM)-Angriff hervorzuheben. Bei diesem Angriffsvektor schleust sich ein Angreifer in eine bestehende Kommunikation ein, um Daten abzufangen, zu manipulieren oder sich als legitimer Kommunikationspartner auszugeben.[101]

Wlazlo et al. demonstrierten in einer cyber-physischen Testumgebung, wie ein Angreifer bei einem MitM-Angriff einen Binary Direct Operate Command (BDOC) abfangen und verändern kann. Bei einem BDOC handelt es sich um einen Steuerbefehl, mit dem Schutzschalter in Umspannwerken direkt aus der Ferne geöffnet oder

[94] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 7.
[95] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 7.
[96] Vgl. Khan et al. (2023): *Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids*, S. 180.
[97] Vgl. Khan et al. (2023): *Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids*, S. 180.
[98] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 7.
[99] Vgl. Alladi et al. (2020): *Industrial Control Systems: Cyberattack trends and countermeasures*, S. 4-7
[100] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 165.
[101] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 164.

geschlossen werden.[102] Der Befehl ist binär codiert und erlaubt nur zwei Zustände: TRIP (Öffnen) und CLOSE (Schließen).

So zeigten sie, wie ein TRIP-Befehl manipuliert und in einen CLOSE-Befehl umgewandelt werden kann.[103] Zusätzlich wird die Antwortnachricht des Zielsystems so verfälscht, dass für das Kontrollzentrum der Anschein entsteht, der ursprüngliche Befehl sei korrekt und unverändert ausgeführt worden.[104]

Ein großes Problem besteht darin, dass solche Angriffe nur sehr geringe Verzögerungen verursachen, die im normalen Betrieb kaum auffallen und dadurch schwer zu erkennen sind.[105] Zudem sind Industrieprotokolle wie DNP3 (hauptsächlich verwendet in Nordamerika und Teilen Asiens) in ihrer Standardversion meist unverschlüsselt.[106] Auch in Europa eingesetzte Protokolle wie IEC 60870-5-104 bieten ohne zusätzliche Schutzmaßnahmen keine ausreichende Sicherheit gegenüber MitM-Angriffen.[107]

3.2.5 Malware

„Malware“ ist ein Oberbegriff für jegliche Art von Schadsoftware, die mit der Absicht entwickelt wurde, einem System zu schaden, es zu manipulieren oder unbemerkt zu kontrollieren.[108] Malware wird in der Regel entweder selbst entwickelt oder über sogenannte Malware-as-a-Service (MaaS) Plattformen bezogen.[109] Solche Plattformen senken die Einstiegshürde für Cyberkriminalität erheblich, da Angreifer keine eigene Malware entwickeln müssen.[110]

In der Stromversorgung kamen verschiedene Arten von Malware zum Einsatz. Zu den bekanntesten gehören BlackEnergy, Industroyer und Industroyer2. Eine genauere Analyse der Funktionsweise der genannten Malware-Varianten erfolgt in Kapitel 3.3.

[102] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 170.
[103] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 169 f.
[104] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 171.
[105] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 166.
[106] Vgl. Wlazlo et al. (2021): *Man-in-the-middle attacks and defence in a power system cyber-physical testbed*, S. 167.
[107] Vgl. Krause et al. (2021): *Cybersecurity in Power Grids: Challenges and Opportunities*, S. 4.
[108] Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 56.
[109] Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 56.
[110] Vgl. ENISA et al. (2024): *ENISA threat landscape 2024 – July 2023 to June 2024*, S. 59.

3.3 Malware-Analysen

Dieser Abschnitt widmet sich der Analyse von Schadsoftware, die bei bedeutenden Cyberangriffen (siehe Abschnitt 3.4) auf die Stromversorgung eingesetzt wurde.

3.3.1 BlackEnergy

Die erste Version von BlackEnergy wurde bereits im Jahr 2007 entwickelt.[111] Ursprünglich handelte es sich bei BlackEnergy um einen einfachen Trojaner, der den Aufbau von Botnets für DDoS-Angriffe sowie die Ausführung einfacher Skripte auf den infizierten Hosts ermöglichte.[112] Die zweite Version BlackEnergy2 erweiterte die ursprüngliche Funktionalität deutlich und ermöglichte durch das variable Integrieren von weiteren Plugins den modularen Ausbau der Malware.[113] So konnten unter anderem Spionage, Datendiebstahl von Zugangsdaten, Keylogging, Netzwerkscans und Phishing durchgeführt werden.[114]

Im Jahr 2015 wurde bei den Cyberangriffen auf mehrere ukrainische VNB schließlich eine neue Variante der Malware beobachtet: BlackEnergy3.[115] Diese Version enthielt erstmals die bekannte Wiper-Malware KillDisk, die in mehreren Varianten auftrat und in der Lage war, Daten von Festplatten entweder vollständig zu löschen oder durch Überschreiben unbrauchbar zu machen.[116] Das spanische CSIRT INCIBE-CERT konnte drei verschiedene Varianten der Wiper-Malware identifizieren:[117]

- Win32/KillDisk.NBB
- Win32/KillDisk.NBC
- Win32/KillDisk.NBD

In den Netzwerken der betroffenen Netzbetreiber konnten zwar Spuren der Malware nachgewiesen werden.[118] Ermittler des US-Department of Homeland Security und

[111] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 7.
[112] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 8.
[113] Vgl. Khan et al. (2016): *Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid*, S. 4 f.
[114] Vgl. Khan et al. (2016): *Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid* , S. 4.
[115] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 11.
[116] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 11.
[117] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 11.
[118] Vgl. NJCCIC: *NJCCIC Threat Profile: BlackEnergy*.

des FBI stellten jedoch fest, dass die Funktionen von BlackEnergy3 den Stromausfall nicht direkt ausgelöst haben, sondern vielmehr den Angriff ermöglichten.[119] (siehe Abschnitt 3.4.1)

3.3.2 Industroyer

Eine weitere Malware, die bei einem Cyberangriff auf die Stromversorgung zum Einsatz kam, ist Industroyer, auch bekannt als CrashOverride (siehe Abschnitt 3.4.2).[120] Im Gegensatz zur Malware BlackEnergy3 fokussierte sich Industroyer direkt auf Kommunikationsprotokolle von industriellen Steuerungssystemen, um Leistungsschalter direkt zu manipulieren.[121] Die Sicherheitsfirma ESET konnte dabei die folgenden Kommunikationsprotokolle feststellen, die von der Malware implementiert wurden:[122]

- IEC 60870-5-101 (auch bekannt als IEC 101)
- IEC 60870-5-104 (auch bekannt als IEC 104)
- IEC 61850
- OLE for Process Control Data Access (OPC DA)

Die Malware besitzt einen modularen Aufbau und setzt sich aus mehreren Komponenten zusammen, die von einer Haupt-Backdoor gesteuert werden.[123] Diese Haupt-Backdoor installiert zusätzliche Komponenten, darunter einen Launcher, der zu einem festgelegten Zeitpunkt verschiedene Payloads ausführen kann.[124] Zu diesen Payloads zählt auch eine Wiper-Malware, die ähnlich wie bei BlackEnergy3 darauf abzielt, Spuren zu verwischen und die Wiederherstellung von Daten zu erschweren.[125] Die einzelnen Payloads sind für spezifische Protokolle entwickelt und entsprechend benannt.[126] Ein Überblick über den Aufbau der Malware wird in der Abbildung 3.3 veranschaulicht.

[119] Vgl. NJCCIC: *NJCCIC Threat Profile: BlackEnergy*.
[120] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems* , S. 2.
[121] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems* , S. 2.
[122] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems* , S. 2.
[123] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems* , S. 3.
[124] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems* , S. 5.
[125] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 13.
[126] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 6-12.

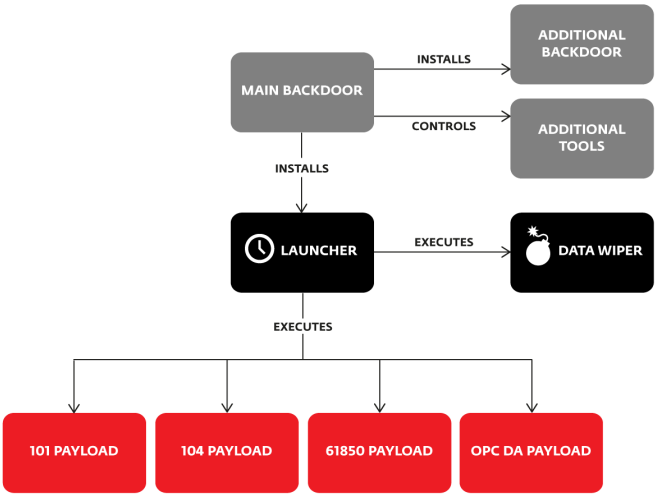

Abbildung 3.3: Vereinfachtes Schema der Win32/Industroyer-Komponenten.[127]

Für den Fall, dass die Haupt-Backdoor entdeckt wird, existiert eine weitere Backdoor, die als Windows-Notepad-Anwendung getarnt ist.[128] Die Haupt-Backdoor kontrolliert zudem diverse Tools, beispielsweise einen selbstprogrammierten Portscanner zur Identifizierung offener Ports im Netzwerk sowie ein DDoS-Tool.[129]

3.3.3 Industroyer2

Im Jahr 2022 entdeckten das ukrainische CSIRT CERT-UA und die slowakische Sicherheitsfirma ESET eine Weiterentwicklung der Malware Industroyer, bekannt als Industroyer2, die ebenfalls bei einem Cyberangriff auf die Stromversorgung eingesetzt wurde (siehe Abschnitt 3.4.3).[130] Die Malware-Variante ähnelt ihrem Vorgänger, weist jedoch eine noch gezieltere und geringere Funktionalität auf.[131]

Im Gegensatz zur Vorgängerversion, die als modulares Framework ausgelegt ist und vier verschiedene Kommunikationsprotokolle implementiert, liegt die neue Variante nur als einzelne ausführbare Datei vor und unterstützt ausschließlich das Protokoll IEC 60870-5-104.[132] Dieses Protokoll wird hauptsächlich in Europa und im Nahen

[127] Übernommen aus Cherepanov (2017): *Win32/Industroyer: A new threat for industrial control systems*, S. 2, Fig. 1.
[128] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 4 f.
[129] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 14 f.
[130] Vgl. Zafra et al. (2022): *INDUSTROYER.V2: Old Malware Learns New Tricks.*
[131] Vgl. Zafra et al. (2022): *INDUSTROYER.V2: Old Malware Learns New Tricks.*
[132] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*

Osten zur Überwachung und Steuerung von Stromnetzen eingesetzt und basiert auf dem TCP-Protokoll.[133]

Ein weiterer Unterschied zur Vorgängerversion besteht darin, dass die neue Malwarevariante dem Angreifer ermöglicht, individuelle Konfigurationen im Quellcode einzubetten, mit denen sich das Verhalten der Malware auf bestimmte Zielsysteme anpassen lässt.[134] Diese Flexibilität erfordert aber eine Neukompilierung, sobald Anpassungen an das Zielsystem vorgenommen werden.[135]

Industroyer2 weist jedoch auch Gemeinsamkeiten mit seinem Vorgänger auf, wie etwa die Ausgabe von Log-Dateien oder Konsolen-Outputs, die dazu dienen, den Ablauf der Malware zu protokollieren.[136] Im Unterschied zur früheren Version besteht diese jedoch nicht aus verständlichem Text, sondern aus schwer interpretierbaren Fehlercodes, was offenbar der Erschwerung einer Analyse dient.[137]

Auch bei Industroyer2 werden mehrere Arten von Wiper-Malware eingesetzt, um Spuren zu verwischen und die Wiederherstellung zu erschweren.[138] ESET konnte die folgenden Wiper-Malware-Varianten für unterschiedliche Betriebssysteme feststellen:[139]

- Neue Version von CaddyWiper (Windows)
- ORCSHRED (Linux)
- AWFULSHRED (Linux)
- SOLOSHRED (Solaris)

3.4 Fallbeispiele realer Cyberangriffe

In diesem Abschnitt werden die bekanntesten Cyberangriffe auf die Stromversorgung näher analysiert. Dabei liegt der Fokus insbesondere auf Angriffen, deren Ziel es war, die Stromversorgung zu unterbrechen oder erheblich zu stören.

[133] Vgl. Zafra et al. (2022): *INDUSTROYER.V2: Old Malware Learns New Tricks.*
[134] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[135] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[136] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[137] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[138] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[139] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*

Diese Fälle wurden ausgewählt, da sie als die bislang eindrucksvollsten und technisch ausgefeiltesten Beispiele gelten. Diese Angriffe bieten außerdem umfangreiche, öffentlich zugängliche Analysen und forensische Daten, die ein tiefergehendes Verständnis der eingesetzten Methoden und ihrer Auswirkungen ermöglichen.

3.4.1 Ukraine 2015 – Cyberangriff auf drei Verteilnetzbetreiber

Am 23. Dezember 2015 kam es in der Ukraine zu einem großflächigen Cyberangriff, bei dem gleichzeitig drei ukrainische VNB angegriffen wurden.[140] Der Stromausfall dauerte in einigen Regionen bis zu sechs Stunden an und betraf schätzungsweise 225.000 Haushalte.[141] Insgesamt gilt dieser Vorfall als der erste dokumentierte und erfolgreich durchgeführte Cyberangriff auf ein Stromnetz weltweit.[142]

Bereits im Mai 2014 wurden erste Versuche registriert, die Malware BlackEnergy per Phishing-E-Mails in der Ukraine zu verbreiten.[143] Im Folgejahr startete eine weitere Phishing-E-Mail-Kampagne, professioneller organisiert und in größerem Umfang. Die Angreifer versendeten täuschend echt gestaltete Nachrichten mit präparierten Microsoft-Office-Dokumenten im Anhang.[144] Öffneten die Empfänger der Mail diese Dokumente, erschien eine Sicherheitswarnung mit der Aufforderung, Makros zu aktivieren, um den vollständigen Inhalt anzuzeigen.[145] Nach Aktivierung der Makros installierte sich die Malware BlackEnergy3.[146] Betroffen waren unter anderem regionale Energieversorger sowie weitere kritische Infrastrukturen, darunter der Schienenverkehr.[147]

Abbildung 3.4 zeigt eine beispielhafte Phishing-E-Mail, wie sie im Rahmen dieser Kampagnen eingesetzt wurde. Die E-Mail, verfasst auf Ukrainisch und scheinbar von der Adresse info@rada.gov.ua versandt, gab vor, eine Mitteilung des ukrainischen Parlaments zu sein. Darin wurde ein angeblicher Präsidialerlass zur Teilmobilma-

[140] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*.
[141] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*.
[142] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack*.
[143] Vgl. Cherepanov und Lipovsky (2016): *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*, S. 1.
[144] Vgl. Cherepanov und Lipovsky (2016): *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*, S. 2.
[145] Vgl. Cherepanov und Lipovsky (2016): *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*, S. 3.
[146] Vgl. INCIBE-CERT (2024): *ICS malware analysis study: BlackEnergy*, S. 8.
[147] Vgl. Cherepanov und Lipovsky (2016): *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*, S. 1.

chung angekündigt, und die Empfänger wurden aufgefordert, Mitarbeiterlisten über den Anhang einzureichen.[148]

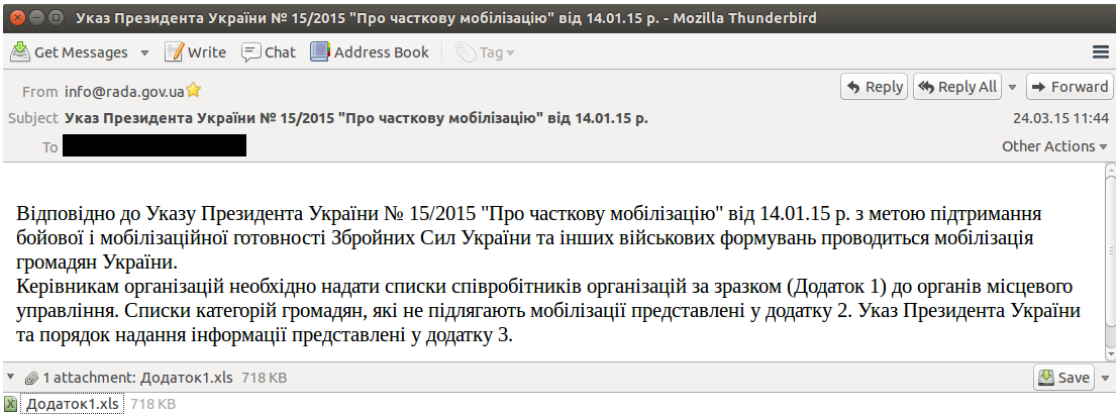

Abbildung 3.4: Phishing-E-Mail aus der BlackEnergy-Kampagne, wie sie auch ukrainische Energieversorger erhielten.[149]

Nach der erfolgreichen Einschleusung der Malware in das Büronetzwerk führten die Angreifer zunächst umfassende Aufklärungsaktivitäten durch. Dazu zählte insbesondere Keylogging, mit dem gültige VPN-Zugangsdaten von Arbeitsstationen im PCN abgefangen wurden.[150] Möglich war dies deshalb, weil keine Multi-Faktor-Authentifizierung implementiert war.[151] Mit den kompromittierten Zugangsdaten gelang den Angreifern, vom Büronetzwerk in das PCN zu pivotieren.[152] Im PCN kam ein passives Monitoring der HMI zum Einsatz, mit dem Bedienabläufe und Steuerlogik analysiert wurden.[153]

Der eigentliche Angriff wurde nach Unternehmensangaben synchronisiert durchgeführt und dauerte ingesamt nur 30 Minuten.[154] Über die kompromittierten HMI steuerten die Angreifer manuell die Leistungsschalter von 27 Umspannwerken und brachten damit Teile des Stromnetzes zum Stillstand.[155] Nach erfolgreicher Sabo-

[148] Eigene inhaltliche Zusammenfassung, basierend auf einer OCR-gestützten Übersetzung der in Abbildung 3.4 dargestellten Screenshots aus dem Ukrainischen.
[149] Übernommen aus CyS Centrum (2016): Cyberbedrohung BlackEnergy2/3. Geschichte der Angriffe auf kritische IT-Infrastruktur der Ukraine, Fig. 10.
[150] Vgl. iTrust, SUTD (2016): *BlackEnergy - Malware for Cyber-Physical Attacks*, S. 8 f.
[151] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 19.
[152] Vgl. Geiger et al. (2020): *An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems*, S. 1538.
[153] Vgl. Geiger et al. (2020): *An Analysis of Black Energy 3, Crashoverride, and Trisis, Three Malware Approaches Targeting Operational Technology Systems*, S. 1538.
[154] Vgl. CISA (2016): *Cyber-Attack Against Ukrainian Critical Infrastructure – ICS Alert.*
[155] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 17.

tage wurden Passwörter geändert, Festplatten mithilfe von der Wiper-Malware KillDisk überschrieben und Firmware in Gateways beschädigt, um eine Systemwiederherstellung zu erschweren oder gar unmöglich zu machen.[156]

Begleitend zu diesem hochkoordinierten Angriff erfolgte ein DDoS-Angriff auf das Callcenter und die Webseite des Versorgers, um den Kundensupport zu stören und gleichzeitig Verwirrung zu stiften.[157] Zudem deaktivierten die Angreifer die unterbrechungsfreie Stromversorgung des Kontrollzentrums über das entsprechende Remote-Interface, sodass die Operatoren buchstäblich im Dunkeln versuchen mussten, den Vorfall zu bewältigen.[158]

3.4.2 Ukraine 2016 – Cyberangriff auf einen Übertragungsnetzbetreiber

Am 17. Dezember 2016 kam es gegen Mitternacht zu einem Cyberangriff auf die Pivnichna-Umspannwerk nördlich von Kiew, das zur nationalen Stromgesellschaft Ukrenergo gehört.[159] In der Folge kam es zu Stromausfällen in etwa einem Fünftel der Stadt Kiew sowie in angrenzenden Regionen.[160] Im Vergleich zum Cyberangriff von 2015 fiel der Ausfall mit rund einer Stunde deutlich kürzer aus.[161] Obwohl die unmittelbaren Auswirkungen begrenzt blieben, wurde die eingesetzte Malware von Experten wie ESET als eine hochgradig modulare und anpassbare Schadsoftware eingestuft.[162] Viele Elemente des Angriffs deuteten darauf hin, dass es sich eher um einen Machbarkeitsnachweis als um den gezielten Einsatz des vollen Potenzials der Malware handelte.[163]

Zwischen Januar und Oktober 2016 erfolgte der initiale Angriffsvektor durch eine Phishing-E-Mail, mit der sich die Angreifer Zugriff auf das Büronetzwerk verschafften.[164] Die beigefügte Schadsoftware war keine Variante von BlackEnergy, sondern eine frei verfügbare Open-Source-Backdoor.[165] Die Backdoor stellte eine verschlüsselte HTTPS-Verbindung zu einem Command and Control (C&C)-Server

[156] Vgl. Bock et al. (2017): *Ukrainian Power Grids Cyberattack.*
[157] Vgl. Rass et al. (2025): *Kritische Infrastrukturen*, S. 17.
[158] Vgl. CISA (2016): *Cyber-Attack Against Ukrainian Critical Infrastructure – ICS Alert.*
[159] Vgl. BBC News (2017): *Ukraine power cut 'was cyber-attack'.*
[160] Vgl. BBC News (2017): *Ukraine power cut 'was cyber-attack'.*
[161] Vgl. BBC News (2017): *Ukraine power cut 'was cyber-attack'.*
[162] Vgl. ESET (2022): *Industroyer: Eine Cyberwaffe, die einem Stromnetz den Stecker rauszog.*
[163] Vgl. Dragos (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations*, S. 11.
[164] Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 4 f.
[165] Vgl. Robert Lipovsky (2016): *New wave of cyberattacks against Ukrainian power industry.*

her, über die die Angreifer aus der Ferne Befehle auf dem infizierten System ausführen konnten.[166]

Um vom Büronetzwerk ins PCN zu pivotieren, nutzten die Angreifer ein System, das sowohl mit dem Büronetzwerk als auch mit dem PCN verbunden war und somit als Brücke zwischen beiden Netzen fungierte.[167] Bereits am 1. Dezember 2016 legten die Angreifer auf diesem System zwei neue Benutzerkonten mit den Namen „admin“ und „System“ an, statteten sie mit entsprechenden Rechten aus und banden sie in die lokale Domäne ein.[168]

Um sich innerhalb des PCN lateral zu bewegen, nutzten die Angreifer unter anderem Windows-Server mit installiertem SQL-Server, die aufgrund ihrer zentralen Einbindung in die Netzwerkinfrastruktur besonders geeignet dafür waren.[169] So kam es im Zeitraum vom 12. bis 15. Dezember 2016 zu intensiven Netzwerkaktivitäten im PCN.[170] Die ersten beobachteten Schritte umfassten Netzwerkerkundung, Verzeichnislistings, Namensauflösung und Authentifizierungsversuche per Remote Procedure Call.[171]

Nach der Ausbreitung im PCN wurde am 16. Dezember die modulare Malware Industroyer, auch bekannt als CrashOverride, im PCN verteilt.[172] Im Gegensatz zum Angriff von 2015, bei dem die Schaltvorgänge manuell über Remote-Zugriff ausgeführt wurden, erfolgte der Angriff 2016 vollständig automatisiert durch das entsprechende Launcher-Modul der Malware.[173]

Das Launcher-Modul hatte zwei Hauptaufgaben: Zum einen kontrollierte es die Ausführung der Payloads, zum anderen startete es etwa ein bis zwei Stunden nach deren Ausführung automatisch die Wiper-Malware KillDisk.[174] Die jeweiligen Payloads verfolgten grundsätzlich alle dasselbe Ziel: Sie steuerten die Leistungsschalter über verschiedene industrielle Kommunikationsprotokolle und lösten deren Öffnung im Umspannwerk aus.[175]

[166]Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 3.
[167]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 5.
[168]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 5.
[169]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 5.
[170]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 8.
[171]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 6 f.
[172]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 8.
[173]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 9.
[174]Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 5.
[175]Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 11-14.

Nach der Manipulation der Leistungsschalter kam die Wiper-Malware zum Einsatz, die relevante Dateien auf den Systemen löschte, um eine Wiederherstellung zu erschweren.[176] Zunächst wurden Registrierungsschlüssel, die für den Start und Betrieb der Systeme erforderlich sind, überschrieben.[177] Anschließend wurden die Laufwerke C: bis Z: durchsucht, um Windows-Binärdateien, Archive, Backup-Dateien, Microsoft SQL Server-Dateien sowie verschiedene Konfigurationsdateien zu überschreiben.[178] Abschließend wurden nahezu alle laufenden Prozesse beendet, wodurch das System abstürzte.[179]

Sämtliche Versuche der Umspannwerkbetreiber, die Kontrolle zurückzugewinnen, blieben erfolglos: Wurde ein Schalter aus der Ferne geschlossen, öffnete die Malware ihn unmittelbar wieder und das in einer Endlosschleife.[180] Diese Endlosschleifen-Manipulation führte dazu, dass die Betreiber vor Ort eingreifen mussten.[181] Um die Kontrolle über das Umspannwerk zurückzugewinnen, trennten die Operatoren des Umspannwerks die Kommunikationsverbindung zum betroffenen Netzwerk.[182] Diese Maßnahme setzte das Umspannwerk in den manuellen Betriebsmodus, was eine physische Präsenz vor Ort erforderlich machte.[183]

Begleitend zum eigentlichen Angriff mit Industroyer wurde ein DoS-Tool eingesetzt, das gezielt Schutzrelais in den Umspannwerken deaktivierte, indem es speziell formatierte UDP-Pakete an SIPROTEC-Geräten sendete.[184] Die Sicherheitslücke in den SIPROTEC-Schutzrelais ist unter der Referenz CVE-2015-5374 bekannt.[185]

Die betroffene Stromgesellschaft Ukrenergo hat nach dem Cyberangriff seine IT-Sicherheitsstrategie grundlegend überarbeitet.[186] So reagierte das Unternehmen 2017 mit einer Reform seiner IT-Infrastruktur und der Einrichtung eines Cyber Incident Response Centers.[187]

[176] Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 15 f.
[177] Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 15 f.
[178] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 14.
[179] Vgl. Slowik (2018): *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*, S. 16.
[180] Vgl. Dragos (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations*, S. 22 f.
[181] Vgl. Dragos (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations*, S. 22 f.
[182] Vgl. Dragos (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations*, S. 22 f.
[183] Vgl. Dragos (2017) *CrashOverride: Analysis of the Threat to Electric Grid Operations*, S. 22 f.
[184] Vgl. Cherepanov (2017): *WIN32/INDUSTROYER A new threat for industrial control systems*, S. 15.
[185] National Institute of Standards and Technology (NIST) (2015): *CVE-2015-5374: Denial-of-Service Vulnerability in Siemens SIPROTEC EN100 Ethernet Module.*
[186] Vgl. Ukrenergo (2018): *UKRENERGO-2017: results of the first reforms*, S. 11.
[187] Vgl. Ukrenergo (2018): *UKRENERGO-2017: results of the first reforms*, S. 11.

3.4.3 Ukraine 2022 – Cyberangriffe auf Hochspannungs-Umspannwerke

Am 8. April 2022 sollte nach aktuellem Kenntnisstand der bis dahin am größten angelegte Cyberangriff auf ein Stromnetz erfolgen, bei dem versucht wurde, mehrere Hochspannungs-Umspannwerke eines großen privaten ukrainischen Energieversorgers außer Betrieb zu setzen.[188] Wäre der Angriff erfolgreich gewesen, wären schätzungsweise zwei Millionen Menschen von Stromausfällen betroffen gewesen.[189] Dank frühzeitiger Warnungen und der engen internationalen Zusammenarbeit, insbesondere mit ESET, Microsoft und CERT-UA, konnte der Cyberangriff jedoch rechtzeitig abgewehrt werden.[190] Die Bevölkerung blieb von den Ereignissen unbeeinträchtigt, und es kam zu keinerlei Unterbrechung der Stromversorgung.[191]

Die eingesetzte Malware stellt eine Weiterentwicklung von Industroyer dar nämlich Industroyer2.[192] Wie bereits erwähnt, handelt es sich dabei um eine schlankere und gezielter eingesetzte Schadsoftware, die laut Angaben von ESET auf dem Quellcode der Payload-Komponente 104 von Industroyer basiert.[193]

Bei diesem Angriff ist bisher unbekannt, wie die Angreifer den Energieversorger initial kompromittiert haben und auf welchem Weg sie vom Büronetzwerk ins PCN pivotierten.[194] In den Konfigurationsdaten der Malware finden sich jedoch Anhaltspunkte dafür, dass der Angreifer bereits vor oder während des Einsatzes der Malware Informationen über das PCN erhoben hat.[195]

Der Angriff lässt sich in drei Phasen unterteilen: In der ersten Phase führten die Angreifer im Büronetzwerk auf mehreren Servern Wiper-Malware aus, die für verschiedene Betriebssysteme ausgelegt war.[196] Außerdem richteten sie eine geplante Aufgabe (Scheduled Task) ein, welche die zweite Phase des Angriffs automatisch initialisierte.[197]

Die Malware prüfte zunächst die Verbindung zu den entfernten Umspannstationen, etablierte anschließend Kommunikationskanäle, führte Statusabfragen (General

[188] Vgl. Tidy (2022): *Ukrainian power grid 'lucky' to withstand Russian cyber-attack.*
[189] Vgl. Tidy (2022): *Ukrainian power grid 'lucky' to withstand Russian cyber-attack.*
[190] Vgl. Tidy (2022): *Ukrainian power grid 'lucky' to withstand Russian cyber-attack.*
[191] Vgl. Tidy (2022): *Ukrainian power grid 'lucky' to withstand Russian cyber-attack.*
[192] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[193] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[194] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[195] Vgl. Zafra et al. (2022): *INDUSTROYER.V2: Old Malware Learns New Tricks.*
[196] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[197] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*

Interrogation) durch und übermittelte gezielte Steuerbefehle, mit denen Leistungsschalter in den Umspannstationen manipuliert werden konnten.[198]

In der dritten Phase führten die Angreifer erneut die Wiper-Malware CaddyWiper auf den Systemen im PCN aus, auf denen Industroyer2 zuvor aktiv gewesen war.[199] Verteilungsvektor von CaddyWiper war die Domänen-GPO: Über kompromittierte Richtlinien gelangte CaddyWiper ins Büronetz und PCN.[200] CaddyWiper löschte Benutzerdaten und Partitionsinformationen von angeschlossenen Laufwerken, wodurch die betroffenen Systeme unbrauchbar und nicht wiederherstellbar wurden.[201]

3.4.4 Dänemark 2023 – Cyberangriffe auf Energieinfrastruktur

> „*Denmark is constantly under attack. But it is unusual that we see so many concurrent, successful attacks against the critical infrastructure.*“[202]

Mit diesen Worten beschreibt SektorCERT, die außergewöhnliche Dimension des Cyberangriffs, der im Mai 2023 die dänische Energieinfrastruktur traf. SektorCERT ist eine gemeinnützige Organisation, die im Besitz dänischer Betreiber kritischer Infrastrukturen ist und von ihnen finanziert wird.[203] Eine der Hauptaufgaben der Organisation besteht darin, Cyberangriffe sektorenübergreifend zu erkennen und zu analysieren.[204] Um diese Aufgaben zu erfüllen, betreibt die Organisation ein eigenes Sensornetzwerk zur Analyse des Netzwerkverkehrs der Betreiber.[205] Im Mai 2023 bestand dieses Sensornetzwerk aus 270 Sensoren, die bei verschieden kritischen Einrichtungen in ganz Dänemark implementiert waren.[206]

Bereits 17 Tage vor den eigentlichen Cyberangriffen meldete der Firewall-Hersteller Zyxel eine kritische Sicherheitslücke in mehreren Firewall-Modellen.[207] Die Sicherheitslücke ist unter der Referenz CVE-2023-28771 bekannt.[208] Konkret handelt es

[198] Vgl. Zafra et al. (2022): *INDUSTROYER.V2: Old Malware Learns New Tricks.*
[199] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[200] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[201] Vgl. ESET Research (2022): *Industroyer2: Industroyer reloaded.*
[202] SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 3.
[203] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 3.
[204] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 3.
[205] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 3.
[206] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 6.
[207] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 6.
[208] National Institute of Standards and Technology (NIST) (2023): *CVE-2023-28771: OS Command Injection Vulnerability in Zyxel Firewall Series.*

sich um eine Schwachstelle bei der Fehlerbehandlung, durch die ein nicht authentifizierter Angreifer durch das Senden speziell präparierter Datenpakete Befehle auf dem Betriebssystem der Firewall ausführen kann.[209]

Die betroffenen Firewalls wurden unter anderem von zahlreichen Unternehmen im dänischen Energiesektor eingesetzt, um den Perimeter zum PCN sowie dessen Teilnetzwerke vor unautorisiertem Zugriff zu schützen.[210] Die Lage war äußerst kritisch, da sich die Sicherheitslücke genau in dem System befand, das eigentlich die industriellen Steuerungssysteme im PCN schützen sollte.[211] Bereits Anfang Mai warnte SektorCERT davor, diese Firewalls umgehend zu patchen, doch bei vielen Betroffenen war das Update aus verschiedenen Gründen nicht installiert worden.[212]

Insgesamt wurden im Zeitraum vom 11. bis zum 25. Mai 22 Unternehmen aus dem Energiesektor kompromittiert.[213] Es kam dabei zu zwei Angriffswellen: die erste am 11. Mai 2023 und die zweite am 22. Mai 2023.[214]

In der ersten Angriffswelle am 11. Mai versuchten die Angreifer, 16 Unternehmen gleichzeitig anzugreifen.[215] Hierzu sendeten sie speziell formatierte UDP-Datenpakete an den VPN-Dienst der Firewalls.[216] Bei 11 Unternehmen war der Angriff erfolgreich, während bei den übrigen 5 die Befehle nicht vollständig ausgeführt wurden.[217] Anschließend richteten die Angreifer auf den kompromittierten Systemen einen C&C-Server ein, über den weitere Befehle an die betroffenen Firewalls übermittelt wurden, um deren Konfiguration und Benutzerdaten auszulesen.[218] Obwohl SektorCERT keine Hinweise darauf fand, wie die Angreifer an Informationen über verwundbare Firewalls gelangten, wussten diese genau, welche nicht öffentlich gelisteten Unternehmen betroffen waren.[219]

Trotz guter Vorbereitung scheiterte die erste Angriffswelle.[220] Zwar gelang es den Angreifern, sich Zugang zu den Firewalls zu verschaffen und diese zu kontrollieren,

[209] National Institute of Standards and Technology (NIST) (2023): *CVE-2023-28771: OS Command Injection Vulnerability in Zyxel Firewall Series.*
[210] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 8.
[211] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 8.
[212] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 9.
[213] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 3.
[214] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 22.
[215] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 22.
[216] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 9.
[217] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 22.
[218] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 22.
[219] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 10.
[220] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 11.

doch bevor sie den Zugriff auf das PCN ausnutzen konnten, wurden sie entdeckt und gestoppt.[221]

In der zweiten Angriffswelle am 22. Mai nutzten die Angreifer bislang unbekannte Schwachstellen in Zyxel-Firewalls aus, noch bevor diese von Zyxel offiziell veröffentlicht wurden.[222] SektorCERT stellte fest, dass zwei Unternehmen nicht autorisierte Software für ihre Zyxel-Firewalls über eine unsichere Verbindung bezogen.[223] Die kompromittierten Firewalls wurden kurz darauf in ein Botnetz eingebunden und anschließend für DDoS-Angriffe gegen Ziele in Hongkong und den USA eingesetzt.[224] Am 23. Mai missbrauchten die Angreifer zudem die Firewall-Infrastruktur eines weiteren Unternehmens, um per Fernzugriff einen Brute-Force-Angriff auf ein kanadisches Unternehmen durchzuführen.[225]

Am 24. Mai veröffentlichte Zyxel zwei neue Sicherheitslücken in denselben Modellen, die bereits von der ersten Schwachstelle betroffen waren.[226] Die neuen Sicherheitslücken sind unter den Referenzen CVE-2023-33009[227] und CVE-2023-33010[228] bekannt. Kurz darauf, noch am selben Tag und am folgenden, wurden Firewalls bei sieben weiteren Unternehmen kompromittiert, und wie bei den vorherigen Angriffen wurden die Firewalls anschließend für zusätzliche DDoS-Angriffe genutzt.[229] Die betroffenen Unternehmen der zweiten Angriffswelle konnten jedoch die Angriffe in Zusammenarbeit mit SektorCERT eindämmen, indem sie noch am selben Tag auf dessen Anforderung in den „Inselbetrieb“ wechselten und den gesamten Internetverkehr blockierten.[230]

Am späten Morgen des 25. Mai verschärfte sich die Lage erheblich: Kurz vor Mittag kontaktierte ein weiteres Unternehmen SektorCERT und meldete den Ausfall der Firewall sowie den Verlust der Verbindung zu drei entfernten Standorten.[231] Da die Firewall gleichzeitig als interner Router im PCN fungierte, wurde der gesamte

[221] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 11.
[222] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 11.
[223] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 22 f.
[224] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 23.
[225] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 13.
[226] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 23.
[227] National Institute of Standards and Technology (NIST) (2023): *CVE-2023-33009: Buffer Overflow in Notification Function of Zyxel Firewall Series Allowing Unauthenticated Denial-of-Service and Remote Code Execution.*
[228] National Institute of Standards and Technology (NIST) (2023): *CVE-2023-33010: Buffer Overflow in ID Processing Function of Zyxel Firewall Series Leading to DoS and Remote Code Execution.*
[229] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 23-25.
[230] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 23.
[231] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 25.

interne Datenverkehr des betroffenen Unternehmens unterbrochen.[232] Durch eine genauere Analyse des Netzwerkverkehrs des betroffenen Unternehmen konnte SektorCERT IP Adressen identifizieren, die vermutlich mit der Sandworm Gruppe in Verbindung stehen.[233] Diese Gruppe steht laut zahlreichen Berichten auch hinter den Cyberangriffen auf die Stromversorgung in der Ukraine in den Jahren 2015 und 2016.[234] Daraufhin nahm SektorCERT Kontakt mit dem Nationalen Zentrum für Cyberkriminalität (NC3) sowie dem Center for Cyber Security auf.[235] Aufgrund der Schwere des Angriffs wurde mit dem betroffen Unternehmen vereinbart, dass alle Verbindungen zum Internet sofort getrennt werden.[236] Die Firewall blieb jedoch weiterhin in Betrieb, um sicherzustellen, dass eventuell im Arbeitsspeicher befindliche Schadsoftware beim Ausschalten nicht gelöscht wird.[237] In den darauffolgenden Tagen analysierten die Experten des NC3 die von SektorCERT gesicherte Malware, um die Angriffsmethoden zu untersuchen und die gewonnenen Erkenntnisse für zukünftige Sicherheitsmaßnahmen zu nutzen.[238] Das betroffene Unternehmen reagierte mit der Bestellung einer neuen Firewall und arbeitete sechs Tage lang im „Inselbetrieb“.[239]

Dank der hervorragenden Zusammenarbeit zwischen SektorCERT, den betroffenen Unternehmen, deren Zulieferern sowie der Polizeiabteilung NC3 blieb die dänische Bevölkerung von den Cyberangriffen unberührt.[240] Es kam zu keiner Beeinträchtigung der Versorgungssicherheit, sodass die Bevölkerung nichts von den Angriffen mitbekam.[241]

[232] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 15.
[233] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 14 f.
[234] Vgl. U.S. Department of Justice (2020): *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware*.
[235] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 15.
[236] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 15.
[237] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 15.
[238] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 16.
[239] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 15.
[240] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 18.
[241] Vgl. SektorCERT (2023): *The Attack Against Danish Critical Infrastructure*, S. 18.

KAPITEL 4

Rechtliche Rahmenbedingungen der EU

In diesem Kapitel wird ein Überblick gegeben, wie die Europäische Union mit verschiedenen Rechtsakten auf die wachsenden Cyberbedrohungen im Bereich der Stromversorgung reagiert hat.

Den Ausgangspunkt bildet die NIS1-Richtlinie, mit der erstmals ein unionsweiter Rechtsrahmen für die Cybersicherheit geschaffen wurde. Sie legte dabei erstmals sehr allgemeine Sicherheitsanforderungen und Meldepflichten für Betreiber wesentlicher Dienste fest (siehe Abschnitt 4.1). Am 27. Dezember 2022 wurde NIS1 durch die NIS2-Richtlinie abgelöst. NIS2 baut auf der Vorgängerrichtlinie auf, weitet den Anwendungsbereich erheblich aus und verschärft die Anforderungen an Cybersicherheitsmaßnahmen (siehe Abschnitt 4.2). Zeitgleich dazu wurde die Richtlinie (EU) 2022/2557 (CER)[242] verabschiedet, die auf die Stärkung der physischen und organisatorischen Resilienz kritischer Einrichtungen abzielt, darunter auch Einrichtungsarten der Stromversorgung.[243] Mit der delegierten Verordnung (EU) 2024/1366 (NCCS)[244] wurden schließlich erstmals sektorspezifische Vorgaben für den Elektrizitätssektor eingeführt (siehe Abschnitt 4.3). Eine zeitliche Übersicht bietet Abbildung 4.1.

[242] Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen, ABl. L 333 vom 27.12.2022, S. 164.

[243] Vgl. Art. 6 und Anhang der RL (EU) 2022/2557.

[244] Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 durch sektorspezifische Cybersicherheitsaspekte grenzüberschreitender Stromflüsse, ABl. L 141 vom 24.5.2024, S. 1.

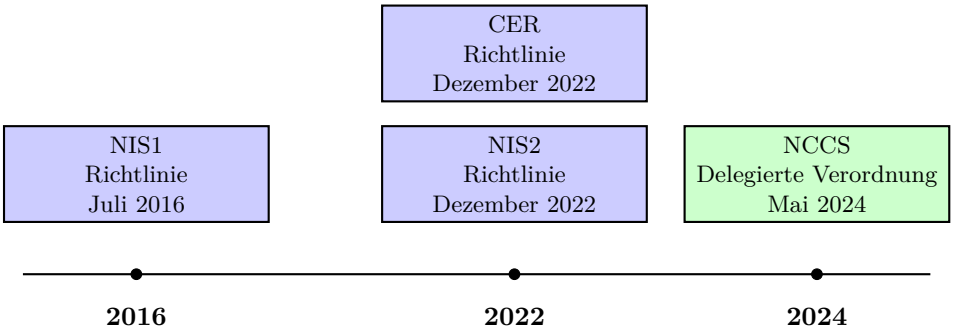

Abbildung 4.1: Zeitliche Übersicht der wichtigsten EU-Rechtsakte zur Cybersicherheit in der Stromversorgung[245]

Um den Rahmen dieser Arbeit einzugrenzen, konzentriert sich dieses Kapitel ausschließlich auf die NIS1-Richtlinie, die darauf aufbauende NIS2-Richtlinie sowie die delegierte Verordnung NCCS. Dabei werden nicht alle darin enthaltenen Maßnahmen behandelt, sondern insbesondere die präventiven Sicherheitsanforderungen und die reaktiven Meldepflichten auf Einrichtungsebene. Zudem wird die Rolle der Computer Security Incident Response Teams (CSIRTs) näher beleuchtet, da ihre Aufgaben eng mit den Meldepflichten im Rahmen dieser Rechtsakte verknüpft sind.

[245] Eigene Darstellung.

4.1 Richtlinie (EU) 2016/1148

Die NIS1-Richtlinie wurde am 6. Juli 2016 im Amtsblatt der Europäischen Union veröffentlicht. Die Richtlinie ist ein Rechtsakt, der die Mitgliedstaaten an das zu erreichende Ziel bindet, ihnen aber die Wahl der Mittel zur Umsetzung überlässt.[246] Die Mitgliedstaaten waren verpflichtet, die Bestimmungen der Richtlinie bis spätestens 9. Mai 2018 in nationales Recht umzusetzen.[247]

4.1.1 Anwendungsbereich

Der Anwendungsbereich der NIS1-Richtlinie beschränkte sich nicht nur auf Einrichtungen der Stromversorgung, sondern umfasste eine Vielzahl kritischer Sektoren, darunter die Bereiche Gesundheit, Verkehr, Wasserversorgung und Finanzwesen, sowie Betreiber digitaler Dienste wie Online-Marktplätze, Cloud-Computing-Dienste und Suchmaschinen.[248] Im Bereich der Stromversorgung sind nach der NIS1-Richtlinie insbesondere folgende Betreiber wesentlicher Diensten betroffen:[249]

- Elektrizitätsunternehmen,[250] die die Funktion der Versorgung[251] erfüllen
- Verteilernetzbetreiber
- Übertragungsnetzbetreiber

Nicht alle der aufgezählten Betreiber sind Betreiber wesentliche Dienste, sondern nur solche, deren Dienste für kritische Tätigkeiten unverzichtbar sind, von Netz- und Informationssysteme abhängen und bei denen ein Sicherheitsvorfall erhebliche Störungen verursachen würde.[252]

4.1.2 Sicherheitsanforderungen und Meldung von Sicherheitsvorfällen

In Artikel 14 der NIS1-Richtlinie sind die präventiven Sicherheitsanforderungen für Betreiber wesentlicher Dienste festgelegt. Diese Vorgaben sind bewusst allgemein und technologieoffen gehalten, enthalten jedoch keine detaillierten technischen oder

[246] Vgl. Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), ABl. C 202 vom 7.6.2016, S. 1.
[247] Vgl. Art. 27 Abs. 1 der RL (EU) 2016/1148.
[248] Vgl. Anhang II und III der RL (EU) 2016/1148.
[249] Vgl. Anhang II der RL (EU) 2016/1148.
[250] Vgl. Art. 2 Nr. 35 der RL (EU) 2009/72/EG.
[251] Vgl. Art. 2 Nr. 19 der RL (EU) 2009/72/EG.
[252] Vgl. Art. 5 Abs. 2 RL (EU) 2016/1148.

organisatorischen Vorgaben. Dabei enthält Absatz 1 Anforderungen an präventive Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus:

> *„Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete und verhältnismäßige technische und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die sie für ihre Tätigkeiten nutzen, zu bewältigen. Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist.“*[253]

Absatz 2 ergänzt diese Vorgaben um Maßnahmen, die darauf abzielen, im Falle eingetretener Sicherheitsvorfälle deren Auswirkungen zu minimieren und die Verfügbarkeit der Dienste sicherzustellen:

> *„Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste geeignete Maßnahmen ergreifen, um den Auswirkungen von Sicherheitsvorfällen, die die Sicherheit der von ihnen für die Bereitstellung dieser wesentlichen Dienste genutzten Netz- und Informationssysteme beeinträchtigen, vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird.“*[254]

Zusätzlich zu den Sicherheitsanforderungen verpflichtet Artikel 14 der NIS1-Richtlinie die Mitgliedstaaten, sicherzustellen, dass Betreiber wesentlicher Dienste erhebliche Sicherheitsvorfälle melden:

> *„Die Mitgliedstaaten stellen sicher, dass die Betreiber wesentlicher Dienste der zuständigen Behörde oder dem CSIRT Sicherheitsvorfälle, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen bereitgestellten wesentlichen Dienste haben, unverzüglich melden. Die Meldungen müssen die Informationen enthalten, die es der zuständigen Behörde oder dem CSIRT ermöglichen, zu bestimmen, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat.[...]“*[255]

[253] Siehe. Art. 14 Abs. 1 der RL (EU) 2016/1148.
[254] Siehe. Art. 14 Abs. 2 der RL (EU) 2016/1148.
[255] Siehe. Art. 14 Abs. 3 der RL (EU) 2016/1148.

Zur Bewertung ob ein Sicherheitsvorfall erhebliche Auswirkungen hat sollen insbesondere folgende Parameter berücksichtigt werden: die Anzahl der betroffenen Nutzer, die Dauer des Vorfalls sowie die geografische Ausbreitung im betroffenen Gebiet.[256]

4.1.3 Computer Security Incident Response Teams

Mit der NIS1-Richtlinie wurde erstmals auf europäischer Ebene die Verpflichtung eingeführt, mindestens ein CSIRTs für Betreiber wesentlicher Dienste auf nationaler Ebene einzurichten.[257]

Die Anforderungen an CSIRTs umfassen sowohl organisatorische als auch technische Aspekte.[258] Zunächst müssen CSIRTs eine hohe Verfügbarkeit ihrer Kommunikationsdienste sicherstellen.[259] Ein weiterer Schwerpunkt liegt auf der Betriebskontinuität, die CSIRTs durch effiziente Anfragenverwaltung, ständige Verfügbarkeit und redundante Infrastrukturen sicherstellen müssen.[260] Schließlich sollen CSIRTs die Möglichkeit haben, sich in internationale Kooperationsnetze einzubringen, um Informationen und Erfahrungen grenzüberschreitend auszutauschen.[261] Durch die NIS-Richtlinie wurde dafür ein CSIRTs-Netzwerk eingeführt.[262]

Die Aufgaben der CSIRTs umfassen dabei die Überwachung und Analyse von Sicherheitsvorfällen auf nationaler Ebene sowie die Reaktion auf solche Vorfälle.[263] Dazu gehört die Ausgabe von Frühwarnungen und Alarmmeldungen sowie die Bekanntmachung und Verbreitung relevanter Informationen an die einschlägigen Interessenträger.[264] Ferner führen CSIRTs eine dynamische Analyse von Risiken und Vorfällen durch und erstellen eine Lagebeurteilung.[265]

4.2 Richtlinie (EU) 2022/2555

Die NIS2-Richtlinie wurde am 27. Dezember 2022 im Amtsblatt der Europäischen Union veröffentlicht. Sie stellt ebenfalls wie ihr Vorgänger einen Rechtsakt in Form

[256] Vgl. Art. 14 Abs. 4 Lit. a–c der RL (EU) 2016/1148.
[257] Vgl. Art. 9 und Anhang I der RL (EU) 2016/1148.
[258] Vgl. Abs. 1 Anhang I der RL (EU) 2016/1148.
[259] Vgl. Abs. 1 Lit. a Anhang I der RL (EU) 2016/1148.
[260] Vgl. Abs. 1 Lit. c Anhang I der RL (EU) 2016/1148.
[261] Vgl. Abs. 1 Lit. d Anhang I der RL (EU) 2016/1148.
[262] Vgl. Art. 1 Abs. 2 Lit. c der RL (EU) 2016/1148; Abs. 2 Lit. a v Anhang I der RL (EU) 2016/1148.
[263] Vgl. Abs. 2 Lit. a i, iii Anhang I der RL (EU) 2016/1148.
[264] Vgl. Abs. 2 Lit. a ii Anhang I der RL (EU) 2016/1148.
[265] Vgl. Abs. 2 Lit. a iv Anhang I der RL (EU) 2016/1148.

einer Richtlinie dar (siehe Abschnitt 4.1). Die Mitgliedstaaten waren verpflichtet, die Bestimmungen der Richtlinie bis spätestens 17. Oktober 2024 in nationales Recht umzusetzen.[266]

4.2.1 Anwendungsbereich

Der Anwendungsbereich der NIS2-Richtlinie beschränkt sich wie bereits bei der Vorgängerrichtlinie nicht auf Einrichtungen der Stromversorgung, sondern erstreckt sich auf insgesamt 18 Sektoren.[267] Im Bereich Stromversorgung übernimmt die NIS2-Richtlinie die bereits in der NIS1-Richtlinie erfassten Einrichtungen und führt diese fort (siehe Abschnitt 4.1.1). Darüber hinaus wurde der Geltungsbereich erweitert, indem weitere Einrichtungsarten aufgenommen wurden. Dazu zählen insbesondere folgende Betreiber wesentlicher Dienste:

- Von der zuständigen Behörde benannte Strombörsen (NEMOs), die den europaweiten Stromhandel organisieren.[268]
- Markteilnehmer, die die Nachfrage oder Erzeugung mehrerer Kunden bündeln, um diese gemeinsam am Strommarkt zu handeln. [269]
- Marktteilnehmer, die den Stromverbrauch von Endkunden steuern um Angebot und Nachfrage auszugleichen.[270]
- Marktteilnehmer, die elektrische Energie speichern, um sie zu einem späteren Zeitpunkt wieder ins Netz einzuspeisen oder in andere Energieformen umzuwandeln.[271]
- Betreiber, die für die Organisation und den Betrieb von Ladepunkten verantwortlich sind und dem Endkunden das Aufladen ermöglichen, auch im Auftrag von Mobilitätsdienstleistern.[272]

[266] Vgl. Art. 41 Abs. 1 der RL (EU) 2022/2555.
[267] Vgl. Anhang I und Anhang II der RL (EU) 2022/2555.
[268] Vgl. Art. 2 Nr. 8 der VO (EU) 2019/943.
[269] Vgl. Art. 2 Nr. 18 der RL (EU) 2019/944.
[270] Vgl. Art. 2 Nr. 20 der RL (EU) 2019/944.
[271] Vgl. Art. 2 Nr. 59 der RL (EU) 2019/944.
[272] Vgl. Anhang I der RL (EU) 2022/2555.

Ein zentrales Element der NIS2-Richtlinie ist die Einteilung der betroffenen Einrichtungen in zwei Kategorien: wesentliche Einrichtungen und wichtige Einrichtungen.[273]

Wesentliche Einrichtungen sind solche, die die Schwellenwerte für kleine und mittlere Unternehmen (KMU) überschreiten.[274] Die Einstufung als KMU richtet sich nach der Empfehlung 2003/361/EG, wonach ein Unternehmen mit weniger als 250 Beschäftigten sowie einem Jahresumsatz von höchstens 50 Mio. EUR oder einer Bilanzsumme von höchstens 43 Mio. EUR als KMU gilt.[275]

Allerdings sieht die Richtlinie ausdrücklich vor, dass auch Einrichtungen unabhängig von ihrer Größe als wesentliche Einrichtungen eingestuft werden können, sofern sie aufgrund ihrer nationalen oder sektorspezifischen Bedeutung als kritisch gelten.[276] Dies betrifft etwa Einrichtungen, die:

- als alleiniger Anbieter eines für die Aufrechterhaltung zentraler gesellschaftlicher oder wirtschaftlicher Tätigkeiten notwendigen Dienstes fungieren,[277]
- deren Störung ein erhebliches Systemrisiko birgt, insbesondere mit möglichen grenzüberschreitenden Auswirkungen,[278]
- oder die aufgrund ihrer besonderen Bedeutung auf nationaler oder regionaler Ebene als kritisch eingestuft werden.[279]

Wichtige Einrichtungen sind Organisationen, die nicht alle Voraussetzungen für die Einstufung als wesentliche Einrichtung erfüllen, etwa aufgrund ihrer geringeren Größe oder geringeren Kritikalität.[280] Auch wenn diese Organisationen nicht als wesentliche Einrichtungen gelten, sind sie dennoch verpflichtet, für ein angemessenes Schutzniveau ihrer Netz und Informationssysteme zu sorgen, unterliegen dabei jedoch einer weniger strengen behördlichen Kontrollen.[281]

[273] Vgl. Art. 3 Abs. 2 und Abs. 3 der RL (EU) 2022/2555.
[274] Vgl. Art. 3 Abs. 1 lit. a der RL (EU) 2022/2555.
[275] Vgl. Art. 2 Abs. 1 der Empfehlung 2003/361/EG.
[276] Vgl. Art. 2 Abs. 2 der RL (EU) 2022/2555.
[277] Vgl. Art. 2 Abs. 2 Lit. b der RL (EU) 2022/2555.
[278] Vgl. Art. 2 Abs. 2 Lit. d der RL (EU) 2022/2555.
[279] Vgl. Art. 2 Abs. 2 Lit. e der RL (EU) 2022/2555.
[280] Vgl. Art. 3 Abs. 2 der RL 2022/2555.
[281] Vgl. Art. 32 und Art. 33 der RL (EU) 2022/2555.

Damit erstreckt sich der Anwendungsbereich der NIS2-Richtlinie deutlich weiter als jener der NIS1-Richtlinie und bezieht eine größere Anzahl an stromversorgungsrelevanten Einrichtungen ein. Zur Umsetzung dieser Einstufung sind die Mitgliedstaaten verpflichtet, bis zum 17. April 2025 eine Liste der wesentlichen und wichtigen Einrichtungen zu erstellen.[282] Diese Liste ist anschließend regelmäßig, alle zwei Jahre, zu überprüfen und bei Bedarf zu aktualisieren.[283]

4.2.2 Sicherheitsanforderungen

In Artikel 21 der NIS2-Richtlinie sind die Sicherheitsanforderungen für Betreiber wesentlicher und wichtiger Einrichtungen geregelt. Wie bereits in der NIS1-Richtlinie wird darin erwähnt, dass Einrichtungen geeignete technische und organisatorische Maßnahmen ergreifen müssen um die Auswirkungen der Sicherheitsvorfälle zu verhindern oder so gering wie möglich zu halten:

> *Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.*[284]

Diese Maßnahmen müssen wie bereits bei der NIS1-Richtlinie verhältnismäßig sein und sich am Stand der Technik, der Größe der Einrichtung, den Umsetzungskosten sowie der Eintrittswahrscheinlichkeit und Schwere potenzieller Vorfälle orientieren.[285] Neu in der NIS2-Richtlinie ist, dass bei der Auswahl der Maßnahmen ausdrücklich europäische und internationale Normen und Standards berücksichtigt werden sollen, sofern solche existieren.[286] Ebenfalls eingeführt wurde der sogenannte „gefahrenübergreifende Ansatz“, der nicht nur die Netz- und Informationssysteme, sondern auch deren physische Umgebung in den Schutz einbezieht.[287]

[282] Vgl. Art. 3 Abs. 3 der RL (EU) 2022/2555.
[283] Vgl. Art. 3 Abs. 5 der RL (EU) 2022/2555.
[284] Siehe Art. 21 Abs. 1 der RL (EU) 2022/2555.
[285] Vgl. Art. 21 Abs. 1 der RL (EU) 2022/2555.
[286] Vgl. Art. 21 Abs. 1 RL (EU) 2022/2555.
[287] Vgl. Art. 21 Abs. 2 RL (EU) 2022/2555.

Ein weiterer bedeutender Unterschied zur NIS1-Richtlinie besteht darin, dass die NIS2-Richtlinie erstmals verbindliche Mindestanforderungen für diese Maßnahmen festlegt.[288] Dabei sind mindestens die folgenden zehn Handlungsbereiche abzudecken:

- *„Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;“*[289]
- *„Bewältigung von Sicherheitsvorfällen;“* [290]
- *„Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;“* [291]
- *„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;“* [292]
- *„Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;“*[293]
- *„Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;“* [294]
- *„Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;“* [295]
- *„Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;“* [296]
- *„Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;“* [297]

[288] Vgl. Art. 21 Abs. 1 der RL (EU) 2022/2555; Art. 14 der RL (EU) 2016/1148.
[289] Siehe Art. 21 Abs. 2 Lit. a der RL (EU) 2022/2555.
[290] Siehe Art. 21 Abs. 2 Lit. b der RL (EU) 2022/2555.
[291] Siehe Art. 21 Abs. 2 Lit. c der RL (EU) 2022/2555.
[292] Siehe Art. 21 Abs. 2 Lit. d der RL (EU) 2022/2555.
[293] Siehe Art. 21 Abs. 2 Lit. e der RL (EU) 2022/2555.
[294] Siehe Art. 21 Abs. 2 Lit. f der RL (EU) 2022/2555.
[295] Siehe Art. 21 Abs. 2 Lit. g der RL (EU) 2022/2555.
[296] Siehe Art. 21 Abs. 2 Lit. h der RL (EU) 2022/2555.
[297] Siehe Art. 21 Abs. 2 Lit. i der RL (EU) 2022/2555.

- *„Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.“* [298]

Zusätzlich hebt die Richtlinie die besondere Bedeutung der Lieferkettensicherheit hervor. Einrichtungen müssen bei Sicherheitsmaßnahmen nicht nur auf ihre Anbieter und Dienstleister achten, sondern auch deren Schwachstellen, die Qualität ihrer Produkte und ihre Cybersicherheitsstandards prüfen.[299] Auch die Ergebnisse von Risikobewertungen auf europäischer Ebene zur Sicherheit kritischer Lieferketten sind dabei zu berücksichtigen.[300]

Ein weiterer wesentlicher Unterschied besteht darin, dass die NIS2-Richtlinie die Leitungsorgane der Einrichtungen verpflichtet, die ergriffenen Sicherheitsanforderungen formell zu genehmigen, deren Umsetzung aktiv zu überwachen und im Falle von Verstößen persönlich zur Verantwortung gezogen zu werden.[301]

4.2.3 Meldung von Sicherheitsvorfällen

Die NIS2-Richtlinie legt verbindliche Meldepflichten für wesentliche und wichtige Einrichtungen gemäß Artikel 23 fest. Ein meldepflichtiger Vorfall liegt vor, wenn es sich um einen erheblichen Sicherheitsvorfall handelt.[302] Ein Sicherheitsvorfall gilt als erheblich, wenn mindestens eines der folgenden Kriterien erfüllt ist:

- *„er schwerwiegende Betriebsstörungen der erbrachten Dienste oder erhebliche finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann“*[303]
- *„er bei anderen natürlichen oder juristischen Personen erhebliche materielle oder immaterielle Schäden bewirkt hat oder bewirken kann“*[304]

Welche konkrete Stelle im Mitgliedstaat im Meldefall zu benachrichtigen ist, hängt von der jeweiligen nationalen Umsetzung der Richtlinie ab. Ein Mitgliedstaat kann

[298] Siehe Art. 21 Abs. 2 Lit. j der RL (EU) 2022/2555.
[299] Vgl. Art. 21 Abs. 3 der RL (EU) 2022/2555.
[300] Vgl. Art. 21 Abs. 3 i.V.m Art. 22 Abs. 1 der RL (EU) 2022/2555.
[301] Vgl. Art. 20 Abs. 1 der RL (EU) 2022/2555.
[302] Vgl. Art. 23 Abs. 1 der RL (EU) 2022/2555.
[303] Siehe Art. 23 Abs. 3 Lit. a der RL (EU) 2022/2555.
[304] Siehe Art. 23 Abs. 3 Lit. b der RL (EU) 2022/2555.

vorsehen, dass Sicherheitsvorfälle entweder der zuständigen nationalen Behörde oder dem jeweils zuständigen CSIRT gemeldet werden.[305] Entscheidet sich ein Mitgliedstaat dafür, die Meldepflicht bei der nationalen Behörde zu verankern, so ist diese verpflichtet, eingehende Meldungen unverzüglich an das zuständige CSIRT weiterzuleiten.[306] Wenn ein öffentliches Interesse besteht, kann die zuständige Behörde entweder selbst die Öffentlichkeit über den Sicherheitsvorfall informieren oder die betroffene Einrichtung auffordern, dies zu tun.[307]

Unabhängig davon, welche Stelle im jeweiligen Mitgliedstaat zuständig ist, unterliegen wesentliche und wichtige Einrichtungen im Gegensatz zur NIS1-Richtlinie genaueren Fristen und genaueren inhaltlichen Vorgaben (siehe Tabelle 4.1).

Zeitpunkt	**Inhalt der Meldung**
Frühmeldung (innerhalb von 24 Stunden)	Angabe, ob der Vorfall möglicherweise rechtswidrig/böswillig ist oder grenzüberschreitende Auswirkungen haben könnte.[308]
Meldung des Sicherheitsvorfalls (innerhalb von 72 Stunden)	Erste Bewertung des Schweregrads, der Auswirkungen und ggf. Kompromittierungsindikatoren.[309]
Zwischenbericht (auf Anforderung)	Statusupdates und relevante Informationen zum Vorfall.[310]
Abschlussbericht (spätestens 1 Monat nach der Meldung)	Vollständige Analyse, Ursachen, ergriffene Maßnahmen und grenzüberschreitende Auswirkungen.[311]

Tabelle 4.1: Meldepflichten und Fristen für erhebliche Sicherheitsvorfälle gemäß der RL (EU) 2022/2555

Sofern zum Zeitpunkt der Einreichung des Abschlussberichts ein Sicherheitsvorfall noch andauert, ist anstelle des Abschlussberichts ein Fortschrittsbericht vorzulegen, der den aktuellen Stand der Ermittlungen und ergriffenen Maßnahmen dokumen-

[305] Vgl. Art. 23 Abs. 1 der RL (EU) 2022/2555.
[306] Vgl. Art. 23 der RL (EU) 2022/2555.
[307] Vgl. Art. 23 Abs. 7 Lit. e der RL (EU) 2022/2555.
[308] Vgl. Art. 23 Abs. 4 Lit. a der RL (EU) 2022/2555.
[309] Vgl. Art. 23 Abs. 4 Lit. b der RL (EU) 2022/2555.
[310] Vgl. Art. 23 Abs. 4 Lit. c der RL (EU) 2022/2555.
[311] Vgl. Art. 23 Abs. 4 Lit. d der RL (EU) 2022/2555.

tiert.[312] Der endgültige Abschlussbericht kann in solchen Fällen innerhalb eines Monats nach Behebung des Vorfalls nachgereicht werden.[313] Voraussetzung dafür ist jedoch, dass der Fortschrittsbericht rechtzeitig eingereicht wurde.[314]

4.2.4 Sanktionen

Bei Verstößen gegen Artikel 21 oder Artikel 23 werden Geldbußen verhängt, abhängig davon, ob es sich um eine wichtige oder wesentliche Einrichtung handelt.[315] Der Mindesthöchstbetrag bemisst sich jeweils an dem höheren Wert von zwei möglichen Beträgen: dem festgelegten Mindestbetrag oder einem prozentualen Anteil am weltweiten Jahresumsatz des vorangegangenen Geschäftsjahres der betroffenen Einrichtung (siehe Tabelle 4.2).[316]

Einrichtungstyp	**Höhe der Geldbuße (Höchstbetrag)**
Wichtige Einrichtung	Mindestens 7 Millionen Euro oder 1,4 % des weltweiten Umsatzes.[317]
Wesentliche Einrichtung	Mindestens 10 Millionen Euro oder 2 % des weltweiten Umsatzes.[318]

Tabelle 4.2: Höhe der Geldbußen bei Verstößen gegen die Berichtspflichten gemäß der RL (EU) 2022/2555

4.3 Delegierte Verordnung (EU) 2024/1366

Die Delegierte Verordnung (EU) 2024/1366 wurde am 24. Mai 2024 im Amtsblatt der Europäischen Union veröffentlicht und ergänzt die Verordnung (EU) 2019/943 über den Elektrizitätsbinnenmarkt durch spezifische Vorschriften an die Cybersicherheit bei grenzüberschreitenden Stromflüssen. Sie ist ein delegierter Rechtsakt[319] in Form

[312] Vgl. Art. 23 Abs. 4 Lit. e der RL (EU) 2022/2555.
[313] Vgl. Art. 23 Abs. 4 Lit. e der RL (EU) 2022/2555.
[314] Vgl. Art. 23 Abs. 4 Lit. e der RL (EU) 2022/2555.
[315] Vgl. Art. 34 Abs. 4 und 5 der RL (EU) 2022/2555.
[316] Vgl. Art. 34 Abs. 4 und 5 der RL (EU) 2022/2555.
[317] Vgl. Art. 34 Abs. 5 der RL (EU) 2022/2555.
[318] Vgl. Art. 34 Abs. 4 der RL (EU) 2022/2555.
[319] Vgl. Art. 290 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), ABl. C 202 vom 7.6.2016, S. 1.

einer Verordnung, die für alle Mitgliedstaaten verbindlich ist und unmittelbar gilt.[320]

Die Verordnung zielt darauf ab, ein hohes und einheitliches Cybersicherheitsniveau im Elektrizitätssektor zu gewährleisten.[321] Damit ergänzt sie die horizontal geltende NIS2-Richtlinie, indem sie sektorspezifische Anforderungen für Einrichtungen mit erheblichen oder kritischen Auswirkungen bei grenzüberschreitenden Stromflüssen festlegt.[322] Dazu gehören Vorschriften zu gemeinsamen Mindestanforderungen, Planung, Überwachung, Berichterstattung und Krisenbewältigung. [323]

4.3.1 Anwendungsbereich

Die Agenturen ACER und ENISA sowie der Übertragungsnetzbetreiberverband ENTSO-E und der Verteilungssnetzbetreiberverband EU-VNBO übernehmen koordinierende Aufgaben bei der Entwicklung und Abstimmung von Cybersicherheitsmaßnahmen und begleiten deren Umsetzung in den Mitgliedstaaten.[324] So erstellt ENTSO-E zusammen mit der EU-VNBO alle drei Jahre einen Bericht über die unionsweite Bewertung des Cybersicherheitsrisikos.[325] Der Bericht analysiert die Folgen von Cyberangriffen auf grenzüberschreitende Stromflüsse, ohne rechtliche, finanzielle oder rufschädigende Folgen zu berücksichtigen.[326]

Ein zentrales Element des Berichts ist der *„Index für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor“* (ECII). Dieser Indikator dient dazu, die potenziellen Folgen von Cyberangriffen auf grenzüberschreitende Stromflüsse zu quantifizieren.[327] Zusammen mit den im Bericht definierten ECII-Schwellenwerten bildet der ECII die Grundlage, um Einrichtungen mit erheblichen oder kritischen Auswirkungen auf grenzüberschreitende Stromflüsse zu identifizieren.[328]

Die Verordnung definiert Einrichtungen mit kritischen und erheblichen Auswirkungen in den Begriffsbestimmungen wie folgt:

[320] Vgl. Art. 288 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), ABl. C 202 vom 7.6.2016, S. 1.
[321] Vgl. Erwägungsgründe 1, 2 und 4 der VO (EU) 2024/1366.
[322] Vgl. ErwGr. 3 und 7 sowie Art. 2 Abs. 1 i.V.m. Art. 24 der VO (EU) 2024/1366 i.V.m. Art. 3 der RL (EU) 2022/2555.
[323] Vgl. Art. 1 der VO (EU) 2024/1366.
[324] Vgl. Art. 6–8 sowie ErwGr. 27 der VO (EU) 2024/1366.
[325] Vgl. Art. 19 Abs. 1 der VO (EU) 2024/1366.
[326] Vgl. Art. 19 Abs. 1 der VO (EU) 2024/1366.
[327] Vgl. Art. 3 Nr. 21 der VO (EU) 2024/1366.
[328] Vgl. Art. 19 Abs. 3 lit. b i.V.m. Art. 24 Abs. 1 (EU) der VO 2024/1366.

> *„Einrichtung mit kritischen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit kritischen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 bestimmt wird.* [329]
>
> *„Prozess mit kritischen Auswirkungen“ bezeichnet einen Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen auf die Cybersicherheit im Elektrizitätssektor über dem Schwellenwert für kritische Auswirkungen liegen.* [330]
>
> *„Einrichtung mit erheblichen Auswirkungen“ bezeichnet eine Einrichtung, die einen Prozess mit erheblichen Auswirkungen durchführt und von den zuständigen Behörden gemäß Artikel 24 ermittelt wird.* [331]
>
> *„Prozess mit erheblichen Auswirkungen“ bezeichnet jeden Geschäftsprozess einer Einrichtung, dessen Indizes für die Auswirkungen von Cybersicherheitsvorfällen im Elektrizitätssektor über den Schwellenwerten für erhebliche Auswirkungen liegen.* [332]

Zusätzlich können auch Gruppen von Einrichtungen als kritisch oder erheblich eingestuft werden, wenn für diese ein erhebliches Risiko besteht, zeitgleich Ziel eines Cyberangriffs zu sein, und ihr aggregierter ECII-Wert die Schwellenwerte überschreitet.[333] In diesen Fällen gelten die Prozesse dieser Einrichtungen abhängig von der Höhe des aggregierten ECII-Werts als Prozesse mit erheblichen oder kritischen Auswirkungen.[334]

4.3.2 Mindest-Cybersicherheitskontrollen und erweiterte Cybersicherheitskontrollen

Gemäß Artikel 28 der NCCS-Verordnung wird ein gemeinsamer Rahmen für die Cybersicherheit im Elektrizitätssektor geschaffen. Dieser Rahmen besteht aus mehreren zentralen Komponenten, darunter Mindest-Cybersicherheitskontrollen [335] und erweiterte Cybersicherheitskontrollen.[336] Zusätzlich zu den Mindest- und erweiter-

[329] Siehe Art. 3 Nr. 5 der VO (EU) 2024/1366.
[330] Siehe Art. 3 Nr. 7 der VO (EU) 2024/1366.
[331] Siehe Art. 3 Nr. 23 der VO (EU) 2024/1366.
[332] Siehe Art. 3 Nr. 24 der VO (EU) 2024/1366.
[333] Vgl. Art. 24 Abs. 3 Lit. a und b der VO (EU) 2024/1366.
[334] Vgl. Art. 24 Abs. 4 der VO (EU) 2024/1366.
[335] Vgl. Art. 28 Abs. 1 Lit. a der VO (EU) 2024/1366.
[336] Vgl. Art. 28 Abs. 1 Lit. b der VO (EU) 2024/1366.

ten Cybersicherheitskontrollen wird der gemeinsame Rahmen durch entsprechende Kontrollen in der Lieferkette erweitert. [337]

Welche Kontrollen anzuwenden sind, richtet sich nach dem Risikoprofil der jeweiligen Einrichtung: Einrichtungen mit erheblichen Auswirkungen müssen die Mindestkontrollen anwenden,[338] während Einrichtungen mit kritischen Auswirkungen die erweiterten Kontrollen anwenden müssen.[339]

Die Entwicklung der Mindest-Cybersicherheitskontrollen und erweiterten Cybersicherheitskontrollen erfolgt gemäß der NCCS-Verordnung wie folgt: Innerhalb von sieben Monaten nach Veröffentlichung des ersten unionsweiten Risikoberichts zur Cybersicherheit erarbeiten die ÜNB in Zusammenarbeit mit ENTSO-E und der EU-VNBO einen Vorschlag für diese Kontrollen.[340] Anschließend werden die Vorschläge von den zuständigen Behörden geprüft und genehmigt.[341]

[337]Vgl. Art. 28 Abs. 4 der VO (EU) 2024/1366.
[338]Vgl. Art. 28 Abs. 2 der VO (EU) 2024/1366.
[339]Vgl. Art. 28 Abs. 3 der VO (EU) 2024/1366.
[340]Vgl. Art. 29 Abs. 1 der VO (EU) 2024/1366.
[341]Vgl. Art. 8 Abs. 5 der VO (EU) 2024/1366.

KAPITEL 5

Nationale Umsetzung in Österreich

In diesem Kapitel wird ein Überblick darüber gegeben, wie die präventiven Sicherheitsanforderungen und reaktiven Meldepflichten der NIS1-Richtlinie in Österreich umgesetzt wurden. Abschließend folgt ein kurzer Ausblick auf den Stand der nationalen Umsetzung der NIS2-Richtlinie.

5.1 Umsetzung der Richtlinie (EU) 2016/1148

Die NIS1-Richtlinie wurde in Österreich im Jahr 2018 durch das Netz- und Informationssystemsicherheitsgesetz (NISG)[342] in nationales Recht umgesetzt. Ein Jahr später im Jahr 2019, trat die NIS-Verordnung (NISV)[343] in Kraft, die die Anforderungen des NISG weiter konkretisiert. Die NISV legt unter anderem fest, was genau unter einem Sicherheitsvorfall in den jeweiligen Sektoren zu verstehen ist, präzisiert die Definition wesentlicher Dienste und konkretisiert die erforderlichen Sicherheitsmaßnahmen.

5.1.1 Anwendungsbereich

Die Ermittlung der Betreiber wesentlicher Dienste im Stromsektor erfolgt durch einen Bescheid des Bundeskanzlers.[344] Dieser Bescheid ist verbindlich, kann jedoch

[342] Netz- und Informationssystemsicherheitsgesetz (NISG), BGBl. I Nr. 111/2018.
[343] Netz- und Informationssystemsicherheitsverordnung (NISV), BGBl. II Nr. 215/2019.
[344] Vgl. § 16 Abs. 4 NISG.

bei veränderten Voraussetzungen angepasst oder aufgehoben werden. Jede Änderung bedarf ebenfalls eines formalen Bescheides.[345]

Gemäß § 4 NISV gelten im Bereich der Stromversorgung insbesondere folgende Einrichtungen als Betreiber wesentlicher Dienste (siehe Tabelle 5.1):

Stromerzeugung	**Stromverteilung**	**Stromübertragung**
• Betreiber von Erzeugungsanlagen mit einer Engpassleistung von mehr als 340 MW, • Betreiber von Steuerungssystemen, die aggregiert eine Gesamtleistung von mehr als 340 MW abdecken.[346]	• Betreiber von Verteilernetzen mit mehr als 88,000 Zählpunkten, • Betreiber von Verteilernetzen, die in einer Landeshauptstadt angesiedelt sind.[347]	• Betreiber von Übertragungsnetzen.[348]

Tabelle 5.1: Betreiber wesentlicher Dienste im Elektrizitätssektor gemäß § 4 NISV

5.1.2 Sicherheitsanforderungen

Mit § 17 Abs. 1 NISG werden die Sicherheitsanforderungen des Art. 14 der NIS1-Richtlinie (siehe Abschnitt 4.1) weitgehend in nationales Recht umgesetzt.

> *„Zur Gewährleistung der NIS haben Betreiber wesentlicher Dienste in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wesentlichen Dienstes nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.“*[349]

[345] Vgl. § 16 Abs. 4 NISG.
[346] Vgl. § 4 Abs. 1 Z 1 Lit. a NISV.
[347] Vgl. § 4 Abs. 1 Z 1 Lit. b NISV.
[348] Vgl. § 4 Abs. 1 Z 1 Lit. c NISV.
[349] Siehe § 17 Abs. 1 NISG.

Die allgemeinen Vorgaben des NISG werden in § 11 NISV konkretisiert. Dort sind Sicherheitsvorkehrungen in elf Kategorien gegliedert, die jeweils durch konkrete Untermaßnahmen präzisiert werden.[350] Ein zentrales Element ist die Risikoanalyse der jeweiligen Netz- und Informationssysteme: Alle Sicherheitsmaßnahmen müssen soweit möglich auf Basis dieser Analyse erfolgen.[351] Die Kategorien sind:[352]

- Governance und Risikomanagement
- Umgang mit Dienstleistern und Dritten
- Sicherheitsarchitektur
- Systemadministration
- Identitäts- und Zugriffsmanagement
- Systemwartung und Betrieb
- Physische Sicherheit
- Erkennung von Vorfällen
- Bewältigung von Vorfällen
- Betriebskontinuität
- Krisenmanagement

Zusätzlich können Betreiber wesntlicher Dienste gemeinsam mit ihren Branchenverbänden dem Bundesminister für Inneres (BMI) sektorenspezifische Sicherheitsvorkehrungen vorschlagen.[353] Ein Beispiel hierfür ist der Leitfaden AT-3SV-Elektrizität des Elektrizitätsverband Oesterreichs Energie, der sektorspezifische Sicherheitsvorkehrungen für den Teilsektor Elektrizität konkretisiert und den Geltungsbereich (NIS-Scope) weiter präzisiert.[354] Solche Leitfäden entfalten zwar keine unmittelbare

[350] Vgl. Anlage 1 NISV.
[351] Vgl. § 11 NISV.
[352] Vgl. Anlage 1 Nr. 1–11 NISV.
[353] Vgl. § 11 Abs. 2 NISG.
[354] Vgl. Pfeiffer et al. (2021): *Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des § 17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV.*

Rechtsverbindlichkeit, dienen jedoch als maßgebliche Orientierung für Betreiber und Behörden bei der Umsetzung der gesetzlichen Anforderungen.[355]

Die Überwachung der Umsetzung der Sicherheitsvorkehrungen liegt beim BMI.[356] Betreiber müssen spätestens alle drei Jahre nachweisen, dass die Sicherheitsmaßnahmen umgesetzt wurden.[357] Der Nachweis kann durch Zertifizierungen nach anerkannten internationalen Normen oder durch Überprüfungen durch qualifizierte Stellen erfolgen.[358] Darüber hinaus ist der BMI berechtigt, nach vorheriger Ankündigung Einsicht in Netz- und Informationssysteme sowie zugehörige Unterlagen zu nehmen.[359]

5.1.3 Meldung von Sicherheitsvorfällen

§ 19 NISG verpflichtet Betreiber wesentlicher Dienste, Sicherheitsvorfälle, die ihre wesentlichen Dienste betreffen, unverzüglich in einem standardisierten elektronischen Format zu melden.[360] Meldungen werden grundsätzlich an das sektorenspezifische CSIRT gerichtet.[361] Gibt es ein solches nicht oder wird es vom Betreiber nicht unterstützt, ist das nationale CSIRT zuständig.[362] Sollte auch dieses fehlen, übernimmt das GovCERT.[363]

Neben der Pflicht zur Meldung an das zuständige CSIRT enthält das NISG auch Vorgaben zum Ablauf und zur inhaltlichen Ausgestaltung der Meldungen. Ein Sicherheitsvorfall ist zunächst durch eine Erstmeldung zu berichten, die alle zum Zeitpunkt bekannten Informationen enthält, insbesondere die Ursache, die betroffene IT sowie die Art der betroffenen Einrichtung oder Anlage.[364] Wenn sich im Nachhinein neue Details ergeben, müssen diese in Nachmeldungen ohne unangemessene weitere Verzögerung ergänzt werden.[365] Sobald der Vorfall vollständig bearbeitet ist, erfolgt eine Abschlussmeldung.[366] Betrifft ein Sicherheitsvorfall

[355] Vgl. Pfeiffer et al. (2021): *Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des § 17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV*, S. 5.
[356] Vgl. § 11 Abs. 3–4 NISG.
[357] Vgl. § 11 Abs. 3 NISG.
[358] Vgl. § 11 Abs. 3 NISG.
[359] Vgl. § 11 Abs. 4 NISG.
[360] Vgl. § 19 Abs. 1 und 3 NISG.
[361] Vgl. § 19 Abs. 2 NISG.
[362] Vgl. § 19 Abs. 2 NISG.
[363] Vgl. § 19 Abs. 2 NISG.
[364] Vgl. § 19 Abs. 3 NISG.
[365] Vgl. § 19 Abs. 3 NISG.
[366] Vgl. § 19 Abs. 3 NISG.

mehrere EU-Mitgliedstaaten, informiert das zuständige CSIRT oder der BMI die entsprechenden Stellen in den betroffenen Ländern.[367]

Ob ein Sicherheitsvorfall im Elektrizitätssektor meldepflichtig ist, richtet sich nach bestimmten Schwellenwerten. Diese sind in § 4 Abs. 2 NISV geregelt und lassen sich wie folgt zusammenfassen (siehe Tabelle 5.2):

Stromerzeugung	**Stromverteilung**	**Stromübertragung**
• Wenn die Leistung einer einzelnen Erzeugungsanlage insgesamt um mehr als 340 MW reduziert wird, oder • wenn die von den Steuerungssystemen kontrollierte Gesamtleistung aller Erzeugungsanlagen mindestens 340 MW unterschreitet.[368]	• Wenn der wesentliche Dienst mehr als 1.056.000 Zählpunktstunden (Anzahl der Zählpunkte × Dauer des Vorfalls in Stunden) ausfällt, oder • bei signifikant geminderter Verfügbarkeit des wesentlichen Dienstes für die Nutzer.[369]	• Wenn der Betrieb eines Übertragungsnetzes für mehr als drei Stunden ausfällt, oder • bei signifikant geminderter Verfügbarkeit des wesentlichen Dienstes für die Nutzer.[370]

Tabelle 5.2: Definition von Sicherheitsvorfall im Elektrizitätssektor gemäß § 4 NISV

5.1.4 CSIRTs und sektorspezifische Umsetzung in der Energieversorgung

Die Einrichtung und Aufgabenverteilung von CSIRTs in Österreich basiert auf § 14 NISG. Demnach können neben dem nationalen CSIRT auch sektorspezifische CSIRTs eingerichtet werden.[371] Ein für diese Arbeit besonders relevantes sektorspezifisches CSIRT ist das 2016 gegründete Austrian Energy CERT (AEC), das speziell

[367] Vgl. § 19 Abs. 5 NISG.
[368] Vgl. § 4 Abs. 2 Z 1 Lit. a NISV.
[369] Vgl. § 4 Abs. 2 Z 1 Lit. b sowie § 3 Abs. 2 und Abs. 8 NISV.
[370] Vgl. § 4 Abs. 2 Z 1 Lit. c sowie § 3 Abs. 2 NISV.
[371] Vgl. § 14 NISG.

für die österreichische Energiewirtschaft und damit auch für die Stromversorgung zuständig ist.[372]

Nach eigenen Angaben übernimmt das AEC derzeit unter anderem folgende Aufgaben:

- *„Die Bearbeitung von täglich eingehenden Anfragen und Sicherheitsmeldungen“*,[373]
- *„die Durchführung von Schulungstätigkeiten“*,[374]
- *„die Teilnahme an internationalen Cyber-Sicherheitsübungen“*,[375]
- *„die Mitarbeit bei der Erstellung technischer Sicherheitskonzepte für die Elektrizitäts- und Erdgaswirtschaft“*,[376]
- *„die Wahrnehmung der Rolle des Primäransprechpartners (Single Point of Contact) bei nationalen und internationalen Security Incidents im Energiesektor“*.[377]

Für die Meldung von Sicherheitsvorfällen stellt das AEC derzeit keine eigenen Meldeformulare zur Verfügung.[378] Sicherheitsvorfälle können stattdessen formlos, bevorzugt verschlüsselt per E-Mail über ein vorgesehenes Postfach gemeldet werden.[379] Eingehende Meldungen werden automatisiert in das interne Bearbeitungssystem übernommen und durch zuständige Fachkräfte betreut.[380]

Sollte eine Kontaktaufnahme per E-Mail aus Sicherheitsgründen nicht möglich oder nicht ratsam sein, ist das AEC während der regulären Geschäftszeiten auch telefonisch erreichbar.[381] Außerhalb dieser Zeiten steht der Energiewirtschaft in Österreich zusätzlich eine Rufbereitschaft zur Verfügung, um in dringenden Fällen reagieren zu können.[382]

[372] Vgl. CERT.at und GovCERT Austria (2016): *Bericht Internet-Sicherheit Österreich 2016*, S. 47–49.
[373] Siehe AEC (2025): *Über uns.*
[374] Siehe AEC (2025): *Über uns.*
[375] Siehe AEC (2025): *Über uns.*
[376] Siehe AEC (2025): *Über uns.*
[377] Siehe AEC (2025): *Über uns.*
[378] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 6.
[379] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 2.11 und 6.
[380] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 2.11 und 6.
[381] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 2.11.
[382] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 3.2; AEC (2025): *Kontakt.*

Dabei ist zu beachten, dass Meldungen der Einrichtungen nicht einheitlich behandelt werden.[383] Das Ausmaß der Unterstützung durch das AEC hängt von folgenden Faktoren ab:[384]

- der Art und Schwere des Vorfalls,
- dem Typ der betroffenen Organisation,
- der Größe der betroffenen Nutzergruppe,
- den zum jeweiligen Zeitpunkt verfügbaren Ressourcen

Zur sicheren Übermittlung von Informationen stellt das AEC sowohl S/MIME-Zertifikate als auch einen PGP-Public-Key zur Verfügung.[385] Diese kryptografischen Verfahren gewährleisten die Vertraulichkeit, Integrität und Authentizität der übermittelten Daten.[386] Das AEC ist außerdem sowohl national als auch international in sicherheitsrelevante Kooperationen eingebunden.[387] Der Austausch sensibler Informationen erfolgt dabei datenschutzkonform nach dem Traffic Light Protocol.[388]

5.2 Umsetzung der Richtlinie (EU) 2022/2555

Die Umsetzung der NIS2-Richtlinie erfolgt in den Mitgliedstaaten der EU derzeit sehr uneinheitlich. Während einige Länder die Anforderungen der Richtlinie bereits vollständig in nationales Recht umgesetzt haben, befinden sich andere noch im Gesetzgebungsprozess oder haben die Umsetzung vorübergehend ausgesetzt.[389]

Am 7. Mai 2025 hat die Europäische Kommission eine begründete Stellungnahme an 19 Mitgliedstaaten versendet, da sie es versäumt haben, die vollständige Umsetzung der NIS2-Richtlinie zu melden.[390] Die 19 Mitgliedstaaten haben nun zwei Monate Zeit, darauf zu reagieren.[391] Reagiert ein Mitgliedstaat nicht oder nur unzureichend auf eine Aufforderung zur Vertragsverletzungsbehebung, kann die Europäische

[383] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 4.1.
[384] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 4.1.
[385] Vgl. AEC (2025): *Kontakt*.
[386] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 2.8.
[387] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 4.2.
[388] Vgl. Rosenkranz (2024): *RFC 2350 – Austrian Energy CERT*, Abschnitt 2.11.
[389] Vgl. Europäische Kommission (2025): *State-of-play of the transposition of the NIS2 Directive*.
[390] Vgl. Europäische Kommission (2025): *State-of-play of the transposition of the NIS2 Directive*.
[391] Vgl. Europäische Kommission (2025): *State-of-play of the transposition of the NIS2 Directive*.

Kommission den Europäischen Gerichtshof anrufen.[392] Der Gerichtshof ist dann befugt, finanzielle Sanktionen gegen den Mitgliedstaat zu verhängen.[393]

Auch Österreich gehört zu den Mitgliedstaaten, die die NIS2-Richtlinie bislang noch nicht vollständig umgesetzt haben. Der nationale Gesetzgebungsprozess zur Novellierung des NISG verläuft derzeit schleppend.[394] Am 19. Juni 2024 wurde das NISG 2024 mit Änderungen im Innenausschuss mit einfacher Mehrheit (ÖVP und Grüne) beschlossen.[395] In der 270. Sitzung des Nationalrats am 3. Juli 2024 kam der Gesetzesentwurf in die zweite Lesung, scheiterte jedoch an der erforderlichen Zweidrittelmehrheit und wurde daher abgelehnt.[396] Die qualifizierte Mehrheit ist notwendig, da das Gesetz Verfassungsbestimmungen umfasst.[397] Eine einfache Mehrheit lag jedoch mit den Stimmen der Grünen und ÖVP vor.[398] Ein konkretes Inkrafttretensdatum steht noch aus, allerdings ist mit einer Verabschiedung im Laufe des Jahres 2025 zu rechnen.[399]

[392]Vgl. Art. 258 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), ABl. C 202 vom 7.6.2016, S. 1.
[393]Vgl. Art. 260 Abs. 3 AEUV, ABl. C 202 vom 7.6.2016, S. 1.
[394]Vgl. Wirtschaftskammer Österreich (2025): *NISG kommt voraussichtlich 2025.*
[395]Vgl. Österreichisches Parlament (2024): *270. Sitzung des Nationalrats vom 3. Juli 2024 (270/NRSITZ)*, TOP 24.
[396]Vgl. Österreichisches Parlament (2024): *270. Sitzung des Nationalrats vom 3. Juli 2024 (270/NRSITZ)*, TOP 24.
[397]Vgl. Österreichisches Parlament (2024): *Nationalrat: Absage für Informationssystemsicherheitsgesetz.*
[398]Vgl. Österreichisches Parlament (2024): *Nationalrat: Absage für Informationssystemsicherheitsgesetz.*
[399]Vgl. Wirtschaftskammer Österreich (2025): *NISG kommt voraussichtlich 2025.*

KAPITEL 6

Fazit

Die vorliegende Arbeit hat gezeigt, dass die Stromversorgung als eine der zentralen kritischen Infrastrukturen durch die fortschreitende Digitalisierung erheblich an Angriffsfläche gewonnen hat. Die Auswertung aktueller Daten zu Sicherheitsvorfällen verdeutlicht zudem einen signifikanten Anstieg seit 2022, der insbesondere im Zusammenhang mit den aktuellen geopolitischen Spannungen steht.

Die analysierten Fallbeispiele zeigten, dass die Ukraine in den vergangenen Jahren unfreiwillig zu einem Testfeld für erfolgreiche Cyberangriffe auf die Stromversorgung wurde. Bei diesen Angriffen war ein wiederkehrendes Muster zu beobachten: Die initiale Angriffsfläche bildete das Büronetzwerk, das in den Jahren 2015 und 2016 durch Social Engineering kompromittiert wurde. Sobald sich die Angreifer im Büronetzwerk initial etabliert hatten, folgte eine systematische Ausspähung des Netzwerks, um sicherheitskritische Informationen zu sammeln, beispielsweise welche Server mit dem PCN verbunden waren oder welche weiteren Kommunikationswege bestanden. Anschließend pivotierten die Angreifer in das PCN, wo eine weitere Aufklärungsphase stattfand. Bei allen analysierten Cyberangriffen führten folgende Kombinationen letztlich zu den Stromausfällen:

- Manipulation von Leistungsschaltern in Umspannwerken
- Einsatz von Wiper-Malware, die systemkritische Daten löschte und die Wiederherstellung erschwerte

Eine weitere Beobachtung ist, dass Angreifer zunehmend darauf achten, ihre Werkzeuge möglichst lange vor Entdeckung zu bewahren. Im Laufe der Zeit wurde bei den eingesetzten Malware-Varianten verstärkt auf Obfuskationstechniken zurückgegriffen, um die Analyse erschweren oder zu verzögern. Der Einsatz verschiedener Wiper-Malware-Varianten, die unter anderem der Beseitigung von Spuren dienten, bestätigt diese Einschätzung. Offenbar sind sich die Angreifer bewusst, dass jeder Leak und jede Spur ihrer Tools zu Gegenmaßnahmen führen kann. Entsprechend versuchen sie, die Entdeckung und das Reverse Engineering ihrer Schadsoftware so lange wie möglich hinauszuzögern.

Als Reaktion auf die zunehmende Bedrohungslage und die zentrale Bedeutung der Stromversorgung für das Funktionieren einer modernen Gesellschaft hat die EU die Cybersicherheitsanforderungen sowie die Meldepflichten kontinuierlich verschärft. Während die NIS1-Richtlinie noch relativ allgemeine Maßnahmen vorsah, wurden diese mit der NIS2-Richtlinie deutlich präzisiert und erweitert. Mit der NIS2-Richtlinie wurde außerdem der Anwendungsbereich deutlich ausgeweitet, sodass nun wesentlich mehr Einrichtungen direkt betroffen sind. Indirekt erfasst die Richtlinie jedoch auch deren Lieferanten und Dienstleister, die künftig strengere Anforderungen ihrer Kunden erfüllen müssen. In Österreich zeigt sich das Ausmaß der Ausweitung sektorübergreifend: Statt rund 100 Unternehmen nach NIS1 könnten künftig bis zu 4.000 Unternehmen aus allen betroffenen Bereichen direkt von der NIS2-Richtlinie betroffen sein.[400]

National wurde die NIS1-Richtlinie 2018 mit dem NISG umgesetzt. 2019 folgte die NISV, die die wesentlichen Dienste der betroffenen Betreiber im Elektrizitätssektor genauer definiert und die präventiven Sicherheitsanforderungen konkretisiert. Zudem legt die NISV fest, was genau unter einem Sicherheitsvorfall in den jeweiligen Sektoren zu verstehen ist. So müssen Betreiber wesentlicher Dienste im Elektrizitätssektor technische und organisatorische Sicherheitsvorkehrungen treffen, regelmäßige Risikoanalysen durchführen und Sicherheitsvorfälle dem AEC als sektorspezifischem CSIRT zu melden.

Die Umsetzung der NIS2-Richtlinie verläuft hingegen in den Mitgliedsstaaten bislang schleppend: Auch Österreich hat die Vorgaben noch nicht vollständig in nationales Recht überführt, da der Gesetzesentwurf die erforderliche qualifizierte Mehrheit nicht erhielt. Eine endgültige Verabschiedung wird jedoch voraussichtlich noch im

[400] Wirtschaftskammer Österreich (2024): *Cybersicherheits-Richtlinie NIS 2: Neue Regelungen für mehr Cybersicherheit in der EU.*

Jahr 2025 erfolgen. Ein ähnliches Bild zeigt sich bei der nationalen Umsetzung der CER-Richtlinie: Obwohl die Umsetzungsfrist bereits am 17. Oktober 2024 endete, haben am 28. November 2024 ebenfalls nur 3 von 27 EU-Mitgliedstaaten nationale Gesetze zur CER-Umsetzung verabschiedet.[401] In Österreich liegt seit Juli 2025 ein entsprechender Regierungsentwurf zum Resilienz kritischer Einrichtungen-Gesetz vor.[402]

Ergänzend zur NIS2-Richtlinie hat die EU mit der NCCS-Verordnung erstmals einen sektorspezifischen Rechtsakt für die Stromversorgung eingeführt, der Cybersicherheitsanforderungen für grenzüberschreitende Stromflüsse festlegt. Diese Anforderungen werden bei Bedarf kontinuierlich aktualisiert und angepasst, wodurch eine praxisnähere und flexiblere Umsetzung ermöglicht wird als bei den eher allgemeinen, rahmenorientierten Vorgaben der NIS-Richtlinien. Die NCCS-Verordnung gilt zwar aufgrund ihrer Rechtsnatur unmittelbar in allen Mitgliedstaaten, ihre Umsetzung erfolgt jedoch schrittweise und wird sich noch über mehrere Jahre erstrecken. Wie aus der Umsetzungsplanung des europäischen Übertragungsnetzbetreiberverband ENTSO-E hervorgeht, beginnt der Prozess auf europäischen Ebene mit der Entwicklung und Genehmigung zentraler Vorgaben.[403] Erst im Anschluss können die betroffenen Stellen mit der Umsetzung auf nationaler beziehungsweise operativer Ebene beginnen.[404] Nach Einschätzung von ENTSO-E wird die vollständige Implementierung der NCCS-Verordnung voraussichtlich bis 2033 abgeschlossen sein.[405]

[401] Vgl. Vertretung der Europäischen Kommission in Deutschland (2024): *Cybersicherheit und Resilienz kritischer Einrichtungen: Vertragsverletzungsverfahren gegen Deutschland und weitere Mitgliedstaaten.*
[402] Vgl. Österreichisches Parlament (2025): *Resilienz kritischer Einrichtungen-Gesetz – RKEG (Entwurf XXVIII/I/186).*
[403] Vgl. ENTSO-E (2024): *Cybersecurity Network Code.*
[404] Vgl. ENTSO-E (2024): *Cybersecurity Network Code.*
[405] Vgl. ENTSO-E (2024): *Cybersecurity Network Code.*

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Bücher

Schwab, Adolf (2022). *Elektroenergiesysteme: Smarte Stromversorgung im Zeitalter der Energiewende*. 7. Aufl. Springer-Verlag GmbH Deutschland. DOI: 10.1007/978-3-662-64774-5.

Pohlmann, Norbert (2019). *Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer Vieweg. DOI: 10.1007/978-3-658-36243-0.

ENISA, Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou und Apostolos Malatras (2021). *ENISA threat landscape 2021 – April 2020 to mid-July 2021*. European Union Agency for Cybersecurity. DOI: 10.2824/324797.

ENISA, Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Rossen Svetozarov Naydenov u. a. (2022). *ENISA threat landscape 2022 – July 2021 to July 2022*. European Union Agency for Cybersecurity. DOI: 10.2824/764318.

ENISA, Ifigeneia Lella, Cosmin Ciobanu u. a. (2023). *ENISA threat landscape 2023 – July 2022 to June 2023*. European Union Agency for Cybersecurity. DOI: 10.2824/782573.

ENISA, Ifigeneia Lella, Marianthi Theocharidou, Elpida Tsekmezoglou u. a. (2024). *ENISA threat landscape 2024 – July 2023 to June 2024*. European Union Agency for Cybersecurity. DOI: 10.2824/0710888.

Rass, Stefan u. a., Hrsg. (2025). *Cybersicherheit in kritischen Infrastrukturen: Ein spieltheoretischer Zugang*. Cham: Springer Nature Switzerland, S. 23–46. DOI: 10.1007/978-3-031-58999-7.

Artikel

Hasan, Mohammad Kamrul u. a. (2023). "Review on cyber-physical and cybersecurity system in smart grid: Standards, protocols, constraints, and recommendations". In: *Journal of Network and Computer Applications*, S. 103540. DOI: 10.1016/j.jnca.2022.103540.

Krause, Tim u. a. (2021). "Cybersecurity in Power Grids: Challenges and Opportunities". In: *Sensors* 21. DOI: 10.3390/s21186225.

Yohanandhan, Rajaa Vikhram u. a. (2020). "Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications". In: *IEEE Access*, S. 151019–151064. DOI: 10.1109/ACCESS.2020.3016826.

Yadav, Geeta und Kolin Paul (2021). "Architecture and security of SCADA systems: A review". In: *International Journal of Critical Infrastructure Protection*, S. 100433. DOI: 10.1016/j.ijcip.2021.100433.

Salahdine, Fatima und Naima Kaabouch (2019). "Social Engineering Attacks: A Survey". In: *Future Internet* 11.4. DOI: 10.3390/fi11040089.

Khan, Faiza, Syed Muhammad Mohsin und Hanif Durad (2023). "Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids". In: *Journal of Computing Biomedical Informatics* 4, S. 172–185. DOI: 10.56979/402/2023.

Alladi, Tejasvi, Vinay Chamola und Sherali Zeadally (2020). "Industrial Control Systems: Cyberattack trends and countermeasures". In: *Computer Communications* 155, S. 1–8. DOI: 10.1016/j.comcom.2020.03.007.

Konferenzbeiträge

Dabrowski, Adrian, Johanna Ullrich und Edgar R. Weippl (2017). "Grid shock: Coordinated load-changing attacks on power grids". In: *Proceedings of the 33rd Annual Computer Security Applications Conference (ACSAC)*. Association for Computing Machinery, S. 303–314. DOI: 10.1145/3134600.3134639.

Velde, Dennis van der u. a. (2020). "Methods for actors in the electric power system to prevent, detect and react to ICT attacks and failures". In: *Proceedings of the 2020 IEEE International Energy Conference (ENERGYCon)*. IEEE, S. 17–22. DOI: 10.1109/ENERGYCon48941.2020.9236523.

Srivastava, Animesh, Bhupender Singh Rawat und Sant Kumar Maurya (2023). “A review on protecting SCADA systems from DDoS attacks”. In: *Proceedings of the 2023 International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, S. 556–561. DOI: 10.1109/ICESC57686.2023.10193650.

Markovic-Petrovic, Jasna D. und Mirjana D. Stojanovic (2013). “Analysis of SCADA system vulnerabilities to DDoS attacks”. In: *Proceedings of the 2013 International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*. IEEE, S. 591–594. DOI: 10.1109/TELSKS.2013.6704448.

Kalluri, Rajesh u. a. (2016). “Simulation and impact analysis of denial-of-service attacks on power SCADA”. In: *Proceedings of the 2016 National Power Systems Conference (NPSC)*. IEEE, S. 1–5. DOI: 10.1109/NPSC.2016.7858908.

Khan, Rafiullah u. a. (2016). “Threat analysis of BlackEnergy malware for synchrophasor based real-time control and monitoring in smart grid”. In: *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research*. BCS Learning & Development Ltd., S. 1–11. DOI: 10.14236/ewic/ICS2016.7.

Geiger, Marcus u. a. (2020). “An analysis of BlackEnergy 3, Crashoverride, and Trisis: Three malware approaches targeting operational technology systems”. In: *Proceedings of the 2020 IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, S. 1537–1543. DOI: 10.1109/ETFA46521.2020.9212128.

Normen

International Organization for Standardization (ISO) (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. URL: https://www.iso.org/standard/73029.html (besucht am 24. 06. 2025).

Vulnerabilitätsberichte

CVE-2015-5374: Denial-of-Service Vulnerability in Siemens SIPROTEC EN100 Ethernet Module, 2015. URL: https://nvd.nist.gov/vuln/detail/CVE-2015-5374, (besucht am 30. 08. 2025).

CVE-2023-28771: OS Command Injection via Improper Error Message Handling in Zyxel Firewall Series, 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-28771, (besucht am 30. 08. 2025).

CVE-2023-33009: Buffer Overflow in Notification Function of Zyxel Firewall Series Allowing Unauthenticated Denial-of-Service and Remote Code Execution, 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-33009, (besucht am 30. 08. 2025).

CVE-2023-33010: Buffer Overflow in ID Processing Function of Zyxel Firewall Series Leading to DoS and Remote Code Execution, 2023. URL: https://nvd.nist.gov/vuln/detail/CVE-2023-33010, (besucht am 30. 08. 2025).

Reports

Europäische Kommission (2022). *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Digitalisierung des Energiesystems – EU-Aktionsplan*. COM/2022/552 final. Europäische Kommission. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:52022DC0552 (besucht am 24. 06. 2025).

Europäischer Rechnungshof (2025). *Das Stromnetz der EU fit machen für Netto-Null-Emissionen*. RV-01-2025. Europäischer Rechnungshof. URL: https://eca.europa.eu/ECAPublications/RV-2025-01/RV-2025-01_DE.pdf (besucht am 24. 06. 2025).

Oesterreichs Energie (2021). *Netzberechnungen Österreich – Einfluss der Entwicklungen von Elektromobilität und Photovoltaik auf das österreichische Stromnetz*. Oesterreichs Energie. URL: https://oesterreichsenergie.at/fileadmin/user_upload/Oesterreichs_Energie/Publikationsdatenbank/Studien/2020/2020.11_Studie_NetzberechnungenAT_PVundEV.pdf (besucht am 15. 07. 2025).

Dragos, Inc. (2018). *Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE*. Techn. Ber. Dragos, Inc. URL: https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf (besucht am 08. 08. 2025).

Cherepanov, Anton (2017). *Win32/Industroyer: A new threat for industrial control systems*. Techn. Ber. ESET. URL: https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (besucht am 16. 07. 2025).

SektorCERT (2023). *The Attack Against Danish Critical Infrastructure*. Techn. Ber. SektorCERT. URL: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf (besucht am 10. 05. 2025).

INCIBE-CERT (2024). *ICS Malware Analysis Study: BlackEnergy*. Techn. Ber. Instituto Nacional de Ciberseguridad (INCIBE). URL: https://www.incibe.es/sites/default/files/2024-02/INCIBE-CERT_ICS_ANALYSIS_STUDY_BLACKENERGY_2024_v1.0.pdf (besucht am 16. 07. 2025).

Cherepanov, Anton und Robert Lipovsky (2016). *BlackEnergy – What We Really Know About the Notorious Cyber Attacks*. Techn. Ber. Virus Bulletin. URL: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cherepanov-Lipovsky.pdf (besucht am 22. 08. 2025).

iTrust, SUTD (2016). *BlackEnergy – Malware for Cyber-Physical Attacks*. Techn. Ber. Singapore University of Technology und Design (SUTD). URL: https://itrust.sutd.edu.sg/wp-content/uploads/2016/10/itrust-analysis-blackenergy.pdf (besucht am 16. 07. 2025).

Dragos, Inc. (2017). *CrashOverride: Analysis of the Threat to Electric Grid Operations*. Techn. Ber. Dragos, Inc. URL: https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (besucht am 05. 06. 2025).

National Power Company Ukrenergo (2018). *UKRENERGO-2017: Results of the First Reforms*. National Power Company Ukrenergo. URL: https://ua.energy/wp-content/uploads/2018/03/fynalnaya-prezentatsyya-engl.pdf (besucht am 04. 06. 2025).

Pfeiffer, Thomas, Armin Selhofer und Mitarbeiter von Oesterreichs Energie (2021). *Sektorenspezifische Sicherheitsvorkehrungen für den Sektor Energie (AT-3SV-Elektrizität) im Sinne des § 17 Abs. 2 NISG mit Einschränkung auf den Teilsektor Elektrizität im Sinne des § 4 Abs. 1 Z 1 NISV*. Leitfaden, Version 1.4. Oesterreichs Energie. URL: https://oesterreichsenergie.at/fileadmin/user_upload/Oesterreichs_Energie/Publikationsdatenbank/Leitfaden/2021/2021.06.24_AT-3SV-Elektrizit%C3%A4t_V1.4.pdf (besucht am 16. 07. 2025).

CERT.at and GovCERT Austria (2016). *Bericht zur Lage der Internet-Sicherheit in Österreich 2016*. CERT.at / GovCERT Austria. URL: https://www.cert.at/media/files/downloads/reports/jahresbericht-2016/files/cert.at-jahresbericht-2016.pdf (besucht am 22. 07. 2025).

Rosenkranz, Wolfgang (2024). *RFC 2350: Austrian Energy CERT Profile*. Austrian Energy CERT. URL: https://www.energy-cert.at/media/files/static/rfc2350/20240528_AEC_rfc2350_signed.txt (besucht am 30. 05. 2025).

Online-Quellen

Eurelectric (2025). *Cybersecurity in the Power Sector*. URL: https://www.eurelectric.org/in-detail/cybersecurity-in-the-power-sector/ (besucht am 15. 07. 2025).

Oesterreichs Energie (2025). *Digitalisierung – warum das Stromnetz intelligent werden muss*. URL: https://oesterreichsenergie.at/fakten/unser-stromsystem-erklaert/digitalisierung (besucht am 24. 06. 2025).

U.S. Department of Justice (2020). *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*. URL: https://www.justice.gov/archives/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and (besucht am 18. 07. 2025).

Vincent, Elise und Cédric Pietralunga (2023). *Cyberattacks on the rise in Europe amidst the war in Ukraine*. URL: https://www.lemonde.fr/en/europe/article/2023/04/03/the-rise-of-cyberattacks-in-europe-amidst-the-war-in-ukraine_6021493_143.html (besucht am 15. 07. 2025).

Bock, Patrice u. a. (2017). *Ukrainian Power Grids Cyberattack*. URL: https://www.isa.org/intech-home/2017/march-april/features/ukrainian-power-grids-cyberattack (besucht am 04. 05. 2025).

New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) (2016). *BlackEnergy*. URL: https://www.cyber.nj.gov/threat-landscape/malware/trojans/blackenergy (besucht am 28. 07. 2025).

ESET WeLiveSecurity (2022). *Industroyer2: Industroyer Reloaded*. URL: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (besucht am 16. 07. 2025).

CyS Centrum (2016). *Cyberbedrohung BlackEnergy2/3. Geschichte der Angriffe auf kritische IT-Infrastruktur der Ukraine [eigene Übersetzung]*. URL: https:

//cys-centrum.com/ru/news/black_energy_2_3 (besucht am 04. 05. 2025).

Cybersecurity and Infrastructure Security Agency (CISA) (2016). *Cyber-Attack Against Ukrainian Critical Infrastructure – ICS Alert (IR-ALERT-H-16-056-01)*. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 (besucht am 04. 05. 2025).

BBC News (2017). *Ukraine power cut 'was cyber-attack'*. URL: https://www.bbc.com/news/technology-38573074 (besucht am 08. 08. 2025).

ESET (2022). *Industroyer: Eine Cyberwaffe, die einem Stromnetz den Stecker rauszog*. URL: https://www.welivesecurity.com/deutsch/2022/06/14/industroyer-eine-cyberwaffe-die-einem-stromnetz-den-stecker-rauszog/ (besucht am 04. 06. 2025).

Tidy, Joe (2022). *Ukrainian power grid 'lucky' to withstand Russian cyber-attack*. URL: https://www.bbc.com/news/technology-61085480 (besucht am 11. 05. 2025).

Kapellmann Zafra, Daniel u. a. (2022). *INDUSTROYER.V2: Old Malware Learns New Tricks*. Google Cloud Threat Intelligence Blog. URL: https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks?hl=en (besucht am 12. 08. 2025).

Austrian Energy CERT (2025a). *Über uns*. URL: https://www.energy-cert.at/de/ueber-uns/ (besucht am 19. 05. 2025).

— (2025b). *Kontakt*. URL: https://www.energy-cert.at/de/kontakt/ (besucht am 20. 05. 2025).

Europäische Kommission (2025). *State-of-play of the transposition of the NIS2 Directive*. URL: https://digital-strategy.ec.europa.eu/en/policies/nis-transposition (besucht am 24. 05. 2025).

Österreichisches Parlament (2024a). *270. Sitzung des Nationalrats vom 3. Juli 2024 (270/NRSITZ)*. URL: https://www.parlament.gv.at/gegenstand/XXVII/NRSITZ/270 (besucht am 10. 09. 2025).

— (2024b). *Nationalrat: Absage für Informationssystemsicherheitsgesetz*. URL: https://www.parlament.gv.at/aktuelles/pk/jahr_2024/pk0785 (besucht am 24. 07. 2025).

Wirtschaftskammer Österreich (2024). *Cybersicherheits-Richtlinie NIS 2: Neue Regelungen für mehr Cybersicherheit in der EU*. URL: https://www.wko.at/it-sicherheit/nis2-uebersicht (besucht am 25. 08. 2025).

Vertretung der Europäischen Kommission in Deutschland (2024). *Cybersicherheit und Resilienz kritischer Einrichtungen: Vertragsverletzungsverfahren gegen Deutschland und weitere Mitgliedstaaten*. URL: https://germany.representation.ec.europa.eu/news/cybersicherheit-und-resilienz-kritischer-einrichtungen-vertragsverletzungsverfahren-gegen-2024-11-28_de (besucht am 10. 09. 2025).

ENTSO-E (2024). *Cybersecurity Network Code*. URL: https://www.entsoe.eu/network_codes/nccs/ (besucht am 30. 07. 2025).

Rechtsquellen

EU

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union. ABl. L 194, S. 1–30.

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). ABl. L 333, S. 80–152.

Delegierte Verordnung (EU) 2024/1366 der Kommission vom 11. März 2024 zur Ergänzung der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates durch Festlegung eines Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse. ABl. L 141, S. 1–44.

Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnologien sowie zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Cybersecurity Act). ABl. L 151, S. 15–69.

Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates. ABl. L 333, S. 164–198.

Vertrag über die Arbeitsweise der Europäischen Union. ABl. C 202, S. 1–388.

Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Aufhebung der Richtlinie 2003/54/EG. ABl. L 211, S. 55–93.

Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über den Elektrizitätsbinnenmarkt. ABl. L 158, S. 54–124.

Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates vom 5. Juni 2019 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt und zur Änderung der Richtlinie 2012/27/EU. ABl. L 158, S. 125–199.

Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. ABl. L 124, S. 36–41.

Österreich

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG). BGBl. I Nr. 111/2018.

Verordnung gemäß § 3 und § 4 NISG (Netz- und Informationssystemsicherheitsverordnung – NISV). BGBl. II Nr. 215/2019.