GESELLSCHAFT
FÜR INFORMATIK

dena
Deutsche Energie-Agentur

Future Energy
Lab

STUDIE

# 2. Themenroadmap der Branchen-plattform Cybersicherheit in der Stromwirtschaft

# Impressum

**Herausgeber:**
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin
Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699
E-Mail: info@dena.de
Internet: www.dena.de

**Autorin:**
Linda Schwarz, Gesellschaft für Informatik e. V.

**Redaktion:**
Nikolas Becker, Gesellschaft für Informatik e. V.
Marius Dechand, dena
Friederike Wenderoth, dena

**Stand:**
Überarbeitete Fassung, Dezember 2024


**Bitte zitieren als:**
Deutsche Energie-Agentur (Hrsg.) (dena, 2024) und Gesellschaft für Informatik e.V. (2024):
2. *Themen-roadmap der Branchenplattform Cybersicherheit in der Stromwirtschaft*

**Hinweis:**
Die Inhalte wurden gemeinsam mit allen Partnern erarbeitet. Die Meinungen einzelner Partner können zu bestimmten Aspekten von den dargestellten Ergebnissen abweichen. Die Verantwortung für den Inhalt liegt allein bei den Autorinnen und Autoren.

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

# Management Summary

**Welche Cybersicherheitsthemen bewegen die Stromwirtschaft?**

Cybersicherheit ist für die Energiebranche ein weiterhin zunehmend wichtiges Thema. Neben der Anzahl und der Professionalität der Angriffe wachsen auch die Anforderungen aus der deutschen und europäischen Gesetzgebung, bei gleichzeitiger Ausweitung des Adressatenkreises dieser Gesetze. Die Branchenplattform Cybersicherheit in der Stromwirtschaft ist eine Austauschplattform für stellvertretende Akteure der Strom- und Digitalwirtschaft sowie für Behörden und Verbände. Ziel der Plattform ist es, Wissen, Erfahrungen und Lösungsansätze zu teilen, um so Fortschritte im Bereich der Cybersicherheit in der Stromwirtschaft auf den Weg zu bringen und die Hürden bei der Umsetzung aktueller und zukünftiger gesetzlicher Vorgaben und Standards zu verringern. Zu diesem Zweck wurde in Zusammenarbeit mit der Gesellschaft für Informatik e.V. gemeinsam mit den Partnern der Branchenplattform eine Themenroadmap entwickelt, die als Grundlage für die zu führenden Debatten dient. Sieben Handlungsfelder wurden identifiziert, die als besonders relevant eingestuft werden. Im Jahr 2024 wurde bereits ein Großteil dieser Themen diskutiert, bearbeitet und teilweise abgeschlossen. Die Themen sind im Folgenden nach Bearbeitungsreihenfolge sortiert und mit ihrem aktuellen Bearbeitungsstand dargestellt:

**Führungskräfte sensibilisieren**

Stand 12/2024: In Zusammenarbeit mit dem Fraunhofer IOSB-AST wurde die Studie „Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft“ erstellt und im September 2024 veröffentlicht.

Mit der Umsetzung der NIS2-Richtlinien soll Cybersicherheit zur Aufgabe der Führungsetage gemacht werden. Allerdings ist die Wahrnehmung der Befragten, dass dies als Motivation für Führungskräfte oftmals nicht ausreicht, um größere Budgets für Cybersicherheitsmaßnahmen bereitzustellen. Eine wichtige Ursache ist vor allem die Undurchsichtigkeit der Kosten von Cybersicherheit und den verschiedenen Komponenten, verbunden mit Schwierigkeiten bei der Ressourcenabschätzung für umfassende Security. Der Stromsektor als Kritische Infrastruktur muss zwar bereits vermehrt Anforderungen erfüllen, aber Cybersicherheit ist mehr als Dienst nach Vorschrift, da täglich neue Technologien entwickelt und Schwachstellen gefunden werden.

**Gemeinsam aus Cyberattacken lernen**

Stand 12/2024: In Zusammenarbeit mit der Gesellschaft für Informatik e.V., Cyber Policy Haus BV und Prof. Dr. Stefan Sütterlin wird eine Studie durchgeführt. Im Februar 2025 ist hierzu eine Pilot-Veranstaltung geplant.

Zahlreiche Unternehmen waren bereits Opfer einer Cyberattacke. Nur wenige davon äußern sich dazu umfassend in der Öffentlichkeit aus Angst vor Reputationsverlust. Jedoch bietet genau dieser Austausch ein enormes Potenzial zur Steigerung der Resilienz des Energiesektors. Eine institutionalisierte Plattform für sowohl brancheninterne, vertrauensvolle Austausche als auch öffentliche Erfahrungsberichte kann einen strukturellen Rahmen für einen kollaborativen Umgang mit Cyberattacken bieten.

**Harmonisierung von Zertifizierungen und vernetzter OT-Systeme im Cybersicherheitsbereich[1]**

Stand 12/2024: In Zusammenarbeit mit der c.con Management GmbH wird bis Mitte 2025 eine Studie durchgeführt.

OT-Systeme weisen sehr spezielle Herausforderungen bei der Umsetzung von Cybersicherheitsmaßnahmen auf, da sie grundsätzlich längere Innovationszyklen haben, meist in proprietäre Systeme eingebunden sind und teilweise auch während der Durchführung von Updates erreichbar bleiben müssen. Um diesen Herausforderungen zu begegnen, können Best-Practice-Ansätze, regulatorische Handlungsempfehlungen sowie kulturelle Denkanstöße im Umgang mit OT-Systemen etabliert werden.

Die Gesetzgebung gibt Betreibern Kritischer Infrastrukturen vor, welche Sicherheitsanforderungen sie zu erfüllen haben. Diese Anforderungen müssen nicht nur umgesetzt, sondern ihre Erfüllung muss auch nachgewiesen werden. Zertifizierungen ermöglichen es Unternehmen, durch unabhängige Prüfung nachzuweisen, dass sie den Anforderungen gerecht werden. Da das Bundesamt für Sicherheit in der Informationstechnik (BSI) offenlässt, wie diese Nachweise konkret aussehen können, gibt es verschiedene Nachweisverfahren, die sich nach etablierten internationalen Standards (ISO/IEC) richten. Die bestehende Komplexität bei Zertifikaten und Nachweisverfahren führt zu einem hohen Aufwand dafür, die passenden Formate herauszusuchen und zu vergleichen.

**Transparenz in der Gesetzgebung erhöhen**

Stand 12/2024: Anfang 2024 hat ein Workshop stattgefunden. Eine Studie befindet sich in Planung.

Es gibt ein umfassendes Regelwerk von Vorschriften zu den Anforderungen an die Cybersicherheit von Betreibern Kritischer Infrastrukturen. Allerdings werden sie von verschiedenen Institutionen mit unterschiedlichen Rollen erarbeitet. Außerdem existiert eine Vielzahl von Organisationen, die Handlungsempfehlungen erarbeiten, Informationen bereitstellen oder einen Erfahrungsaustausch zur Cybersicherheit anregen.

**Test- und Weiterbildungsmöglichkeiten ausbauen**

Stand 12/2024: Bearbeitung noch nicht geplant

Regelmäßige Cybersicherheitsübungen, der Ausbau von Testmöglichkeiten für das Zusammenspiel von IT- und OT-Systemen sowie Testlabore zur Einbindung neuer Software in eine realitätsnahe Testumgebung bieten einen substanziellen Mehrwert zur Stärkung der Resilienz von Unternehmen. Dieses Angebot kann durch die Entwicklung von Konzepten zu stromwirtschaftsspezifischen Weiterbildungen oder Cybersicherheitsübungen sowie eine Sammlung von Anforderungen an Testlabore spezifiziert und erweitert werden.

**Eine Wissensbasis zur Klassifizierung von Bedrohungen und Angriffen schaffen**

Stand 12/2024: Bearbeitung noch nicht geplant

Bereits bestehende Frameworks zur Klassifizierung von Angriffen wie das MITRE ATT&CK Framework oder das Cyber Kill Chain Framework bieten sehr umfassende Informationen zu Cyberangriffen. Eine stromwirtschaftsspezifische Aufbereitung dieser Informationen kann den Zugang dazu erheblich erleichtern. Dabei können auch bereits bestehende stromwirtschaftsspezifische Informationen aufgenommen werden.

[1] Die Themen „Herausforderungen vernetzter OT-Systeme angehen“ und „Die Harmonisierung von Zertifizierungen vorantreiben“ aus der ersten Auflage der Themenroadmap (11/2023) wurden zusammengefasst, um Synergieeffekte bei diesen Themen zu nutzen.

Im Jahr 2024 wurden nach Fertigstellung der Themenroadmap die darin identifizierten Themen priorisiert und teilweise Inhalte dazu erarbeitet. Mit dieser aktualisierten Themenroadmap werden ein Überblick über die bisherige und ein Ausblick auf die zukünftige fachliche Arbeit der Branchenplattform Cybersicherheit in der Stromwirtschaft gegeben.

# Inhalt

# 1 Hintergrund

Mit der Energiewende sollen Tausende Solarzellen, Windanlagen oder Biogasanlagen auf nachhaltigerem Wege schaffen, was vorher wenige Kraftwerke geleistet haben. Das Stromnetz wird damit flexibler, aber auch komplexer. Denn diese Solarzellen und Windanlagen sind fast allesamt an das Stromnetz angeschlossen und miteinander vernetzt, um eine stabile Versorgung zu gewährleisten. Wenn die Sonne nicht scheint und die Solarzellen keinen Strom liefern, können andere Erzeuger darüber informiert werden und die fehlende Energie bereitstellen.

Diese Vernetzung und Kommunikation laufen vor allem digital. Sie beginnen bei den Erzeugern, die ihre Anlagen digital überwachen und steuern. Sie setzen sich in der Stromübertragung und -verteilung fort, wenn die jeweiligen Erzeuger sich wie oben beschrieben miteinander über die Auslastung des Stromnetzes austauschen und mit ihrem Strom handeln. Schließlich sind auch immer mehr Haushalte mit Smart Metern digital vernetzt: Die intelligenten Stromzähler können Informationen zu Stromtarifen übertragen und dementsprechend sogar den Verbrauch anpassen.

Das digital vernetzte Stromnetz, das unsere Versorgung auf der einen Seite erleichtert und flexibler macht, bringt auf der anderen Seite neue Schwachstellen mit sich: Cyberangriffe[2] auf vereinzelte Anlagen oder Systeme könnten über die breite Vernetzung vielen weiteren Akteuren Schaden zufügen und zu großflächigen Stromausfällen führen (Hecht, Langer und Smith, 2014).

Dass Cyberangriffe eine reale Bedrohung darstellen, zeigt die steigende Zahl an registrierten Vorfällen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023). Cyberangriffe werden zum Teil aus finanziellen Interessen (Erpressung durch Ransomware-Angriffe), zum Teil aus politischem Kalkül durchgeführt. Mit dem Beginn des Krieges in der Ukraine haben politische Motivationen in Europa noch einmal deutlich zugenommen.[3] Bekannt geworden ist zum Beispiel der Angriff auf den Satellitennetzbetreiber Viasat und dessen KA-Sat-Netz, infolgedessen auch in Deutschland mindestens 3.000 Windräder ausfielen.[4] Die Energiebranche erlebe seit Beginn des Krieges in der Ukraine eine neue Qualität der Cyberbedrohungen, sagte Wolfram Axtheld, Geschäftsführer des Bundesverbands Windenergie, bereits im Frühjahr 2022.[5]

Um Cyberangriffe zu verhindern und ihre Folgen abzumildern, müssen alle Akteure auf vielen Wegen zusammenarbeiten. Politische Akteure reagieren, indem sie Cybersicherheitsvorgaben für Organisationen entwickeln und verabschieden. Dabei gelten für Akteure aus dem Bereich Kritischer Infrastrukturen (KRITIS-Betreiber) besondere Anforderungen: etwa durch die NIS2- und die CER-Richtlinie, die in Deutschland aktuell mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (Inkrafttreten voraussichtlich im Frühjahr 2025) sowie dem KRITIS-Dachgesetz (Inkrafttreten voraussichtlich ebenfalls im Frühjahr 2025) umgesetzt werden. Viele weitere Stakeholder des Stromsektors (z. B. kleine Unternehmen oder IT-Dienstleister) fallen jedoch aktuell unter keine Verordnung oder werden mit den beiden Gesetzen erstmalig besondere Nachweise führen müssen.

Diese und weitere Sicherheitsvorgaben umzusetzen, bedeutet für die Akteure der Stromwirtschaft keine einmalige Anstrengung. Aufgrund sich ständig entwickelnder Software, technologischer Fortschritte, laufend

[2] Das Kunstwort *Cyber* wird im Sinne von *die Informationstechnik* bzw. *IT-Systeme betreffend* verwendet.
[3] https://news.microsoft.com/de-de/autoritaere-staaten-verstaerken-cyber-angriffe-auf-kritische-infrastrukturen/ (zuletzt besucht am 07.10.2024)
[4] https://www.spiegel.de/netzwelt/web/viasat-satellitennetzwerk-offenbar-gezielt-in-osteuropa-gehackt-a-afd98117-5c32-4946-ab8a-619f1e7af024 (zuletzt besucht am 07.10.2024)
[5] https://background.tagesspiegel.de/cybersecurity/energie-funknetz-fuer-krisenzeiten (zuletzt besucht am 07.10.2024)

neu enttarnter Schwachstellen und neu hinzukommender Systeme und Akteure ist Cybersicherheit eine Herausforderung, der es sich täglich neu zu stellen gilt. Dabei müssen die Akteure der Stromwirtschaft auch mit Dienstleistern der Digitalwirtschaft kommunizieren und sie einbinden.

Mit der Branchenplattform Cybersicherheit in der Stromwirtschaft wurde ein Format geschaffen, bei dem Akteure aus Strom- und Digitalwirtschaft beste Bedingungen vorfinden, um mit- und untereinander zu kommunizieren und gemeinsam Lösungen für mehr Sicherheit zu entwickeln. Der zum Start der Plattform initiierte Prozess zur Entwicklung einer Themenroadmap diente dazu, relevante Themen für diesen Austausch zu identifizieren. Dieser Prozess wurde im Auftrag der Deutschen Energie-Agentur (dena) mit Unterstützung der Gesellschaft für Informatik (GI) durchgeführt und mit einer Umfrage und einem darauffolgenden Workshop in hohem Grad partizipativ gestaltet (mehr zum Prozess im Anhang). Die hier vorliegende Aktualisierung berücksichtigt neue Entwicklungen und Ereignisse sowie Ergebnisse der Branchenplattform. All dies wird in den Kapiteln 3 und 4 vorgestellt. Zunächst wird aber ein Einblick in die Hintergründe und Ziele der Branchenplattform Cybersicherheit in der Stromwirtschaft gegeben.

# 2 Die Branchenplattform Cybersicherheit in der Stromwirtschaft

Die vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderte Branchenplattform Cybersicherheit in der Stromwirtschaft ist im Herbst 2022 gestartet, um zentrale Akteure der Strom- und Digitalwirtschaft in den Austausch zu bringen. Die Plattform ist ein institutionalisiertes Dialogformat. Mit und in ihr sollen die Beteiligten Wissen, Erfahrungen und Lösungsansätze teilen und gemeinsam neue Denkansätze aus dem Dialog heraus entwickeln. Die Plattform soll den teilnehmenden Partnern somit einen Rahmen bieten, durch den sie ein Verständnis für die gegenseitigen Bedürfnisse entwickeln und in dem Kooperationen und gemeinsame Entwicklungen angeregt werden. Im Idealfall machen die Partner der Plattform gemeinsam Fortschritte auf dem Weg zu einer cybersicheren und digitalen Energiewirtschaft und teilen das gewonnene Wissen mit der Fachöffentlichkeit.

Um dieses Ziel zu erreichen, bietet die Branchenplattform eine Reihe von Veranstaltungen sowie wissenschaftliche Begleitung durch Kurzgutachten. Ein fester Partnerkreis aus Akteuren bildet den Kern dieser Branchenplattform. Die Beteiligten kommen aus der Stromwirtschaft, der Digital- und Cybersicherheitswirtschaft, der Wissenschaft, Behörden, Start-ups und der dena. Es liegt ein besonderes Augenmerk darauf, auch kleinere Unternehmen zu involvieren.

Beteiligte Akteure / Organisationen (Stand 12/2024):

BayWa r.e. renewable energy GmbH

Bitkom e.V.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bundesministerium für Wirtschaft und Klimaschutz (BMWK)

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)

Bundesverband Windenergie (BWE)

Cloudflare Germany GmbH

Der Mittelstand BVMW e.V.

DKE – VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.

eco – Verband der Internetwirtschaft e.V.

EnBW Cyber Security GmbH

EnergieDock GmbH

Energiequelle GmbH

EWE NETZ GmbH

genua GmbH

intcube GmbH

KISTERS AG

Next Kraftwerke GmbH

performio GmbH

Power Plus Communications AG (PPC)

Rhebo GmbH

Rohde & Schwarz GmbH & Co. KG

SMA Solar Technology AG

solbytech GmbH

SoSafe GmbH

TEN Thüringer Energienetze GmbH & Co. KG

The Mobility House AG

Verband kommunaler Unternehmen e.V. (VKU)

Westfalen Weser Netz GmbH

**Kritische Infrastrukturen des Stromsektors**

Die Stromversorgung stellt eine **kritische Dienstleistung** dar. In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (vgl. Kapitel 3.5) wird definiert, was unter den Begriff **Kritische Infrastruktur** fällt. Dazu wird berechnet, welche Nettoleistung zu einem Stromausfall führt, der mindestens 500.000 Personen betrifft. Mit dem noch vom Bundestag zu verabschiedenden NIS2-Umsetzungsgesetz bleiben die **Schwellenwerte des BSI-Gesetzes** für KRITIS-Betreiber grundsätzlich gültig. Allerdings gelten durch das neue Gesetz neue Anforderungen für erheblich mehr Organisationen. Rund 30.000 Unternehmen werden voraussichtlich ab kommendem Jahr neu reguliert (Stand: November 2024, mehr dazu in Kapitel 3.5). Die von NIS2 betroffenen Unternehmen in Deutschland teilen sich in drei Gruppen mit unterschiedlich hohen Anforderungen auf: die bestehenden Betreiber kritischer Anlagen (KRITIS) sowie die besonders wichtigen und die wichtigen Einrichtungen.[6]

- **Zu den KRITIS-Betreibern** gehören etwa die Betreiber von Erzeugungsanlagen, Übertragungsnetzen sowie zentralen Anlagen und Systemen für den Stromhandel. Für sie gelten die bisherigen Schwellenwerte.
- **Besonders wichtige Einrichtungen** sind Unternehmen ab 250 Mitarbeiterinnen und Mitarbeitern und mit über 50 Millionen Euro Umsatz. Unternehmen, die essenzielle Dienstleistungen im KRITIS-Bereich (wie im Stromsektor) erbringen, zählen größenunabhängig zu den besonders wichtigen Einrichtungen. Das betrifft zum Beispiel digitale Dienste, die im Stromsektor unerlässlich sind, wie etwa Anbieter von SCADA-Systemen (Supervisory Control and Data Acquisition).
- **Wichtige Einrichtungen** haben mindestens 50 Mitarbeiterinnen und Mitarbeiter und über 10 Millionen Euro Umsatz.

[6] https://www.openkritis.de/it-sicherheitsgesetz/einrichtungen-unternehmensgroesse-nis2.html (zuletzt besucht am 07.01.2025)

# 3 Sieben identifizierte Handlungsfelder für die Branchenplattform

Die folgenden sieben durch den partizipativen Themenroadmap-Prozess (siehe Anhang) identifizierten Handlungsfelder decken sowohl regulatorische und organisatorische als auch technische Probleme auf, die die Stakeholder beschäftigen. Wir stellen diese Handlungsfelder jeweils vor und geben in grau hinterlegten Info-Boxen ausführlichere Hintergrundinformationen zu einzelnen Aspekten sowie zum aktuellen Bearbeitungsstand. Schließlich geben wir für die jeweiligen Handlungsfelder Empfehlungen, wie die Teilnehmer der Branchenplattform sie angehen könnten. Die Themen sind in dieser Ausgabe der Themenroadmap nach ihrer Priorität und Bearbeitungsreihenfolge sortiert.

## 3.1 Führungskräfte sensibilisieren

**Aktueller Stand:** Abgeschlossen

Das Thema „Führungskräfte sensibilisieren“ wurde am 28. Oktober 2024 mit der Veröffentlichung der Studie Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft abgeschlossen.

Ziel der Studie ist es, Geschäftsleitungen und andere Entscheidungsebenen im Stromsektor dabei zu unterstützen, Kosten, Nutzen und Rentabilität von Cybersicherheitsmaßnahmen zu bewerten. Dabei werden die Herausforderungen der unzureichenden Transparenz hinsichtlich der Kosten von IT-Sicherheitsmaßnahmen und ihren Komponenten sowie des Personalmangels adressiert. Die Studie wurde im Hinblick auf die Investitionsbedarfe erarbeitet, die aus den neuen KRITIS-Gesetzen (Referentenentwurf zum NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz)) resultieren.

Zur Veranschaulichung möglicher Investitionen wird eine IT-Sicherheitsreferenzarchitektur eines Verteilnetzbetreibers vorgestellt. Aus den resultierenden Prozessen werden implementierbare IT-Sicherheitsmaßnahmen abgeleitet, die im Rahmen von Investitionen in IT-Sicherheit umgesetzt werden können. Eine Beispielrechnung zu den finanziellen Auswirkungen von IT-Sicherheitsmaßnahmen und nachfolgenden Investitionseffekten wird anhand des Modells zum Return on Security Investment (RoSI) durchgeführt. Die Berechnung erfolgt auf Basis der im NIS2UmsuCG-Entwurf angegebenen Erfüllungsaufwände zur Implementierung der darin geforderten Maßnahmen sowie der dort abgeschätzten Schadenskosten vor und nach der Implementierung der Maßnahmen. Die Studie basiert auf den Angaben des Referentenentwurfs vom 24. Juni 2024. Nach Verabschiedung der finalen Gesetzgebung muss erneut geprüft werden, welche Bestimmungen tatsächlich umgesetzt wurden.

**Wesentliche Ergebnisse**

- In Interviews mit Unternehmensvertreterinnen und -vertretern der Energiebranche wurde durchgängig die Wichtigkeit der Geschäftsleitung in Bezug auf IT-Sicherheit betont. Auch gibt es bereits eine hohe Sensibilität der Geschäftsleitung für Investitionen in IT-Sicherheitsmaßnahmen. Die Plausibilität des im NIS2UmsuCG angegebenen Erfüllungsaufwands zur Implementierung der Maßnahmen und der abgeschätzten Schadenskosten wurde bestätigt.
- Die Bewertung der Kosten mithilfe des RoSI zeigt, dass für wichtige Einrichtungen die Investitionen bereits im ersten Jahr rentabel sind. Für besonders wichtige Einrichtungen ist dies ab dem zweiten Jahr der Fall.
- Die Beispielrechnung zeigt, dass die Investitionen, die das NIS2UmsuCG fordert, rentabel sind, trotz der für die Stromwirtschaft sehr niedrig angesetzten Kosten im Falle eines IT-Sicherheitsvorfalls.

Die Studie wurde in Zusammenarbeit mit dem Fraunhofer IOSB-AST erstellt.

Mit dem NIS2-Umsetzungsgesetz wird Cybersicherheit zur Aufgabe von Führungskräften, indem sie für Cybersicherheit offiziell verantwortlich gemacht werden. Spätestens ab dem Inkrafttreten des Gesetzes (voraussichtlich im Frühjahr 2025) sollten Führungskräfte also motivierter sein, Cybersicherheit bestmöglich in ihrer Organisation umzusetzen.

Dass diese Motivation bisher nicht hoch genug ist, zeigt sich etwa daran, wie viel Budget KRITIS-Betreiber für IT-Sicherheit veranschlagen: In der Europäischen Union investieren sie im Schnitt 41 Prozent weniger als vergleichbare Unternehmen in den USA. Insgesamt gibt es große Differenzen in den Unternehmensbudgets für Cybersicherheit, wobei vor allem kleine und mittlere Unternehmen meist viel zu wenig investieren.[7] Damit korrespondierend zeigte sich in der von uns durchgeführten Umfrage, dass es große Unterschiede bei der Durchsetzung grundlegender Sicherheitsvorkehrungen gibt.

Eine wichtige Ursache für die zu geringen Budgets und eine damit korrelierende unzureichende Umsetzung von Cybersicherheit liegt darin, dass sich noch zu wenige Führungskräfte der Brisanz des Themas Cybersicherheit bewusst sind: Viele Budgetverantwortliche erkennen nicht die Notwendigkeit, mehr in IT-Sicherheit zu investieren, wenn bisher alles gut gegangen ist. Dies hat wiederum zur Folge, dass Cyberkriminelle immer wieder erfolgreich sind.

Da der Stromsektor eine Kritische Infrastruktur darstellt, müssen viele Unternehmen der Stromwirtschaft zwar vermehrt Anforderungen erfüllen. So müssen KRITIS-Betreiber alle zwei Jahre eine „nach dem Stand der Technik“ umgesetzte Sicherheitsstrategie nachweisen (vgl. Kapitel 3.4). Da quasi täglich neue Technologien entwickelt und Schwachstellen gefunden werden, ist es jedoch wichtig, Cybersicherheit auch tagtäglich ernsthaft zu verfolgen und umzusetzen. Dass Sicherheit nie zu hundert Prozent erreicht werden kann, mag viele frustrieren. Es ist deshalb aber umso wichtiger, Führungskräfte dafür zu sensibilisieren.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, die Sensibilisierung von Führungskräften weiter voranzubringen:

- Menschen werden stärker für ein Thema sensibilisiert, wenn sie es weniger abstrakt, dafür aber persönlicher wahrnehmen. Leider zeigt sich immer wieder, dass vor allem Unternehmen, die erfolgreich angegriffen wurden, intensiver in Cybersicherheit investieren. Die Branchenplattform bietet die Möglichkeit des persönlichen Austauschs und kann sie nutzen, um Beteiligten die Folgen eines Cyberangriffs aus ihrer persönlichen Perspektive zu verdeutlichen und damit für die Relevanz einer gut etablierten Cybersicherheit zu sensibilisieren.
- Man kann Führungskräfte nicht nur mit Negativszenarien sensibilisieren, sondern auch die Vorteile von Cybersicherheit für ihr Unternehmen herausstreichen. Dies hat den Vorteil, Cybersicherheit weniger als Last und mehr als positiv besetzten Erfolgsfaktor zu etablieren. Tatsächlich gibt es Hinweise, dass Investitionen in Sicherheit nicht nur Unternehmensbeziehungen stärken, sondern auch zu einem höheren Umsatz führen können. Grund dafür ist einerseits, dass immer mehr Unternehmen in der Zusammenarbeit eine starke Cybersicherheit erfragen. Andererseits erleichtert ein großes Know-how zu Cybersicherheit Investitionen in die Digitalisierung und Vernetzung (Trend Micro, 2023). Dementsprechend bietet es sich an, mit der Branchenplattform stromwirtschaftsspezifische Vorteile von Investitionen in Cybersicherheit zu erarbeiten und zu verbreiten. Dabei kann etwa Bezug zur zunehmenden Vernetzung von OT-Systemen genommen werden (vgl. Kapitel 3.3).
- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Oktober 2023 die neue Publikationsreihe Management Blitzlicht gestartet. Mit ihr wird explizit die Führungsetage von Unternehmen adressiert, um sie schnell und kompakt über aktuelle Themen der Cybersicherheit zu informieren. Ein ähnliches Format mit stromwirtschaftsspezifischen Themen könnte die Branchenplattform aufsetzen.

[7] https://background.tagesspiegel.de/cybersecurity/bei-cybersicherheit-gibt-es-keinen-koenigsweg (zuletzt besucht am 06.01.2025)

## 3.2 Gemeinsam aus Cyberattacken lernen

**Aktueller Stand:** In Bearbeitung

Das Zielbild dieses Themas wurde in mehreren Sitzungen der Branchenplattform diskutiert und geschärft. Es wurde deutlich, dass es eines interdisziplinären Ansatzes zum gemeinsamen Lernen aus Cyberattacken bedarf, der die bestehenden Angebote anderer Anbieter sinnvoll ergänzt und zu einer Weiterentwicklung dieser Formate beiträgt. Mit dieser Zielstellung wurde die Bearbeitung des Themenmoduls im Oktober beauftragt:

Es sollen in einer Hintergrundanalyse Grundlagen der Psychologie und weiterer relevanter Disziplinen (z.B. Pädagogik, Kommunikation, Risikomanagement oder verwandte Fachgebiete) zur Wissensvermittlung von abstrakten und komplexen Themen anhand des Beispiels von Cyberangriffen auf das Energiesystem aufbereitet werden. Dabei soll insbesondere auf die Voraussetzungen für die Bereitschaft zum „gemeinsamen Lernen“ im Sinne positiver Effekte und negativer Effekte (z. B. Sorge vor Imageschäden beim öffentlichen Teilen von Erfahrungen aus einem Cyberangriff, Schweigepflichten durch Auflagen von Versicherungen oder aufgrund der Regulatorik) sowohl für diejenigen, die ihre Erfahrungen teilen, als auch für die Adressaten eingegangen werden. Daraus soll ein interdisziplinärer Ansatz zum gemeinsamen Lernen bzw. zur Herstellung eines vertrauensvollen Lernumfelds in Bezug auf Erfahrungen aus Cyberangriffen entwickelt und es sollen geeignete Formate (z.B. Veranstaltungen, (digitale) Plattformen, Medien) zur Umsetzung dieses Ansatzes identifiziert werden.

Der entwickelte Ansatz soll auf das Format einer Veranstaltung mit Erfahrungsberichten von angegriffenen Unternehmen aus der Energiewirtschaft angewendet werden, deren Durchführung begleitet werden soll. Im Idealfall sollten aus dem Ansatz bereits die Rahmenbedingungen für die Veranstaltung (z.B. Größe, Vertraulichkeit, Zielgruppe etc.) abgeleitet werden können. Im Anschluss soll durch geeignete Methoden die Effektivität dieses Ansatzes quantifiziert und es sollen konkrete Handlungsempfehlungen für verschiedene Stakeholder formuliert werden.

Die Veranstaltung soll Anfang Februar 2025 stattfinden. Der Ergebnisbericht wird Mitte 2025 veröffentlicht.

Dieses Themenmodul wird gemeinsam mit einem Konsortium aus der Gesellschaft für Informatik e.V., Cyber Policy Haus BV und Prof. Dr. Stefan Sütterlin bearbeitet.

Ein Ziel der Branchenplattform ist es, den Austausch zwischen den Akteuren der Strom- und Digitalwirtschaft voranzubringen. Besonders wichtig ist ein solcher Austausch über Themen, zu denen Akteure bisher wenig auskunftsfreudig sind, nämlich zu eigenen Cybersicherheitsstrategien und Erfahrungen mit Cyberangriffen.

Bisher gibt es nur wenige Unternehmen, die sich von sich aus öffentlich zu Cyberangriffen auf ihre Organisation äußern. Grund dafür ist vor allem die Furcht vor einem Reputationsverlust.[8] Diese Furcht könnte etwa daher rühren, dass laut einer Umfrage die Mehrheit deutscher Unternehmen nicht mehr mit einem Unternehmen zusammenarbeiten wollen würde, bei dem es schon einmal zu einem Cyberangriff gekommen ist.[9]

[8] https://background.tagesspiegel.de/cybersecurity/schweigen-ist-gold (zuletzt besucht am 11.10.2024)
[9] https://background.tagesspiegel.de/cybersecurity/unternehmen-scheuen-zusammenarbeit-nach-cyberangriff (zuletzt besucht am 11.10.2024)

Andererseits halten mindestens genauso viele Unternehmen es für richtig, transparent mit Cyberangriffen umzugehen.[10] Auch Expertinnen und Experten empfehlen immer wieder Transparenz statt Geheimhaltung.[11]

Die Branchenplattform bietet eine außergewöhnliche Chance, einen Rahmen zu schaffen, in dem sich verschiedene Stakeholder vertrauensvoll und (noch) nicht öffentlich zu ihren Cybersicherheitsstrategien und Erfahrungen mit Angriffen austauschen können. Je offener dieser Austausch ist, desto mehr Lernpotenzial ergibt sich für die Beteiligten.[12] Im besten Fall etabliert sich ein bleibendes Vertrauensverhältnis, mit dem sich ein andauernder Austausch zu diesen momentan meist noch geheim gehaltenen Vorfällen etabliert, von dem alle profitieren.

Es gibt Strukturen, mit denen sich Stakeholder gegenseitig über Gefahren informieren und diesbezüglich Strategien entwickeln können, um im Idealfall Cyberangriffe abzuwehren oder kürzere Reaktionszeiten zu gewährleisten. Momentan werden dafür vermehrt nicht nur von einzelnen Unternehmen, sondern auch auf politischer Ebene breit vernetzte Security Operations Center (SOC) aufgebaut (z. B. in Berlin[13] oder geplant auf EU-Ebene[14]). Die Aufgabe von SOC ist es, Daten über Cybersicherheitsangriffe und -alarme zu sammeln, zu analysieren, nach ihrer Kritikalität zu bewerten und zu kommunizieren. Ähnlich, aber proaktiv statt reaktiv agieren in vielen großen Unternehmen etablierte Strukturen im Sinne eines Cyber Defense Center (CDC).[15] Die Mitarbeiterinnen und Mitarbeiter von CDC schauen nicht nur auf die internen Systeme, sondern überwachen permanent die allgemeine Bedrohungslage (z. B. neue Angriffsvektoren oder Zero-Day Vulnerabilities), um identifizierte Risiken proaktiv zu melden und möglichen Angriffen zuvorzukommen.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, den Austausch voranzubringen:

- Ein interner Erfahrungsaustausch zu Cyberangriffen sollte gut vorbereitet werden. Wichtig ist, ein gemeinsames Verständnis für das Ziel des Austauschs zu schaffen. Es sollte allen Beteiligten bewusst sein, dass es nicht um eine Bewertung von Ereignissen und Handlungen, sondern um das daraus entstehende Lernpotenzial geht. Da Vertrauen die Basis für den Austausch ist, sollten sich die Beteiligten im besten Fall bereits gut kennen.
- Wichtig ist die Nachhaltigkeit des Voneinanderlernens. Eine allgemeine Awareness auf der Managementebene eines Unternehmens bedeutet nicht, dass dieses Unternehmen Cybersicherheitsmaßnahmen tatsächlich einführt und umsetzt – und dass auch seine Mitarbeiterinnen und Mitarbeiter dies tun. Für die Etablierung einer tatsächlichen Cybersicherheitskultur braucht es mitunter eine individuelle Ansprache und niedrigschwellige Angebote. Mitglieder der Branchenplattform könnten sich darüber austauschen oder sie evaluieren.
- Auf der Branchenplattform kann darüber diskutiert werden, welche Vorteile es bringt, eine Cyberattacke zu melden und öffentlich zu machen. Die Branchenplattform kann die Möglichkeit bieten, Erfahrungen von Teilnehmern zusammenzufassen und anonymisiert oder nicht anonymisiert zu veröffentlichen.
- Es gibt eine Vielzahl von Leitfäden dazu, wie man sich nach einer Cyberattacke am besten verhält, zum Beispiel den Erste-Hilfe-Leitfaden des BSI. Solche Leitfäden können als Grundlage dienen, um eigene Kontexte und Erfahrungen zu reflektieren und sich darüber auszutauschen (vgl. Kapitel 3.6)

[10] https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2023.html (zuletzt besucht am 11.10.2024)
[11] Zum Beispiel https://background.tagesspiegel.de/cybersecurity/mit-transparenz-erreichen-unternehmen-mehr-als-mit-verschleierungstaktik (zuletzt besucht am 11.10.2024)
[12] https://background.tagesspiegel.de/cybersecurity/cyberangriffe-zwei-unternehmen-berichten (zuletzt besucht am 11.10.2024)
[13] https://www.itdz-berlin.de/aktuelles/franziska-giffey-eroeffnet-security-operations-center-im-itdz-berlin-1196292.php (zuletzt besucht am 11.10.2024)
[14] https://ec.europa.eu/newsroom/dae/redirection/document/95049 (zuletzt besucht am 11.10.2024)
[15] https://background.tagesspiegel.de/cybersecurity/proaktiver-schutz-mit-einem-cyber-defense-center(zuletzt besucht am 11.10.2024)

- Mit der Branchenplattform können Informationen zu bestehenden und geplanten SOC und CDC gesammelt und mit den Bedarfen der Stakeholder abgeglichen werden. Sollten bestehende Strukturen nicht ausreichen, können erste Schritte unternommen werden, um ein SOC oder CDC für die Branche zu konzeptionieren. Dabei können Synergien womöglich zu einer branchenspezifischen Wissensbasis hergestellt werden (vgl. Kapitel 3.7)

## 3.3 Herausforderungen vernetzter OT-Systeme angehen

**Aktueller Stand:** In Bearbeitung

Das Thema „Herausforderungen vernetzter OT-Systeme angehen“ wurde auf dem 2. Forum Cybersicherheit in der Stromwirtschaft der Branchenplattform im September 2024 diskutiert. Auf Basis dessen wurde dieses Thema mit dem Thema „Die Harmonisierung von Zertifizierungen vorantreiben“ (vgl. Kapitel 3.4) kombiniert und mit dem Titel „Harmonisierung von Zertifizierungen und vernetzter OT-Systeme im Cybersicherheitsbereich**“** versehen. Im November 2024 wurde ein Workshop mit ausgewählten Partnern der Branchenplattform durchgeführt, um die Zielsetzung dieses kombinierten Themenmoduls zu schärfen. Daraus abgeleitet wurde hierzu die Erstellung einer Studie ausgeschrieben. Die Studie besteht aus zwei Teilen: Der erste Teil dient der Erstellung einer Übersicht zu den geltenden Zertifizierungen im Cybersicherheitskontext für einen ausgewählten Bereich der Energiebranche. Basierend auf dieser Übersicht soll eine Bewertung hinsichtlich der Harmonisierungspotenziale erfolgen. Der zweite Teil der Studie fokussiert sich auf die Untersuchung einer Problemstellung im Kontext der zunehmenden Vernetzung von OT und IT in KRITIS-Unternehmen. Ziel ist die Aufarbeitung dieses Themas für ein besseres Problemverständnis sowie das Ableiten von Handlungsbedarfen.

Die Digitalisierung im Energiesektor verbindet auch zunehmend IT[16]- mit OT-Komponenten[17]. Deren **Digitalisierung und Vernetzung** können unternehmerische Vorteile und eine größere Flexibilität hervorbringen. Beispielsweise können Daten aus der OT genutzt werden, um zu entscheiden, wann eine Wartung erforderlich ist, und zeitgenaue Überwachungen von Systemen werden unproblematischer. OT-Systeme können auch über Schnittstellen zu anderen Systemen verfügen, um etwa zu evaluieren, wie sich Schalthandlungen auf Stromleitungen oder Transformatoren auswirken (Haug, Spath und Hatt, 2021).

Die Vielzahl an Optionen, die sich aus vernetzten OT-Systemen ergeben, sind mit weiteren technischen Möglichkeiten, politischen Vorhaben und sicherheitskritischen Herausforderungen verbunden. Dazu gehören die Sektorenkopplung, die Energiewende und die Zunahme an kleinen Energieerzeugern. Über die in diesem Zusammenhang relevanten Themen geben wir in der grau hinterlegten Box einen Überblick.

[16] IT = Informational Technology; Hardware und Software zur elektronischen Datenverarbeitung (z. B. die Speicherung, Übertragung und Verwendung von digitalen Informationen für Zwecke des Geschäftsbetriebs)
[17] OT = Operational Technology; Hardware und Software zur Steuerung und Kontrolle von physischen Prozessen und Geräten (wie z. B. Anlagen)

**Vernetzte OT-Systeme im Hinblick auf aktuelle Vorhaben und Herausforderungen**

Vernetzte OT-Systeme bilden die technische Grundlage für die Umsetzung der **Sektorenkopplung**. Der Grundgedanke von Sektorenkopplung besteht darin, durch einen holistischen Ansatz das gesamte Energiesystem zu dekarbonisieren, indem beispielsweise große Teile der Energieverbraucher elektrifiziert und durch intelligentes Lastmanagement dringend benötigte Flexibilitäten für den Stromsektor angeboten werden.

Da Windstärken oder Sonnenstunden stark schwanken und die Produktion **erneuerbarer Energien** daher nur begrenzt koordiniert werden kann, ist Sektorenkopplung im Rahmen der Energiewende dementsprechend ein Schlüsselkonzept, um produzierte und überschüssige Energie effizienter zu nutzen. Die Sektorenkopplung nimmt damit eine wichtige Rolle dabei ein, Klimaschutzziele zu erreichen (Wietschel et al., 2018).

Mit der Sektorenkopplung stehen **intelligente Energiesysteme** eng in Verbindung. Denn mit der Vernetzung der OT-Systeme wird oft auch deren Digitalisierung, also der Anschluss von Anlagen und Geräten an das Internet, vorangetrieben. Intelligente Energiesysteme (Smart Grids) nutzen dies zum Beispiel dafür, dass eine Waschmaschine erst dann angeschaltet wird, wenn ein Energieüberschuss besteht. Mittels digitaler Vernetzung können die Systeme Informationen zu Preisen, Verfügbarkeiten, Netzauslastungen und Energiebedarf verarbeiten und darauf basierende Entscheidungen treffen.

Mit der Sektorenkopplung wächst das Netzwerk miteinander verbundener Systeme, zu dem neuerdings neben großen und kleinen Anlagen auch immer mehr intelligente Endgeräte zählen. Eine solche Komplexitätszunahme ist eine der größten Herausforderungen für die Sicherheit. Es vergrößern sich mögliche Angriffsflächen für **Cyberattacken**, da neue zu schützende Verbindungen und Knotenpunkte entstehen.

**Die Sicherheit der Verbindungen** zwischen den Systemen und Anlagen (bzw. Endgeräten), also die Sicherheit der Gateways, umfasst vor allem eine abgesicherte Kommunikation zwischen verschiedenen Systemen. Sie muss entsprechend unterschiedliche Standards und Systemsprachen berücksichtigen. Durch eine unzureichende Sicherheit der Gateways könnten Angreifer zum Beispiel mittels eines DDoS-Angriffs (Distributed Denial of Service) Steuerungsbefehle im Netz blockieren oder falsche Informationen an sie senden. Damit könnte die Energieversorgung gestört oder unterbrochen werden.

**Datenräume** bieten hier das Potenzial, die Sicherheit der Kommunikation zu verbessern. Sie verschaffen berechtigten Akteuren Zugang zu OT-Daten und ermöglichen eine Verknüpfung mit weiteren Datenräumen und deren Kontrolle (Reiberg, Niebel und Kraemer, 2022). Sie können die IT-Sicherheit erhöhen, indem die Datenströme zentralisiert überwacht und verschlüsselt werden. (Basis hierfür ist natürlich die Erfüllung hoher IT-Sicherheitsanforderungen.)

Weiterhin könnten Datenräume dazu beitragen, aktuelle Daten von Verbrauchern, Erzeugern und Speicheranlagen miteinander zu verknüpfen und zu analysieren. Dies wäre hilfreich, um etwa die Energieeffizienz zu steigern sowie Energieüberschüsse und -mangel schneller und besser abschätzen zu können und entsprechend zu reagieren. Durch die zunehmende Zahl an Kleinanlagen würden Datenräume den Überblick über die aktuelle Stromerzeugung und aktuelle Stromverbräuche voraussichtlich deutlich erleichtern. Datenräume sind damit auch eine mögliche Basis für die sichere Einbindung von weiteren Endgeräten wie Smart Metern, da deren Daten auf einer solchen Plattform sicher gespeichert und verarbeitet werden könnten.

Auch die **Sicherheit der Endgeräte** für das gesamte Energiesystem und damit der Knotenpunkte selbst ist nicht zu vernachlässigen. Zu ihnen zählen neben den Smart Metern etwa die Smart-Home-Endgeräte. Horák and Huraj (2019) beschreiben eindrücklich, wie smarte Thermostate Ziel von DDoS-Angriffen werden können: Diese Angriffe könnten die Thermostate so manipulieren, dass sie eine tiefere Temperatur vortäuschen als in Wirklichkeit herrscht. Dies bewirkt, dass Heizungen unnötig hochgefahren werden. Im schlimmsten Fall hätte dies nicht nur eine lokale Auswirkung auf den Verbrauch und die Temperatur, sondern würde auch Marktpreise manipulieren.

Voraussetzung für intelligente Energiesysteme ist eine weite Verbreitung von **Smart Metern**. Denn Smart Meter ermöglichen es, Informationen von einer Vielzahl kleinerer Systeme über deren Energieverbrauch und -produktion mit einem Zeitstempel von fern auszulesen. Die Verbreitung von Smart Metern liegt in Deutschland zurzeit jedoch noch im unteren einstelligen Prozentbereich, während sie in Nachbarstaaten wie Dänemark bei fast 100 Prozent.[18] Angesichts der politischen Bestrebungen in Deutschland (wie dem Smart-Meter-Gesetz (Gesetz zum Neustart der Digitalisierung der Energiewende) von 2023) sind mittelfristig jedoch ihre stärkere Verbreitung und damit eine Zunahme der beschriebenen Gefahr absehbar.

Aus den Eigenheiten von OT-Systemen sowie ihrer Digitalisierung und Vernetzung ergeben sich bezüglich der Cybersicherheit zahlreiche Herausforderungen.

- **Lange Lebensdauer:** Viele OT-Systeme und ihre Komponenten sind bereits seit vielen Jahren oder sogar seit Jahrzehnten in Betrieb. Ursprünglich war ihre Vernetzung nicht vorgesehen. Es handelte sich um abgekapselte Systeme, die sicherheitstechnisch bisher eher irrelevant waren. Die Beschäftigung mit ihrer Sicherheit ist also vergleichsweise neu.

  Die OT-Systeme sind oft nicht nur schon lange in Betrieb, sie haben auch weiterhin eine hohe Lebenserwartung: 30 bis 50 Jahre Betrieb sind keine Seltenheit (Petersen, Stock und Federrath, 2023). Geeignete Sicherheitsmaßnahmen müssen daher veraltete, nicht leicht zu ersetzende, verwundbare und

[18] https://iot-analytics.com/smart-meter-adoption/ (zuletzt besucht am 07.01.2025)

teilweise nicht mehr updatebare Systeme schützen. Viele Hersteller von OT-Systemen existieren zudem nicht mehr, sodass bestimmte Informationen nicht mehr erfragt werden können.

Die lange Lebensdauer von OT-Systemen steht damit im Konflikt mit einer vergleichsweise kurzen Lebensdauer von IT, die etwa fünf Jahre beträgt. Die Laufzeit der Anlagen und der Supportzeitraum der Hersteller decken sich nicht.

Wenn die Sicherheit von OT-Systemen aufgrund veralteter Software nicht mehr gewährleistet werden kann, müssten sie ausgetauscht werden. Dies verursacht enorme Kosten. Auch die Sicherung alter OT-Systeme mit aktueller Technik ist nicht wirtschaftlich.

- **Kaum oder unterschiedliche Standards:** Die OT-Systeme laufen meist mit jeweils eigenen, sehr verschiedenen proprietären Systemen. Standard-Sicherheitslösungen sind für sie nicht brauchbar. Es müssen jeweils spezielle Lösungen gefunden werden. Sind Standards vorhanden, so unterscheiden sie sich je nach Sektor, was die Gewährleistung der Sicherheit der Verbindung dieser Systeme erschwert.
- **Risiko beim Nachrüsten:** Hersteller von OT-Systemen geben eine Gewährleistung. Sie erlischt jedoch, wenn Komponenten ausgetauscht werden oder die Hardware mit neuer Software ausgerüstet wird.
- **Konstante Erreichbarkeit:** Manche OT-Systeme (wie industrielle Steuerungsanlagen) müssen während der Durchführung von Updates mindestens teilweise erreichbar bleiben, damit das Energiesystem in einem operativen Zustand bleibt (Petersen, Stock und Federrath, 2023). Dies erschwert es, die Systeme sicher zu halten.
- **Wachsende Netzwerke**: Die Verbreitung intelligenter Energiesysteme und der damit zusammenhängende Anschluss von IoT-Endgeräten an das Stromnetz bieten neue Angriffsflächen, die sowohl lokale als auch systemübergreifende Auswirkungen haben können.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, die Herausforderungen vernetzter OT-Systeme weiter zu bearbeiten:

- Mit der Branchenplattform könnten Best-Practice-Ansätze für die Vernetzung und die Sicherung spezifischer Systeme gesammelt werden, um somit Erfahrungen zu teilen.
- Es können konkrete Vorschläge erarbeitet werden, um den BSI-Grundschutz OT-spezifisch zu erweitern. Hier bietet es sich auch an, sich mit der Bundesnetzagentur (BNetzA) auszutauschen, die für die Sicherheitsanforderungen von Energieanlagen zuständig ist (vgl. Kapitel 3.4).
- Da die Beschäftigung mit OT-Sicherheit noch vergleichsweise neu ist, könnte die Branchenplattform Unternehmen dazu ermutigen, einen positiven kulturellen Umgang mit OT-Sicherheit zu etablieren. Hierbei könnten zum Beispiel Anreize erarbeitet werden, Sicherheitslücken in OT-Systemen zu identifizieren und zu melden und somit einen transparenteren Umgang damit zu schaffen.

Dieses Thema ist eng verwandt mit dem Thema „Die Harmonisierung von Zertifizierungen vorantreiben“ und wird daher aktuell in einem gemeinsamen Themenmodul bearbeitet.

## 3.4 Die Harmonisierung von Zertifizierungen vorantreiben

**Aktueller Stand:** In Bearbeitung

Das Thema „Die Harmonisierung von Zertifizierung vorantreiben“ wurde mit dem Thema „Herausforderungen vernetzter OT-Systeme angehen“ kombiniert und befindet sich derzeit in Bearbeitung. Für mehr Informationen siehe Kapitel 3.3.

Die Gesetzgebung gibt Betreibern Kritischer Infrastrukturen vor, welche Sicherheitsanforderungen sie zu erfüllen haben (vgl. Kapitel 3.5). Diese Anforderungen müssen nicht nur umgesetzt, sondern ihre Erfüllung muss auch nachgewiesen werden.

Zertifizierungen ermöglichen es Unternehmen, durch unabhängige Prüfung nachzuweisen, dass sie die Anforderungen erfüllen. Da das BSI offenlässt, wie diese Nachweise konkret aussehen können, gibt es verschiedene Nachweisverfahren, die sich nach etablierten internationalen Standards (ISO/IEC) richten. Teilweise sind die Verfahren den unterschiedlichen Anforderungen an Branchen und Organisationen geschuldet, zu einem großen Teil dürften Vereinheitlichungen aber unproblematisch sein.[19]

Die bestehende Komplexität bei Zertifikaten und Nachweisverfahren führt zu einem hohen Aufwand dafür, die passenden Formate herauszusuchen und zu vergleichen. So gibt es beispielsweise ein Mapping der Plattform „OpenKRITIS“, das fünf verschiedene Standards mit 100 KRITIS-Anforderungen abgleicht. Bei diesem Mapping zeigt sich, dass die Standards diese Anforderungen teils nicht, teils in mehreren Unterkapiteln thematisieren.[20] Auch die Beteiligten des Themenroadmap-Prozesses gaben an, dass sie nicht alle zu erbringenden Nachweise für notwendig halten, und beklagten den damit verbundenen großen, nicht immer zielführenden Aufwand.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, das Thema Zertifizierungen und ihre Harmonisierung weiter zu bearbeiten:

- Für die Teilnehmer der Branchenplattform dürfte es besonders interessant sein, sich über Änderungen auszutauschen, die mit dem NIS2-Umsetzungsgesetz auf sie zukommen. Hierbei können insbesondere Unternehmen, die bisher noch keine derartigen Nachweispflichten erbringen mussten, von diesbezüglich erfahrenen Unternehmen profitieren.
- Die Beteiligten könnten konkrete Vorschläge diskutieren, wie Zertifizierungen vereinheitlicht bzw. harmonisiert werden sollten.
  - Dafür könnten in einem ersten Schritt gemeinsam Ideen gesammelt werden. Diese Diskussion sollte lösungsorientiert moderiert werden, um die eventuell vorhandene Frustration über hohe Aufwände abzufangen. Ein möglicher Weg dafür könnte sein, zunächst gemeinsam nachzuvollziehen, mit welchem Hintergrund verschiedene Sicherheitsanforderungen entstehen und entstanden sind.

[19] https://background.tagesspiegel.de/cybersecurity/wie-wirksam-sind-die-it-sicherheitsgesetze (zuletzt besucht am 11.10.2024)
[20] https://www.openkritis.de/r/OpenKRITIS_Mapping_KRITIS-Cyber-Security.pdf (zuletzt besucht am 11.10.2024)

- In einem zweiten Schritt könnten mit der Branchenplattform Möglichkeiten aufgezeigt und vermittelt werden, über die sich die Akteure aktiv mit ihren Vorschlägen einbringen können. Beispielsweise ruft die European Union Agency for Cybersecurity (ENISA) regelmäßig mit „Calls for Participation“ dazu auf, dass sich Akteure aktiv mit Vorschlägen dazu einbringen, wie Cybersicherheitszertifikate entwickelt und durchgesetzt werden sollen.

**IT-Sicherheitsnachweise im Stromsektor**

Mit einer ISO-27001-Zertifizierung weist eine Organisation einen **allgemeinen IT-Grundschutz** nach. Dieses Zertifikat ist weit verbreitet und international anerkannt. Für KRITIS-Betreiber ist diese Zertifizierung jedoch nicht ausreichend. Der § 8a des BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) verlangt von KRITIS-Betreibern weitere Nachweise. Der Grund ist, dass bei der ISO-27001-Norm bestimmte Risiken akzeptiert werden, wenn sie keine größere Gefahr für das Unternehmen darstellen. Das aber ist für KRITIS-Betreiber inakzeptabel, denn entscheidend sind hier die Risiken für die versorgten Personen – und nicht die nur für das Unternehmen.

**Für KRITIS-Betreiber** bedeutet das, dass sie nach internen Audits oder Zertifizierungen die Maßnahmen von unabhängigen Prüfstellen in einem eigenen Prüfbericht bestätigen lassen müssen. Dabei muss nachgewiesen werden, dass die IT-Sicherheitsvorkehrungen dem „Stand der Technik“ entsprechen (BSIG). Dieser Nachweis ist seit 2018 alle zwei Jahre zu erbringen. Allerdings macht das BSI keine genauen Vorschriften darüber, wie dieser Nachweis konkret auszusehen hat, es gibt lediglich die Art der einzureichenden Unterlagen vor. Dementsprechend haben sich viele verschiedene Standards etabliert (eine Übersicht findet sich hier: https://www.openkritis.de/massnahmen/kritis-security-standards.html). Unternehmen eines jeweiligen Sektors können außerdem gemeinsam einen branchenspezifischen Sicherheitsstandard (B3S) erarbeiten und ihn vom BSI als Stand der Technik absegnen lassen.

Für **Betreiber von Energieversorgungsnetzen und Energieanlagen** gibt es jedoch eine Sonderregel: Für sie hat die Bundesnetzagentur (BNetzA) im Auftrag des BSI den IT-Sicherheitskatalog für Betreiber von Energieanlagen erstellt. Seit dem 1. Mai 2023 sind sie (gemäß IT-Sicherheitsgesetz 2.0) zudem auch verpflichtet, ein System zur Angriffserkennung zu etablieren, es prüfen zu lassen und einen entsprechenden Nachweis vorzulegen. Hierzu hat das BSI 2022 eine Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung erstellt.

Mit der EU-NIS2-Umsetzung und dem KRITIS-Dachgesetz (vgl. Kapitel 3.5) werden sich die Nachweispflichten betroffener Unternehmen ändern und vor allem viele Organisationen neu zu solchen Nachweisen verpflichtet werden. Die bisherigen Pflichten aus dem BSI-Gesetz bleiben in Grundzügen erhalten, werden jedoch teils präzisiert, teils verschärft und neu strukturiert. Ein von OpenKRITIS bereitgestelltes Mapping von NIS2 auf die ISO 27001 gibt einen guten Überblick über die zu erwartenden Vorgaben.

Abgesehen davon gibt es **eigene Industriestandards und Zertifizierungsprozesse für bestimmte Komponenten oder Produkte**. So regelt das im Mai 2023 verabschiedete Gesetz zum Neustart der Digitalisierung der Energiewende, dass das BSI für die Standardisierung der Cybersicherheit von Smart Meter Gateways verantwortlich ist. Gesonderte Standards gelten etwa für Steuereinheiten, Ladeeinrichtungen, Wärmepumpen oder energiewirtschaftliche Prozesse.

## 3.5 Transparenz in der Gesetzgebung erhöhen

**Aktueller Stand:** In Bearbeitung

Im Januar 2024 fand im Rahmen der Branchenplattform ein Online-Workshop zum NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) und seine Auswirkungen auf den Stromsektor statt. Die Teilnehmer bekamen Einblicke in die Arbeit des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) und der Bundesnetzagentur (BnetzA) sowie in die Auswirkungen des NIS2UmsuCG auf Unternehmen in der Stromwirtschaft. Sowohl für erfahrenere als auch für kleinere Unternehmen, die nun von den neuen Maßnahmen betroffen sein werden, ist eine Klärung der Umsetzung verschiedener Aspekte der Verordnung erforderlich.

Aufgrund der verspäteten Verabschiedung des Gesetzes wurde dieses Themenmodul auf 2025 verschoben. Voraussichtlich wird seine Bearbeitung im ersten Quartal 2025 ausgeschrieben und bis Mitte 2025 abgeschlossen werden.

Regularien beinhalten für Betreiber Kritischer Infrastrukturen (wie die Stromwirtschaft) die Anforderungen an ihre Cybersicherheit. Mit ihnen sollen klare Regelungsziele und entsprechende Maßnahmen kommuniziert werden. Da Cybersicherheit ein aktuelles und relevantes Thema ist, nehmen sich politische Akteure ihm vermehrt an. Außerdem existiert eine Vielzahl von Organisationen, die Gesetze und Handlungsempfehlungen erarbeiten, Informationen bereitstellen oder einen Erfahrungsaustausch zu Cybersicherheit anregen. Zurzeit sind mehr als 80 Akteure Teil des nationalen Ökosystems zur Cybersicherheit, darunter Ministerien, Behörden und Plattformen (Herpig und Dutke, 2023).

So viele Akteure und damit verbundene Papiere tragen zu einer komplexen Gesetzeslage bei. So sprach Manuel Atug, Gründer und Sprecher der AG KRITIS, bei der Ausschusssitzung zu Cybersicherheit Anfang 2023 von „zu viele[n] Akteure[n]“ und „ineffektive[n] Gesetze[n]“[21]. Für die Umsetzung der NIS2-Richtlinie sowie der CER-Richtlinie wünschen sich Betroffene auch nach Verbesserungen auf Grundlage von Anhörungen noch immer Harmonisierungen mit anderen Gesetzen, um etwa eine Doppelregulierung zu vermeiden.[22] Diesen Wunsch teilen auch am Themenroadmap-Prozess Beteiligte. Darüber hinaus sprachen sie an, dass Anforderungen stärker betriebliche Kontexte berücksichtigen müssten, damit sie umsetzbar bleiben. Auch wenn politische Akteure Sicherheit mit hohen Anforderungen durchsetzen wollen: Cybersicherheit lässt sich nicht allein auf dem Papier herstellen (vgl. Kipker, 2023). Eine zu hohe Komplexität, zu wenig Transparenz und ein zu geringer Praxisbezug gefährden die Akzeptanz von Vorschriften.

[21] https://www.bundestag.de/resource/blob/984658/767a3abc17eed5a9eae39377204dc052/27-Sitzungsprotokoll-mit-Anlagen-OeA.pdf (zuletzt besucht am 06.11.2024)
[22] https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/streit-um-schwellenwerte (zuletzt besucht am 14.10.2024)

**Gesetzgebung in Deutschland und Europa**

**In der deutschen Gesetzgebung** bildet aktuell das Gesetz über das Bundesamt Sicherheit in der Informationstechnik (BSI-Gesetz, BSIG) für Kritische Infrastrukturen und ihre Betreiber die Rechtsgrundlage. In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz werden die einzelnen Sektoren (wie der Stromsektor) näher beschrieben und Schwellenwerte aufgeführt, um Betreiber Kritischer Infrastrukturen zu definieren. Diese Verordnung wurde zuletzt 2023 novelliert und wird voraussichtlich 2025 durch das NIS2-Umsetzungsgesetz erweitert.

Das IT-Sicherheitsgesetz (2015) erweiterte das BSIG zuerst. Es schreibt unter anderem fest, dass KRITIS-Betreiber IT-Sicherheit nach dem „Stand der Technik" umzusetzen haben und erhebliche IT-Sicherheitsvorfälle an das BSI melden müssen (§ 8a BSIG). (Das IT-Sicherheitsgesetz 2.0 (2021) hat die Kompetenzen des BSI weiter gestärkt.)

Für Betreiber von Energieversorgungsnetzen und Energieanlagen gibt es jedoch eine Bereichsausnahme: Für sie ist die Bundesnetzagentur zuständig und erstellt eigene Sicherheitsanforderungen.

**Auf europäischer Ebene** wurde 2016 die NIS-Richtlinie veröffentlicht, die erstmals einen gemeinsamen europäischen Standard für Cybersicherheit definiert hat. In Deutschland wurden Anforderungen, die noch nicht durch das IT-Sicherheitsgesetz abgedeckt wurden, 2017 mit dem NIS-Richtlinien-Umsetzungsgesetz implementiert.

Ende 2022 verabschiedete die EU-Kommission die NIS2-Richtlinie. Dis NIS2-Richtlinie weitet Cybersicherheitsvorgaben auf mehr (nämlich sowohl mittlere als auch große) Unternehmen der Kritischen Infrastruktur und damit auch des Stromsektors aus: Von bisher etwa 2.000 regulierten Unternehmen erweitert sich die Anzahl auf über 30.000. Damit fallen in Deutschland Zehntausende Unternehmen erstmals unter die EU-Regulierung.

Für die Umsetzung der Richtlinie in Deutschland beschloss das Kabinett im Juli 2024 das NIS2-Umsetzungsgesetz, dass das BSI-Gesetz erweitern wird. Mit der NIS2-Betroffenheitsprüfung des BSI können Unternehmen in wenigen Schritten schon jetzt herausfinden, inwiefern sie Maßnahmen ergreifen müssen.

Gleichzeitig zur NIS2-Richtlnie trat auf EU-Ebene die CER-Richtlinie in Kraft, mit der Mitgliedsstaaten kritische Einrichtungen identifizieren und ihre physische Sicherheit stärken sollen. Deutschland setzt diese Richtlinie derzeit mit dem KRITIS-Dachgesetz um (aktuell liegt dazu ein Referentenentwurf des Bundesministeriums des Innern und für Heimat (BMI) vor).

Im Oktober 2024 verabschiedete der EU-Rat außerdem den Cyber Resilience Act (CRA), der ab 2027 Anwendung finden soll. Damit werden Anforderungen an die Cybersicherheit für „Produkte mit digitalen Bestandteilen" verbindlich festgelegt. Damit sind jegliche Software- oder Hardwareprodukte und ihre Lösungen mit einem Fernzugriff über ein Produkt oder Netzwerk gemeint. Auch Akteure der Stromwirtschaft, die etwa digitale Steuerungssysteme oder Smart Meter herstellen und einsetzen, werden somit vom CRA berührt werden.

[23] https://www.eco.de/presse/cybersicherheit-nur-wenige-unternehmen-in-deutschland-sind-auf-nis2-vorbereitet/ (zuletzt besucht am 07.01.2025)

Für die Branchenplattform bieten sich folgende Möglichkeiten an, die Transparenz der Gesetzgebung zu erhöhen:

- Die Teilnehmer wünschen sich klare Ansprechpersonen auf Behördenseite (BSI, BNetzA). Mit der Branchenplattform könnte eine Übersicht über relevante Anlaufstellen erstellt und es könnten weitergehende Wünsche der Teilnehmer gesammelt und an die Behörden weitergeleitet werden.
- Über die Branchenplattform können Best Practices ausgetauscht und verschriftlicht werden, wie Akteure der Stromwirtschaft die Gesetzgebung in verschiedenen Kontexten umsetzen. Dieser Vorschlag bei dem abstrakte Vorgaben mit praktischen Beispielen erläutert würden, erfuhr unter den Beteiligten des Themenroadmap-Prozesses eine breite Zustimmung. Bei der Methodik könnte man sich an bestehenden Methoden und Beispielen orientieren (z. B. Lechner et al., 2018).
- Mit der Branchenplattform könnten bereits existierende Informationsangebote und Überblicke zu bestehenden Regularien recherchiert und bezüglich des stromwirtschaftlichen Bedarfs evaluiert werden. Daraus resultierend könnten Empfehlungen ausgesprochen und verbreitet werden. Bereits vorhandene Angebote sind beispielsweise die folgenden:
  - Das BSI bietet eine Vielzahl von Schriften und Erläuterungen an. Dazu gehört etwa die Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung, die die Anforderungen des § 8a BSIG konkretisiert. Die Orientierungshilfe gibt Unternehmen Anhaltspunkte, wie ein Angriffserkennungssystem individuell gestaltet werden kann, und definiert Anforderungen rund um Protokollierung, Detektion (Erkennung) und Reaktion für Betreiber. Dabei geht es sowohl um technische Kriterien als auch um organisatorische und prozessuale Anforderungen.
  - Die Bundesnetzagentur bietet einen umfangreichen Überblick zum Thema IT-Sicherheit im Energiesektor. Hierzu gehören unter anderem IT-Sicherheitskataloge für die Betreiber von Strom- und Gasnetzen sowie für die Betreiber von Energieanlagen. Diese Sicherheitskataloge definieren Mindeststandards, die für den Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme notwendig sind, um den sicheren Netzbetrieb zu gewährleisten.
  - Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) bietet eine ausführliche Handreichung zum „Stand der Technik". Dieser unbestimmte Rechtsbegriff sorgt bei KRITIS-Betreibern immer wieder für Verwirrung[24] und war auch während der Entwicklung der Themenroadmap mehrfach Thema. In der Handreichung wird der „Stand der Technik" für relevante Systeme, Komponenten und Prozesse im Sinne des IT-Sicherheitsgesetzes zusammengefasst. Sie gibt konkrete Hinweise und Handlungsempfehlungen.
  - Der Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) hat mehrere stromwirtschaftsspezifische Whitepaper zur Cybersicherheit in Stromnetzen verfasst. Dazu gehört etwa das Papier zu „Sicherheitsanforderungen für IT und Steuerungstechnik in der Energiewirtschaft", in dem regulatorische Anforderungen aufgeführt und Hilfestellungen für ihre Umsetzung gegeben werden.
  - Der Cybersecurity Navigator bietet einen Überblick über Rechtsvorschriften und Standards für Kritische Infrastrukturen. Mittels eines einfachen Dropdown-Menüs lassen sich unter anderem sektoren- und branchenspezifische Normen und Standards sowie Rechtsvorschriften auffinden.

[24] https://intrapol.org/wp-content/uploads/2017/02/Kipker-DuD-2016-Unbestimmte-Rechtsbegriffe.pdf (zuletzt besucht am 26.10.2024)

Der Navigator geht aus einem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekt hervor.

- Die unabhängige Plattform OpenKRITIS bietet einen guten Überblick über aktuelle Regularien und Gesetzentwürfe zum Schutz Kritischer Infrastrukturen inklusive übersichtlicher Tabellen. Auf der Plattform finden sich auch Stellungnahmen.
- Die Stiftung interface (vormals: Stiftung Neue Verantwortung) aktualisiert zweimal jährlich einen Überblick über Deutschlands staatliche Cybersicherheitsarchitektur. Dieses Papier beinhaltet eine Einordnung sämtlicher relevanten Cybersicherheitsakteure in Deutschland (Bundes-, Landes- und kommunale Ebene) sowie auf UN-, EU- und NATO-Ebene.

## 3.6 Test- und Weiterbildungsmöglichkeiten ausbauen

**Aktueller Stand:** Bearbeitung noch nicht geplant

In einer Umfrage unter mehr als 5.000 Beschäftigten deutscher Unternehmen gaben 60 Prozent der Befragten an, dass sie sich mehr Aufklärung und Weiterbildungsmöglichkeiten zu IT-Sicherheit wünschen. Nur etwa die Hälfte der Unternehmen bietet für alle Mitarbeiterinnen und Mitarbeiter Schulungen oder Trainings rund um das Thema Cybersicherheit an, in kleinen Unternehmen sind es gerade einmal 38 Prozent. Eine ebenso hohe Zahl (38 Prozent) bewertet das Verantwortungsbewusstsein der Beschäftigten außerhalb der IT-Abteilung ihrer Unternehmen als unzureichend (Froitzheim und Koch, 2023).

Es gibt viele Möglichkeiten, die Belegschaft weiterzubilden. Neben klassischen (Online-)Seminaren und Schulungen können etwa Security-Awareness- und Phishing-Tests durchgeführt oder klassische Vorträge angeboten werden. Die nachhaltige Wirkung solcher Formate im Hinblick auf Verhaltensänderungen der Mitarbeiterinnen und Mitarbeiter unterscheidet sich jedoch stark und wird selten untersucht.

Cybersicherheitsvorfälle können auch mit Szenarien nachgestellt und in inszenierten Situationen geübt werden. Es gibt Serious Games (zum Beispiel das Brettspiel „Neustart“ zu einem Blackout auf kommunaler Ebene[25]) und Tabletop Exercises, die auf die speziellen Bedürfnisse von Organisationen ausgerichtet sind[26]. Mit diesen Übungen testet man die Reaktionsfähigkeit und Resilienz des Unternehmens sowohl auf menschlicher (organisatorischer) als auch auf technischer Ebene (z.B. redundante Kommunikationswege). Diese Übungen bilden die Ausgangslage, um organisatorische Veränderungen im Umgang mit Cyberrisiken anzustoßen.

Bekannte große Krisenübungen sind die „Länder- und Ressortübergreifenden Krisenmanagementübungen“ (LÜKEX), die im Abstand von wenigen Jahren stattfinden. (Ein großflächiger Stromausfall wurde zuletzt 2004 geübt.[27] Im September 2023 simulierte man mit LÜKEX einen Cyberangriff auf deutsche Behörden, der auch Kritische Infrastrukturen lahmlegt.[28]) Ein wichtiger Übungsbestandteil dabei ist, dass die Übungen mit vielen Beteiligten aus Bund und Ländern sowie weiteren Organisationen (wie dem Technischen Hilfswerk) stattfinden. Dies stärkt die für den Ernstfall notwendige Zusammenarbeit und Vernetzung.

[25] https://gfkv.org/neustart/ (zuletzt besucht am 02.10.2024)
[26] https://www.stiftung-nv.de/publications/cybersecurity-policy-exercises-practice (zuletzt besucht am 02.10.2024)
[27] https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/krisenmanagement/luekex/luekex-node.html (zuletzt besucht am 02.10.2024)
[28] https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/so-war-der-erste-luekex-tag (zuletzt besucht am 02.10.2024)

Eine nicht repräsentative Umfrage unter Stromnetzbetreibern ergab, dass Sicherheitsübungen zur Reaktion auf Cyberangriffe bei vielen deutschen Stromnetzbetreibern nicht oder nur unregelmäßig stattfinden. Nur ein sehr geringer Teil der 44 befragten Unternehmen führt solche Übungen mindestens einmal jährlich durch. Gleichzeitig gibt es ein großes Interesse bei den Befragten, an organisierten Cybersicherheitsübungen teilzunehmen (Wagner und Chadenas, 2022).

Die Beteiligten des Themenroadmap-Prozesses wünschen sich außerdem einen Ausbau von Testmöglichkeiten. Motivierender Ausgangspunkt hierfür ist vor allem ein Konflikt zwischen stabilen, meist aber alten Systemen auf der einen und innovativen, meist aber noch nicht lange getesteten und daher unsicheren Systemen auf der anderen Seite (vgl. Kapitel 3.3). Testlabore bieten die Möglichkeit, neu entwickelte Software unter nachgestellten Bedingungen auszuprobieren, etwaige Probleme zu ermitteln und kontextspezifische Analysen durchzuführen.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, Test- und Weiterbildungsmöglichkeiten auszubauen:

- Über die Branchenplattform kann evaluiert werden, inwiefern es sinnvoll ist, Weiterbildungen organisations- und stromwirtschaftsspezifisch auszurichten. Es können Inhalte und Konzepte für solche Weiterbildungen entwickelt und diskutiert werden.
- Die Branchenplattform kann Akteure einbinden, um stromwirtschaftsspezifische Sicherheitsübungen zur Reaktion auf Cyberangriffe zu planen und durchzuführen. In der Planung kann auf bestehende Literatur und vorhandene Erfahrungen zurückgegriffen werden: Schütze und Beigel (2022) fassen Learnings aus von ihnen durchgeführten Cybersicherheitsübungen zusammen und geben einen detaillierten Überblick, wie sie diese Übungen vorbereitet und durchgeführt haben. Gaskova und Massel (2021) erläutern verschiedene Modelle, welche extremen Szenarien sich nach einer Cyberattacke im Energiesektor eröffnen können.
- Über die Branchenplattform können Anforderungen an spezifische Testlabore, etwa zur IT-/OT-Schnittstelle, gesammelt und erste Schritte zur Etablierung solcher Testlabore unternommen werden.

## 3.7 Eine Wissensbasis zur Klassifizierung von Bedrohungen und Angriffen schaffen

**Aktueller Stand:** Bearbeitung noch nicht geplant

Cyberattacke ist nicht gleich Cyberattacke. Die Angriffe unterscheiden sich in ihren Techniken und Taktiken, sodass unterschiedlich auf sie reagiert werden muss. Eine bekannte Taktik ist zum Beispiel, dass Angreifer Ressourcen suchen, die sie zur Unterstützung ihrer Operationen nutzen können. Dazu verwenden sie beispielsweise die Technik, E-Mail-Konten zu kapern und sie für gezielte Angriffe (z. B. Phishing) zu missbrauchen.

Es haben sich verschiedene Ansätze etabliert, Cybersicherheitsmaßnahmen zu klassifizieren. Dazu gehört die einfache und klassische dreigeteilte Einteilung in Maßnahmen der Prävention, Detektion und Reaktion. Etwas detaillierter ist zum Beispiel das NIST Cybersecurity Framework mit fünf sogenannten „Funktionen“, um sich gegen Cyberangriffe zu wappnen: Identify, Protect, Detect, Respond, Recover.

Manchmal ist es hilfreich, die Perspektive zu wechseln. Daher haben sich auch verschiedene Ansätze etabliert, die die Strategien und Wege von Cyberkriminellen auflisten und kategorisieren. Dieser Perspektivenwechsel kann etwa dabei helfen, mögliche Schwachstellen in den eigenen Systemen zu entdecken. Etablierte Übersichten sind das Cyber Kill Chain Framework sowie das MITRE ATT&CK Framework. Es gibt außerdem zahlreiche Weiterentwicklungen oder eigene Ansätze von Unternehmen (z. B. Kim, Kwon und Kim, 2019; einen guten Überblick bietet Pols, 2023).

**Das Cyber Kill Chain Framework**

Das Cyber Kill Chain Framework wurde vom US-amerikanischen Rüstungs- und Technologiekonzern Lockheed Martin Corporation entwickelt. Das Konzept der „Kill Chain" stammt ursprünglich aus der militärischen Abwehr, 2011 übertrug es das Unternehmen auf die Cybersicherheit.

Das Cyber Kill Chain Framework beschreibt in sieben Stufen ein immer tieferes Vordringen eines Cyberkriminellen in das System des Opfers. Das Modell stellt damit Schritt für Schritt dar, wie Angreifer handeln, wenn sie eine Cyberattacke durchführen: vom Sammeln von Informationen über das Opfer über die Installation eines permanenten Zugangs zum System des Opfers bis zur eigentlichen Verwirklichung des Ziels, etwa der Verschlüsselung oder des Herunterladens von Daten. Das Framework ist damit nützlich, um für jeden der sieben Schritte entsprechende Abwehrstrategien umzusetzen.

**Das MITRE ATT&CK Framework**

Das MITRE ATT&CK Framework ist eine Wissensdatenbank über verschiedene Cyberangriffe, die diese in ihren verschiedenen Taktiken, Techniken und Verfahren strukturiert. Das Framework wurde zum ersten Mal 2013 von der gemeinnützigen Organisation MITRE veröffentlicht und wird seitdem, basierend auf realen Beobachtungen, laufend aktualisiert.

Das MITRE ATT&CK Framework besteht aus drei verschiedenen Matrizen: Die Enterprise-Matrix umfasst Informationen für verschiedene Betriebssysteme (Windows, Linux, macOS) sowie Netzwerke und Clouds. In dieser Haupt-Matrix sind zurzeit 14 verschiedene Taktiken und (diesen zugeordnet) 196 Techniken aufgelistet, die Cyberkriminelle verwenden können. Die Mobile-Matrix zielt auf Strategien für die Betriebssysteme Android und iOS. Die dritte Matrix umfasst Informationen für industrielle Kontrollsysteme.

Es gibt bereits verschiedene stromsektorspezifische Ansätze, um IT-Sicherheitsmaßnahmen und -lösungen zu kategorisieren. Beispielsweise geben Sun, Hahn und Liu (2018) einen guten, mittlerweile aber einige Jahre alten Überblick über Cybersicherheitsschwachstellen und -lösungen bei Stromnetzen. Petersen, Stock und Federrath (2023) sowie Haug, Spath und Hatt (2021) erläutern konkrete Bedrohungsszenarien für Energieinfrastrukturen. Van der Velde et al. (2020) stellen einen auf einer Simulation basierenden Ansatz vor, mit dem sie auf die spezifischen Herausforderungen der fortschreitenden Dezentralisierung und Vernetzung von Stromversorgungsnetzen reagieren. All diese Ansätze unterscheiden sich und weichen von allgemeinen, vereinfachenden Systematisierungen wie denen des Cyber Kill Chain Framework und des MITRE ATT&CK Framework ab.

Für die Branchenplattform bieten sich folgende Möglichkeiten an, eine stromwirtschaftsspezifische Wissensbasis zu etablieren:

- Das MITRE ATT&CK Framework bietet eine enorme Fülle an Informationen. Für Akteure der Strom- und Digitalwirtschaft könnte es hilfreich sein, diese bezüglich der in der Stromwirtschaft genutzten Systeme und häufiger Angriffsvektoren zu durchforsten und zu präzisieren – und damit einen weniger komplexen Überblick zu geben. Sollte daraus eine stromwirtschaftsspezifische Wissensbasis entstehen, wäre eine regelmäßige Aktualisierung notwendig. Voraussetzung für diese Wissensbasis sind eine Recherche zu in der Stromwirtschaft verbreiteten Systemen sowie ein offener Austausch zu Erfahrungen mit Cyberangriffen (vgl. Kapitel 3.2).
- Ein Gutachten könnte einen Überblick über bereits bestehende Arbeiten zu stromsektorspezifischen Cybersicherheitsmaßnahmen und -lösungen geben. Diese Arbeiten könnten evaluiert und Gemeinsamkeiten und Lücken herausgearbeitet werden. Ziel dieser Maßnahme könnte sein, besonders hilfreiche Ansätze zu finden und weiterzuentwickeln bzw. zu verbreiten.

# 4 Weitere Themen des Roadmap-Prozesses

Die folgenden Themen wurden im Themenroadmap-Prozess diskutiert, aber nicht als relevante Handlungsfelder identifiziert. Wir führen hier kurz in sie ein. Auf der Branchenplattform könnten diese Themen eventuell zu einem späteren Zeitpunkt oder als Aspekte der oben aufgeführten Handlungsfelder behandelt werden.

## 4.1 Grundlegendes Sicherheitsmanagement umsetzen

Die Umfrage im Themenroadmap-Prozess ergab, dass es sehr variiert, ob grundlegende Sicherheitsvorkehrungen in Organisationen umgesetzt werden. Dazu gehört etwa, regelmäßige Updates für IT- und OT-Systeme oder Maßnahmen durchzuführen, um Supply-Chain-Angriffe zu erkennen. Die Teilnehmer verbanden dieses Thema vor allem mit praktischen Problemen dabei, gesetzliche Anforderungen umzusetzen (vgl. Kapitel 3.5). Umsetzungsprobleme können außerdem einer unzureichenden Sensibilisierung geschuldet sein (vgl. Kapitel 3.1).

## 4.2 Dem Fachkräftemangel begegnen

Der Fachkräftemangel wird zwar auf politischer Ebene immer wieder thematisiert.[29] Doch Prozessautomatisierungen sind eine Möglichkeit, ihm zu begegnen. Die Beteiligten des Themenroadmap-Prozesses erwähnten, dass die dafür grundlegende Vernetzung von Systemen einer besonderen Fachexpertise bedarf, da sich die Logiken von bisher abgekapselten Systemen zum Teil drastisch unterscheiden.

Der Fachkräftemangel spielte auf dem Branchenplattform-Treffen im September 2024 eine bedeutendere Rolle. Hierbei wurde insbesondere die Sorge geäußert, dass digitale Lösungen nicht ausreichen würden, um die Lücke durch die bald in Ruhestand gehenden Fachkräfte zu füllen. Es braucht Maßnahmen, die darüber hinausgehen, etwa durch verstärkte Bemühungen in der Ausbildung oder in der Förderung von Frauen (die in der Branche bisher nur wenig vertreten sind).

## 4.3 Sich auf neue Technologien einstellen

Welche Auswirkungen neue Technologien (z. B. Quantencomputing) auf die IT-Sicherheit haben, beschäftigte die Teilnehmer des Themenroadmap-Prozesses eher wenig. Gegenwärtige Herausforderungen scheinen drängender zu sein. Der Blick in die Zukunft mag einerseits unsicher sein – andererseits ist es strategisch klug, sich frühzeitig mit wahrscheinlich eintretenden Herausforderungen auseinanderzusetzen.

## 4.4 Bedürfnissen kleiner Unternehmen begegnen

Für kleine und mittlere Unternehmen kann es eine besondere Herausforderung sein, mit beschränkten finanziellen Mitteln eine zufriedenstellende Cybersicherheit zu gewährleisten. Dies wurde auch von den Beteiligten des Themenroadmap-Prozesses immer wieder bestätigt. Sie plädierten aber dafür, dieses Thema nicht

[29] Vgl. https://www.lanline.de/it-security/cybersecurity-bedrohung-fuer-unternehmen-waechst.255816.html und https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap (zuletzt besucht am 11.10.2024)

als eigenes Handlungsfeld zu betrachten, sondern es stattdessen in jedem mit der Branchenplattform adressierten Handlungsfeld mitzudenken.

## 4.5 IT-Sicherheit als Kriterium in Vergabeprozessen aufwerten

Mit der Energiewende und der damit einhergehenden Vernetzung und Digitalisierung gibt es neue Stakeholder in der Stromwirtschaft, es entstehen neue Abhängigkeiten und Lieferketten. Diese Abhängigkeiten können zu Kettenreaktionen führen. Ein Angriff auf von externen Dienstleistern entwickelte und zur Verfügung gestellte Software trifft im schlimmsten Fall Tausende Akteure. Ein bekanntes Beispiel ist die 2019 gestartete Cyberattacke auf den US-Konzern SolarWinds, bei der mehrere Tausend Kundinnen und Kunden gehackt werden konnten.[30] Nach dem Pager-Angriff auf die Hisbollah im September 2024 gilt die diesbezügliche Aufmerksamkeit auch zunehmend der Hardware und ihren Komponenten.[31] Um diesen Zusammenhang dreht sich auch die Diskussion darüber, ob und unter welchen Umständen man Komponenten des chinesischen Herstellers Huawei verwendet. Am prominentesten hierbei ist die Diskussion um die Einbindung von Huawei in den 5G-Netzausbau. Hier hat die Bundesregierung beschlossen, dass Netzbetreiber Komponenten von Huawei aus dem Kernnetz entfernen und mittelfristig relevante Software dieses Herstellers ersetzen müssen.[32] Auch für die Energiewirtschaft muss das Verhältnis zu Huawei und anderen internationalen Herstellern geklärt werden. Beispiel hierfür ist die Verwicklung von Huawei in den Bau von Windanlagen.[33]

Ein Unternehmen kann sich mittels eines Supply-Chain-Risikomanagements vor vielen Risiken schützen.[34] Dem vorausgehend sollte IT-Sicherheit bereits in Vergabeprozessen stärker priorisiert werden. Im Themenroadmap-Prozess zeigte sich, dass selbst bei IT-sicherheitsrelevanten Ausschreibungen der Preis das ausschlaggebende Kriterium ist, während Reputation und Vendor Lock-in bzw. Abhängigkeiten eine untergeordnete oder keine Rolle spielen. Die Branchenplattform könnte anknüpfend an die ohnehin vom BMWK angestrebte Reform des Vergaberechts[35] Empfehlungen zur Vergabe von IT/OT (im KRITIS-Bereich) entwickeln.

## 4.6 Den Herausforderungen der Sektorenkopplung begegnen

Die Anforderungen, die sich aus der sich vollziehenden und weiter angestrebten Sektorenkopplung ergeben, wurden von den Beteiligten des Themenroadmap-Prozesses als sehr relevant eingeschätzt. Die im Rahmen eines Workshops stattfindende vertiefende Diskussion führte jedoch immer wieder zu den Anforderungen, die sich aus der Vernetzung von IT- und OT-Systemen ergeben (vgl. Kapitel 3.3). Wir empfehlen daher, das Thema Sektorenkopplung im Rahmen dieses Handlungsfeldes mit zu berücksichtigen und dabei womöglich spezifische Herausforderungen der branchenübergreifenden Zusammenarbeit herauszuarbeiten.

[30] https://www.spektrum.de/news/solarwinds-ein-hackerangriff-der-um-die-welt-geht/1819187 (zuletzt besucht am 11.10.2024)
[31] https://www.fr.de/politik/jedes-geraet-einzeln-manipuliert-so-gelang-der-pager-angriff-auf-die-hisbollah-hersteller-mit-statement-zr-93306706.html (zuletzt besucht am 14.10.2024)
[32] https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/nur-ein-halbes-aus (zuletzt besucht am 14.10.2024)
[33] https://www.focus.de/finanzen/news/energiewende-stockt-windkraft-ausbau-ohne-die-chinesen-wird-es-schwierig_id_189455119.html (zuletzt besucht am 14.10.2024)
[34] https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Management-Blitzlicht/Management_Blitzlicht_node.html (zuletzt besucht am 11.10.2024)
[35] https://table.media/esg/analyse/vergaberecht-was-die-reform-fuer-nachhaltiges-wirtschaften-bedeutet/ (zuletzt besucht am 14.10.2024)

# 5 Fazit

Die Themenroadmap schafft für die Branchenplattform Cybersicherheit in der Stromwirtschaft eine Grundlage für einen zielgerichteten Multi-Stakeholder-Dialog. Sie umfasst sieben Handlungsfelder zur Cybersicherheit in der Stromwirtschaft, die über einen partizipativen Prozess identifiziert wurden und an denen sich die inhaltliche Arbeit der Branchenplattform ausrichtet.

Die sieben Handlungsfelder der Themenroadmap werden nicht allesamt und zeitgleich in der Branchenplattform angegangen. Um tatsächlich drängende Probleme zuerst zu lösen, wurden zunächst die Themen bearbeitet, die im Themenroadmap-Prozess am meisten Diskussionen hervorgerufen haben und im weiteren Verlauf von den Partnern der Branchenplattform priorisiert wurden. Das Themenmodul „Führungskräfte sensibilisieren“ (vgl. Kapitel 3.1) wurde bereits abgeschlossen. Die Themenmodule „Gemeinsam aus Cyberattacken lernen“ (vgl. Kapitel 3.2), „Herausforderungen vernetzter OT-Systeme angehen“ (vgl. Kapitel 3.3), „Die Harmonisierung von Zertifizierungen vorantreiben“ (vgl. Kapitel 3.4) und „Transparenz in der Gesetzgebung erhöhen“ (vgl. Kapitel 3.5) befinden sich derzeit in Bearbeitung. Für die Themen „Test- und Weiterbildungsmöglichkeiten ausbauen“ (vgl. Kapitel 3.6) und „Eine Wissensbasis zur Klassifizierung von Bedrohungen und Angriffen schaffen“ (vgl. Kapitel 3.7) ist derzeit noch keine Bearbeitung vorgesehen.

Darüber hinaus empfiehlt die Gesellschaft für Informatik e.V., die frühzeitige Beschäftigung mit zu erwartenden Veränderungen nicht zu vernachlässigen. Sie kann vielen Beteiligten langfristig Vorteile bringen. Wir empfehlen daher, die Themen Fachkräftemangel und neue Technologien (vgl. Kapitel 4.2 und 4.3) mittelfristig in der Branchenplattform zu adressieren, obwohl sie von den Beteiligten des Roadmap-Prozesses nicht zu den sieben relevantesten Handlungsfeldern gezählt wurden.

# Anhang: Der Prozess hinter der Themenroadmap

Viele Akteure bringen viele verschiedene Kontexte und Herausforderungen mit. Am Anfang gilt es, diese zu sortieren und für alle Beteiligten relevante Themen und Probleme zu identifizieren. Dies war das Ziel eines am Anfang der Branchenplattform stehenden Arbeitsprozesses, der Erstellung einer Themenroadmap.

Der mit Unterstützung der Gesellschaft für Informatik e.V. (GI) erstellten Themenroadmap ging ein etwa sechsmonatiger Prozess voraus. Dieser Prozess umfasste eine Recherche, eine Umfrage unter beteiligten Stakeholdern sowie einen Workshop, der die Ergebnisse der Umfrage noch einmal zur Diskussion stellte. Im Folgenden geben wir einen Überblick über die jeweiligen Arbeitsschritte.

## Der Delphi-Ansatz als Inspiration

Mit vielen Akteuren sind auch viele verschiedene Kontexte und Herausforderungen verbunden. Deshalb bestand die Aufgabe bei der Erstellung der Themenroadmap zunächst darin, diese Vielfalt an Themen und Herausforderungen von diversen Stakeholdern einzuholen und ihr gerecht zu werden. Entsprechend den verschiedenen Hintergründen und Kenntnissen der Stakeholder war zu erwarten, dass unterschiedliche Verständnisse und Einschätzungen geäußert werden. Die Stakeholder sollten die Chance erhalten, ihre individuellen Sichtweisen und Kompetenzen einzubringen. Gleichzeitig sollten sie neue Perspektiven von anderen Akteuren aufgezeigt bekommen, ihre Einschätzungen entsprechend überdenken und sich auf gemeinsame Themen einigen.

Um diesen Herausforderungen zu begegnen, haben wir uns methodisch an der Delphi-Methode orientiert. Die Delphi-Methode ist eine strukturierte Form der Befragung (Grunwald, 2010). Die Grundidee der Methode ist eine mehrstufige Befragung von Expertinnen und Experten, in unserem Fall den Stakeholdern der Branchenplattform. Sie werden zunächst einzeln zu ihren Einschätzungen befragt. Dies wurde durch eine im Folgenden beschriebene Umfrage umgesetzt. Anschließend werden ihnen die Gesamtergebnisse der Befragung und damit die Einschätzungen anderer Fachleute unterbreitet. Dies wurde mittels einer Zusammenfassung der Ergebnisse in einer Themenfeldanalyse umgesetzt. Die Expertinnen und Experten erhalten schließlich die Möglichkeit, sich mit den anderen darüber auszutauschen, ihre Meinungen womöglich zu überdenken und, soweit möglich, einen Konsens zu erzielen. Dies wurde im Rahmen eines Workshops realisiert (vgl. Abbildung 1). Das Ergebnis sind die oben aufgeführten und erläuterten Themen.

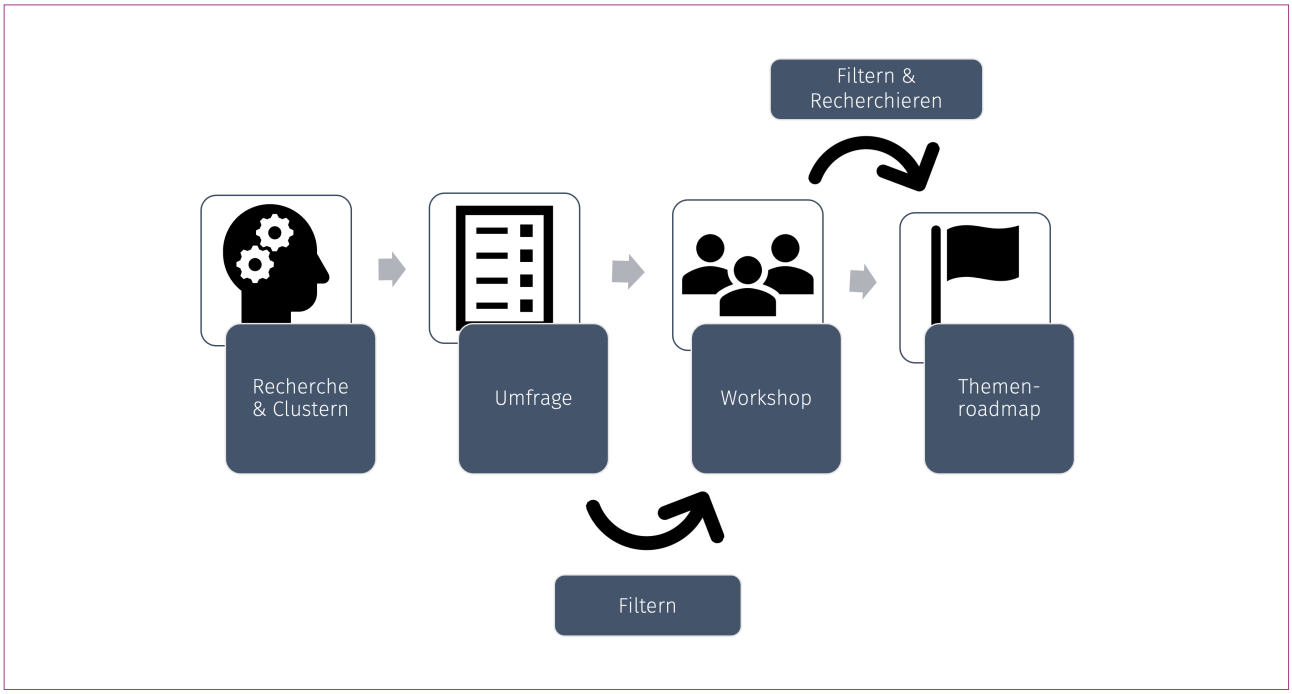



Abbildung 1 Skizzierter Prozess der Themenroadmap

## Eine strukturierende Basis mit dem ENISA-Framework

Zur Strukturierung der Themen haben wir uns an das ENISA-Framework zur Bewertung nationaler IT-Sicherheitsfähigkeiten[36] angelehnt. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Sie leistet einen Beitrag zur Unionspolitik im Bereich der Cybersicherheit, erhöht die Vertrauenswürdigkeit von IKT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, kooperiert mit den Mitgliedsstaaten sowie den Organen und Einrichtungen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Kapazitätenaufbau und Sensibilisierung im Bereich der Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürgerinnen und Bürger Europas zu gewährleisten. Mit dem ENISA-Framework wird ein Rahmen vorgestellt, mit dem die Mitgliedsstaaten der Europäischen Union ihre nationalen Cybersicherheitsstrategien selbst bewerten können (Sarri et al., 2020).

Die Aufgaben und Ziele, die die ENISA für Akteure der Europäischen Union übernimmt bzw. verfolgt, ähneln zu großen Teilen denen, die mit der Branchenplattform Cybersicherheit für die Stromwirtschaft adressiert werden sollen, hier natürlich im kleineren Rahmen, nämlich für die Akteure der Strom- und Digitalwirtschaft in Deutschland. Zu diesen Zielen gehören die Kooperation zwischen verschiedenen Akteuren, das Anvisieren gemeinsamer Herausforderungen, ein Wissensaustausch und der Aufbau von Vertrauen mit dem letztendlichen Ziel, mehr Sicherheit für die Gesellschaft zu gewährleisten. Dementsprechend haben wir für die Themenroadmap dieses Framework herangezogen, um mögliche und letztendliche Themen der Branchenplatt-

[36] https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-de.pdf (zuletzt besucht am 23.10.2024)

form zu strukturieren. Dazu gehört vor allem die Orientierung an den vier Hauptclustern des ENISA-Framework:

A) Governance und Standards im Bereich der Cybersicherheit
B) Kapazitätenaufbau und Sensibilisierung
C) Gesetze und Bestimmungen
D) Zusammenarbeit

Diese Cluster haben wir wie folgt an die Zielgruppen und Bedarfe der Branchenplattform angepasst, um für die Umfrage passende und den Gesamtbereich abdeckende Thesen zu erstellen:

Der Themenbereich „**Governance und Standards**“ ist dahingehend angelegt worden, eine angemessene Governance, geeignete Standards und bewährte Verfahren im Bereich Cybersicherheit abzufragen. Er umfasste verschiedene Aspekte der Cyberabwehr: Umsetzung grundlegender Sicherheitsvorkehrungen, Identifikation von Cybersicherheitsvorfällen oder die Entwicklung von Strategien zum Umgang mit Cybersicherheitsvorfällen.

In dem Cluster „**Kapazitätenaufbau und Sensibilisierung**“ haben wir Ziele zusammengefasst, die die Grundlage für den Aufbau von Kapazitäten bilden. Es umfasst die Fähigkeit der Strom- und Digitalwirtschaft, kontinuierlich Cybersicherheitskompetenzen auszubauen und das allgemeine Niveau an Kenntnissen und Kompetenzen in diesem Bereich zu erhöhen. Außerdem fragten wir darin nach der Fähigkeit, auf neue Entwicklungen im Bereich der Cybersicherheit sowie auf Sicherheitsvorfälle zu reagieren.

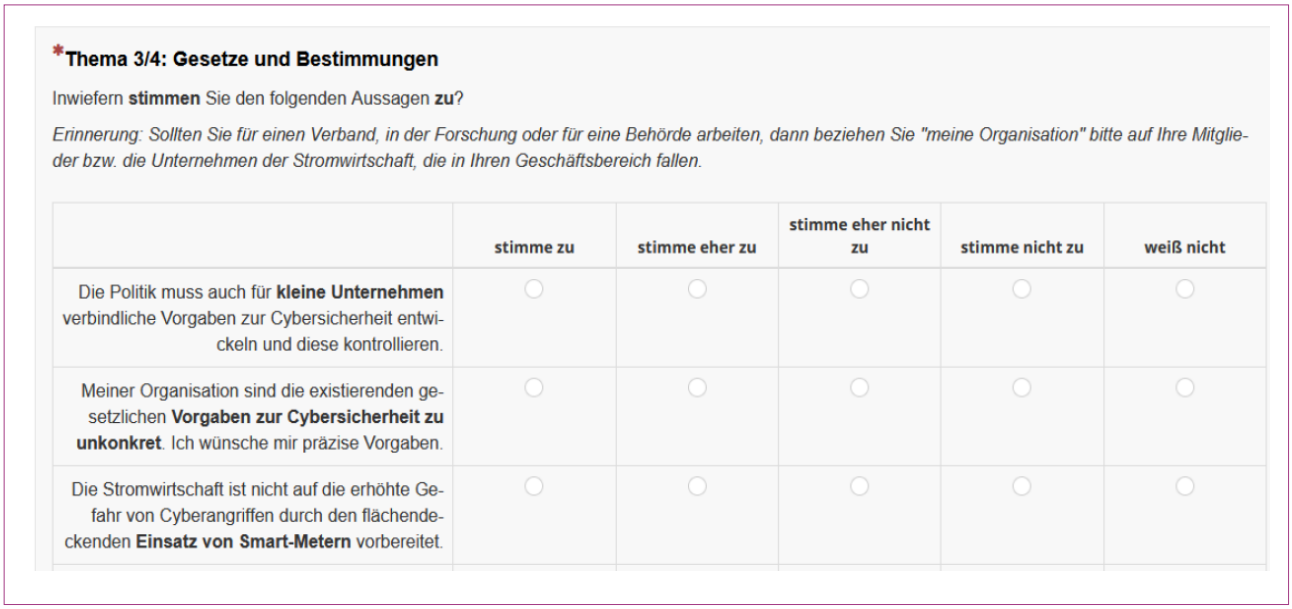
Mit dem Cluster „**Gesetze und Bestimmungen**“ haben wir abgefragt, inwiefern die gesetzlichen und rechtlichen Instrumente ausreichend und praktisch umsetzbar sind, um der Zunahme von Cyberkriminalität und damit verbundenen Cybervorfällen zu begegnen und ihnen entgegenzuwirken.

Das Cluster „**Zusammenarbeit**“ wurde aufgestellt, um ein Meinungsbild zur Zusammenarbeit und zum Informationsaustausch innerhalb der Stromwirtschaft, zwischen Digital- und Stromwirtschaft sowie zwischen Stromwirtschaft und Politik und Behörden zum besseren Verständnis und zur Reaktion auf ein sich ständig änderndes Bedrohungsumfeld einzuholen.

## Eine Umfrage für ein erstes Meinungsbild

Auf Grundlage von Recherchen und einer Beratung durch den IT-Sicherheitsexperten Prof. Hannes Federrath haben wir eine Reihe von Thesen entworfen und je einem der aus dem ENISA-Framework angelehnten Cluster zugeordnet. Die Befragten klickten sich von Cluster zu Cluster mit den jeweiligen Thesen. Den einzelnen Thesen sollten sie jeweils in Abstufungen zustimmen oder nicht zustimmen oder sich einer Positionierung enthalten (vgl. Abbildung 2). Im Anschluss an die Bewertung der jeweiligen Thesen eines Clusters sollten die Befragten bewerten, welche maximal zwei der mit den Thesen angesprochenen Themen sie für am relevantesten halten.

Insgesamt beinhaltete die Umfrage 23 Thesen sowie zusätzlich drei Fragen, um Hintergrundinformationen zu den Befragten zu erhalten (z. B. die Position der Teilnehmerinnen und Teilnehmer in ihrer Organisation). Die Online-Umfrage lief im Juni 2023, die Befragten hatten mehr als drei Wochen Zeit für die Beantwortung.



*Thema 3/4: Gesetze und Bestimmungen

Inwiefern **stimmen** Sie den folgenden Aussagen **zu**?

*Erinnerung: Sollten Sie für einen Verband, in der Forschung oder für eine Behörde arbeiten, dann beziehen Sie "meine Organisation" bitte auf Ihre Mitglieder bzw. die Unternehmen der Stromwirtschaft, die in Ihren Geschäftsbereich fallen.*

| | stimme zu | stimme eher zu | stimme eher nicht zu | stimme nicht zu | weiß nicht |
|---|---|---|---|---|---|
| Die Politik muss auch für **kleine Unternehmen** verbindliche Vorgaben zur Cybersicherheit entwickeln und diese kontrollieren. | ○ | ○ | ○ | ○ | ○ |
| Meiner Organisation sind die existierenden gesetzlichen **Vorgaben zur Cybersicherheit zu unkonkret**. Ich wünsche mir präzise Vorgaben. | ○ | ○ | ○ | ○ | ○ |
| Die Stromwirtschaft ist nicht auf die erhöhte Gefahr von Cyberangriffen durch den flächendeckenden **Einsatz von Smart-Metern** vorbereitet. | ○ | ○ | ○ | ○ | ○ |

Abbildung 2 Ausschnitt aus der Umfrage zur Themenroadmap der Branchenplattform Cybersicherheit in der Stromwirtschaft (Screenshot)

Zur Umfrage haben wir hauptsächlich die Beteiligten der Branchenplattform eingeladen. Zusätzlich schickten wir die Umfrage Forscherinnen und Forschern mit Bezug zu IT-Sicherheit (bisher nicht in der Branchenplattform vertreten) sowie an Netzbetreiber und Energieversorgungsunternehmen, die in der Branchenplattform nur wenig vertreten sind. Die Umfrage richtete sich damit vorrangig an Teilnehmer der Branchenplattform.

Es nahmen 33 Organisationen teil. Von ihnen kam etwa die Hälfte aus der Energiewirtschaft und rund ein Viertel aus der Digitalwirtschaft. Die weiteren Befragten ordneten ihre Organisation der Forschung (18 Prozent), Behörden und Verbänden (12 Prozent) oder Sonstigem (12 Prozent) zu.

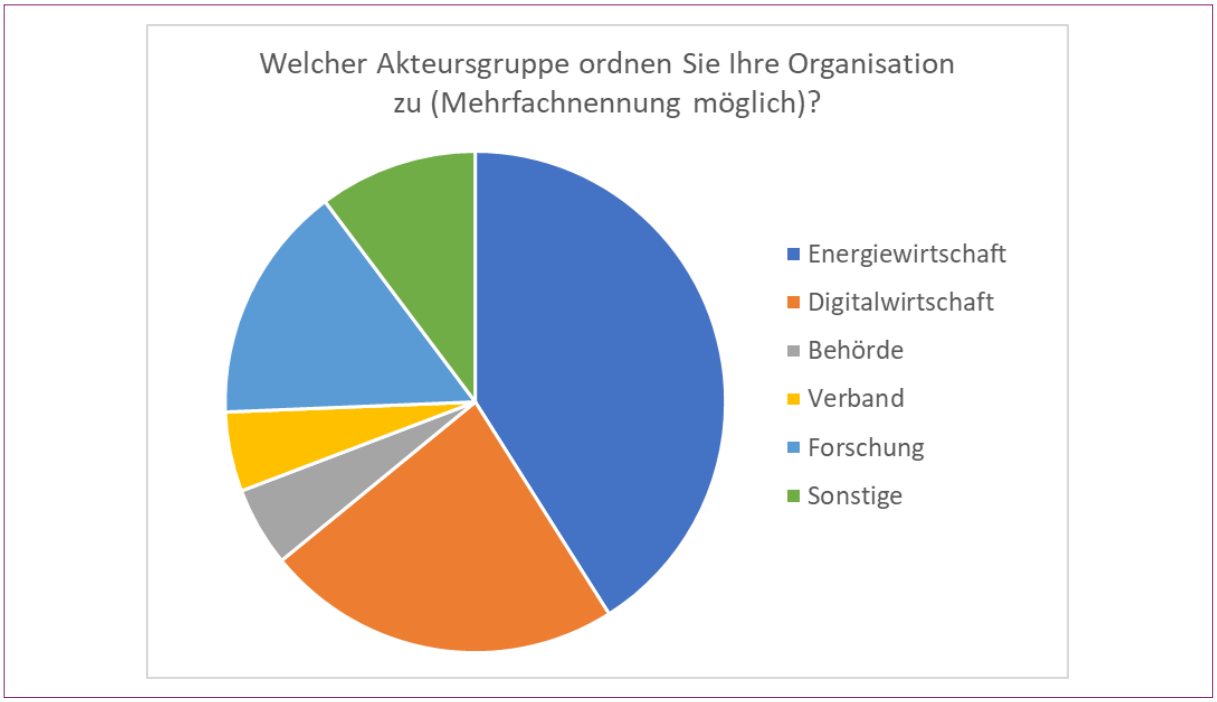



Abbildung 3 Verteilung der Akteursgruppen der 33 Umfrageteilnehmerinnen und -teilnehmer (Mehrfachnennung war möglich)

Die zweite Abfrage zu der Position der jeweiligen Teilnehmerinnen und Teilnehmer ergab: Mit ca. 40 Prozent ordnete sich die größte Gruppe dem IT-Bereich (IT-Sicherheitsbeauftragte / CSO / CISO bzw. CIO / Leiterin oder Leiter der IT) zu. Fast ein Viertel gehört zum Management oder zur Geschäftsführung, fast ein weiteres Viertel kommt aus der Forschung oder es handelt sich um Referentinnen bzw. Referenten. Etwa ein Achtel machte keine Angaben.

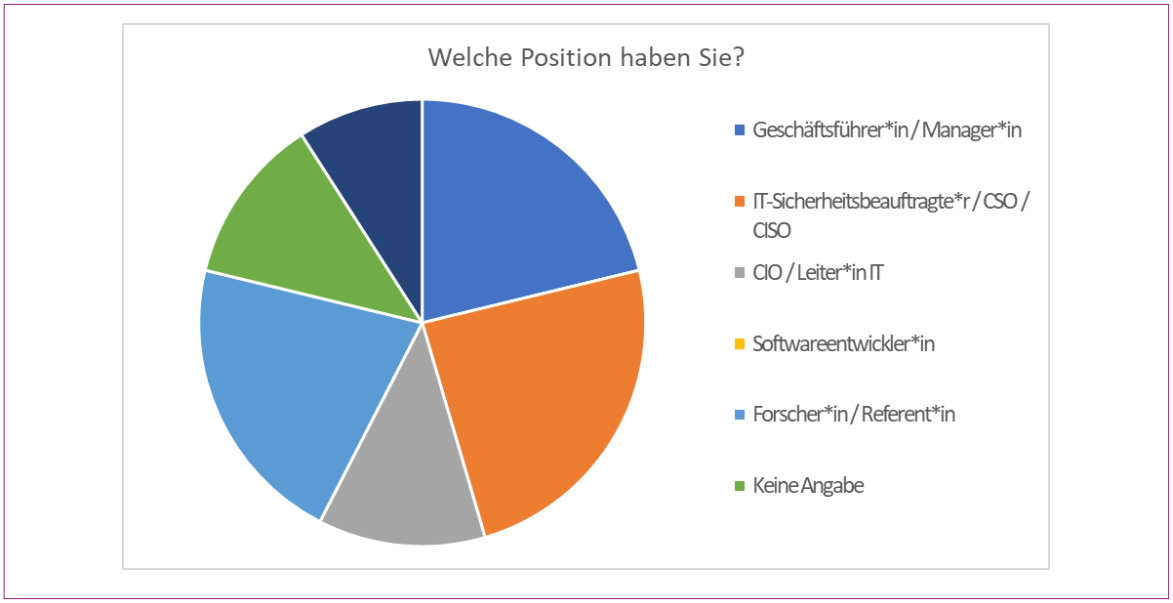



Abbildung 4 Verteilung der Jobpositionen der 33 Umfrageteilnehmerinnen und -teilnehmer (Mehrfachnennung war möglich)

Als Ergebnis der Umfrage haben wir fünf Thesen identifiziert, die für fast alle Befragten relevant waren:

1. Durch die integrierte Energiewirtschaft (Sektorenkopplung) ergeben sich spezifische Anforderungen im Bereich Cybersicherheit, die unbedingt angegangen werden müssen.
2. Es braucht eine auf die Stromwirtschaft ausgerichtete systematische Wissensbasis zur Klassifizierung von Bedrohungen und Angriffen, zum Beispiel in Form der MITRE ATT&CK Matrix.
3. Die Harmonisierung von nationalen und europäischen Zertifizierungen sollte weiter vorangetrieben werden.
4. Führungskräfte und Vorstände müssen stärker für die Vorteile von Investitionen in Cybersicherheitsmaßnahmen sensibilisiert werden.
5. Es fehlt an individuell auf Organisationen der Stromwirtschaft zugeschnittenen Schulungen, Cybersicherheitsübungen und Testlaboren für Forschungszwecke zur Cybersicherheit.

Acht Thesen wurden von den Befragten ambivalent beantwortet: Die Zustimmungen wichen stark voneinander ab, je nachdem aus welchem Bereich die jeweiligen Teilnehmerinnen und Teilnehmer stammen oder welche Position sie besetzen.

1. IT-Systeme und OT-Komponenten meiner Organisation erhalten regelmäßig Sicherheits-Updates.
2. Meine Organisation setzt aktuelle und innovative Softwarelösungen zur Abwehr von Cyberangriffen ein.
3. Meine Organisation setzt Maßnahmen um, die Supply-Chain-Angriffe (Angriffe auf über Dienstleister bereitgestellte Software) auf IKT-Komponenten erkennen und abwehren.
4. Kleine Unternehmen sind finanziell nicht in der Lage, notwendige Cybersicherheitsmaßnahmen umzusetzen.
5. Meiner Organisation fehlt eine Übersicht und Zusammenfassung aktuell geltender Regularien, Standards und Guidelines zur Cybersicherheit in Deutschland und der EU.
6. Meine Organisation weiß genau, welche Behörden und Akteure (inklusive Gremien und AGs) für sie rund um das Thema Cybersicherheit relevant sind.
7. Meiner Organisation sind die existierenden gesetzlichen Vorgaben zur Cybersicherheit zu unkonkret. Ich wünsche mir präzise Vorgaben.
8. Bestehende Sicherheitslösungen aus anderen Branchen sind universell und daher auch gut auf die Stromwirtschaft übertragbar.

Die zehn restlichen Thesen wurden aussortiert.

## Ein Workshop zur Abwägung der Plattform-Themen

Der dreistündige Workshop fand online im August 2023 statt. Es nahmen 15 Personen, darunter eine Auswahl an Beteiligten der Branchenplattform sowie ein Vertreter der Forschung, teil. Bei der Auswahl der Teilnehmerinnen und Teilnehmer haben wir darauf Wert gelegt, dass die Energie- und die Digitalwirtschaft, Behörden und Verbände jeweils gut vertreten sind. Den Teilnehmerinnen und Teilnehmern haben wir im Vorfeld eine Themenfeldanalyse mit den Ergebnissen der Umfrage zur Verfügung gestellt.

Ziel des Workshops war es, dass die Beteiligten wichtige Themen und Fragen für die Branchenplattform identifizieren. Sie sollten dazu verschiedene Assoziationen oder Einstellungen zu den Themen herausarbeiten, Schnittstellen zwischen den Themen identifizieren und einzelne Aspekte ausdifferenzieren.

Der Workshop umfasste dementsprechend eine Einführung und anschließende Diskussion der a) ambivalent beantworteten Thesen der Umfrage sowie b) drei weiterer als relevant bewerteter Thesen, zu denen wir uns differenziertere Erläuterungen zur Relevanz erhofften. Die jeweiligen Themen und Thesen wurden aufgeteilt und in zwei Gruppen mit folgenden Leitfragen ausdiskutiert:

1. Was verbinde ich mit dem Thema?
2. Welche Herausforderungen stellen sich speziell in meiner Organisation?
3. Welche Ansätze/Lösungen gibt es?
4. Wozu möchte ich mich noch austauschen / habe ich Fragen / bestehen noch Bedarfe?

Zum Ende des Workshops wurde ein Meinungsbild darüber eingeholt, welche der besprochenen Thesen die Teilnehmerinnen und Teilnehmer zur weiteren Behandlung in der Branchenplattform empfehlen. Auf Basis dieser Ergebnisse und weiterer Recherchen haben wir die vorliegende Themenroadmap erstellt.

# Abbildungsverzeichnis

# Literaturverzeichnis


Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023): Die Lage der IT-Sicherheit in Deutschland 2023. Bonn. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6 (abgerufen am: 4. Februar 2025).

Froitzheim, U.J. und Koch, C. (2023): Cybersicherheit in Zahlen. G DATA CyberDefense AG. Verfügbar unter: https://www.gdata.de/fileadmin/web/de/documents/Studies/G_DATA_Cybersicherheit_in_Zahlen_2023.pdf (abgerufen am: 4. Februar 2025).

Gaskova, D.A. und Massel, A.G. (2021): Modeling scenarios of extreme situations in the energy sector caused by cyber threats, E3S Web of Conferences. Edited by F.-J. Lin et al., 289, S. 03005. Verfügbar unter: https://doi.org/10.1051/e3sconf/202128903005.

Grunwald, A. (2010): Technikfolgenabschätzung: eine Einführung. Zweite, grundlegend überarbeitete und wesentlich erweiterte Auflage. Berlin: edition sigma (Gesellschaft, Technik, Umwelt, N.F., 1).

Haug, G.H., Spath, D. und Hatt, H. (2021): Resilienz digitalisierter Energiesysteme – Wie können Blackout-Risiken begrenzt werden? Halle (Saale), München, Mainz: Deutsche Akademie der Naturforscher Leopoldina e.V. – Nationale Akademie der Wissenschaften acatech – Deutsche Akademie der Technikwissenschaften e.V. – Union der deutschen Akademien der Wissenschaften e.V.

Hecht, T., Langer, L. und Smith, P. (2014): Cybersecurity Risk Assessment in Smart Grids.

Herpig, S. & Dutke, F. (2023): Deutschlands staatliche Cybersicherheitsarchitektur. Stiftung Neue Verantwortung. Verfügbar unter: https://www.interface-eu.org/storage/archive/files/cybersicherheitsarchitektur_elfteauflage1123.pdf.

Horák, T. und Huraj, L. (2019): Smart Thermostat as a Part of IoT Attack. In: R. Silhavy (Hrsg.): Cybernetics und Automation Control Theory Methods in Intelligent Algorithms. Cham: Springer International Publishing (Advances in Intelligent Systems und Computing), S. 156–163. Verfügbar unter: https://doi.org/10.1007/978-3-030-19813-8_17.

Kim, H., Kwon, H. und Kim, K.K. (2019): Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications, 78(3), S. 3153–3170. Verfügbar unter: https://doi.org/10.1007/s11042-018-5897-5.

Kipker, D.-K. (2023): Schriftliche Stellungnahme „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“. 27. Sitzung. Berlin: Digitalausschuss des Deutschen Bundestags. Verfügbar unter: https://www.bundestag.de/resource/blob/929758/9725e00cad76feaa54527f0130050b14/Stellungnahme-Kipker-data.pdf.

Lechner, U. et al. (Hrsg.) (2018): CASE | KRITIS: Fallstudien zur IT-Sicherheit in kritischen Infrastrukturen. Berlin: Logos.

Petersen, T., Stock, J. und Federrath, H. (2023): Bedrohungsszenarien für Energieinfrastrukturen. Universität Hamburg, Norddeutsches RealLabor. Verfügbar unter: https://svs.informatik.uni-hamburg.de/publications/2023/2023-07-28-NRL-Whitepaper-UHH.pdf (abgerufen am: 4. Februar 2025).

Pols, P. (2023): The Unified Kill Chain. Raising Resilience against Advanced Cyber Attacks. Verfügbar unter: https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf.

Reiberg, A., Niebel, C., & Krämer, P. (2022): Was ist ein Datenraum. Definition des Konzeptes Datenraum.

Rösch, D., Kummerow, A., Bauer, T., Simou, K. und Wenderoth, F. (2024). Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft. Deutsche Energie-Agentur GmbH (dena). Verfügbar unter: https://www.dena.de/PUBLIKATION2006.

Sarri, A. et al. (2020): Rahmen zur Bewertung nationaler Fähigkeiten. European Union Agency for Cybersecurity (ENISA). Verfügbar unter: https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-de.pdf (abgerufen am: 4. Februar 2025).

Schütze, J. und Beigel, R. (2022): Cybersecurity Policy Exercises in Practice. Learnings from Implementing Tabletop Exercises in Different Countries. Stiftung neue Verantwortung e.V. Verfügbar unter: https://www.stiftung-nv.de/sites/default/files/cybersecurity_policy_exercises_in_practice.pdf (abgerufen am: 4. Februar 2025).

Sun, C.-C., Hahn, A. und Liu, C.-C. (2018): Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems, 99, S. 45–56. Verfügbar unter: https://doi.org/10.1016/j.ijepes.2017.12.020.

Trend Micro (2023): IT-Security als Wegbereiter. Trend Micro Deutschland GmbH. Verfügbar unter: https://www.trendmicro.com/explore/it-security-als-wegbereiter/2265-tl-de-wp (abgerufen am: 4. Februar 2025).

van der Velde, D. et al. (2020): Methods for Actors in the Electric Power System to Prevent, Detect and React to ICT Attacks and Failures. In: 2020 6th IEEE International Energy Conference (ENERGYCon). Gammarth, Tunisia: IEEE, S. 17–22. Verfügbar unter: https://doi.org/10.1109/ENERGYCon48941.2020.9236523.

Wagner, J. und Chadenas, O. (2022): Netzbetreiber-Umfrage Cybersicherheit. Zum Stand der Cybersicherheit im deutschen Stromnetz. Deutsche Energie-Agentur (dena). Verfügbar unter: https://future-energy-lab.de/app/uploads/2022/08/ANALYSE_Umfrage-Cybersicherheit.pdf.

Wietschel, M., Plötz, P., Pfluger, B., Klobasa, M., Eßer, A., Haendel, M., ... & Albert, D. (2018): Sektorkopplung: Definition, Chancen und Herausforderungen (No. S01/2018). Karlsruhe: Frauenhofer ISI.

www.dena.de

Deutsche Energie-Agentur