

**Future Energy**  
Lab

STUDIE

**3. Themenroadmap  
der Branchenplattform  
Cybersicherheit in der  
Stromwirtschaft**

Ein Projekt der

**dena**

# 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](mailto:info@dena.de)  
Internet: [www.dena.de](http://www.dena.de)

## Autorinnen und Autoren:

Linda Schwarz, Gesellschaft für Informatik e. V.  
Marieke Petersen, Gesellschaft für Informatik e. V.  
Nikolas Becker, Gesellschaft für Informatik e. V.  
Marius Dechand, dena

GESELLSCHAFT  
FÜR INFORMATIK



## Redaktion:

Friederike Wenderoth, dena

## Stand:

Überarbeitete Fassung, September 2025  
Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

## Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2025) und Gesellschaft für Informatik e.V. (2025):  
*3. Themenroadmap 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 Energie

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Energie. 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

## **Ein Ort des Austauschs für zentrale Akteure der Strom- und Digitalwirtschaft**

Das Thema Cybersicherheit gewinnt für die Energiebranche weiterhin an Bedeutung. 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 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. Seit 2022 widmet sich die Branchenplattform diesem Zweck. Es wurden zahlreiche Partnersitzungen, Workshops und öffentliche Veranstaltungen durchgeführt, wodurch sich die Branchenplattform zu einem wichtigen Austauschort und Impulsgeber entwickelt hat.

## **Welche Cybersicherheitsthemen bewegen die Stromwirtschaft?**

Gemeinsam mit der Gesellschaft für Informatik e.V. und den Partnern der Branchenplattform wurde eine Themenroadmap entwickelt, die als Grundlage für die zu führenden Debatten dient. Die identifizierten Handlungsfelder wurden in der Branchenplattform priorisiert. Darauf aufbauend wurden vier Themenmodule ausgearbeitet und die Ergebnisse durch Studien für die Fachöffentlichkeit aufbereitet:

### Führungskräfte sensibilisieren

Mit der Umsetzung der NIS2-Richtlinie soll Cybersicherheit zur Führungsaufgabe werden. Doch viele Befragte sehen darin keine ausreichende Motivation, um höhere Budgets bereitzustellen – unter anderem wegen der schwer einschätzbaren Kosten und Ressourcen. Trotz besonderer Anforderungen an den Stromsektor als Kritische Infrastruktur bleibt eine strategische Verankerung auf Leitungsebene essenziell, da ständig neue Technologien und Schwachstellen entstehen. Mit dem Ziel, Geschäftsleitungen und andere Entscheidungsebenen im Stromsektor dabei zu unterstützen, Kosten, Nutzen und Rentabilität von Cybersicherheitsmaßnahmen zu bewerten, wurde von der dena in Zusammenarbeit mit dem Fraunhofer IOSB-AST die Studie „Cyber-Fit: Investitionen in die Cybersicherheit der Stromwirtschaft“ erstellt und im September 2024 veröffentlicht.

### Gemeinsam aus Cyberattacken lernen

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. In Zusammenarbeit mit der Gesellschaft für Informatik e.V., Cyber Policy Haus BV und Prof. Dr. Stefan Sütterlin wurde die Studie „Gemeinsam lernen. Lern- und Austauschformate zu Cybersicherheit in der Energiewirtschaft“ durchgeführt. Die daraus erarbeiteten Lernformate wurden im Februar 2025 in einer Pilot-Veranstaltung getestet.

## Harmonisierung von Zertifizierungen und vernetzte OT-Systeme im Cybersicherheitsbereich<sup>1</sup>

OT-Systeme bringen besondere Herausforderungen im Hinblick auf die Cybersicherheit mit sich: Lange Innovationszyklen, proprietäre Technik und mangelnde Update-Zugänglichkeit machen es schwerer, sie abzusichern. Best Practices und regulatorische Empfehlungen helfen, diese Komplexität zu adressieren. Betreiber Kritischer Infrastrukturen müssen laut Gesetz nicht nur Sicherheitsanforderungen erfüllen, sondern dies auch nachweisen. 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. In Zusammenarbeit mit der c.con Management Consulting GmbH und dem OFFIS e.V. wurde daher eine Studie zu Harmonisierungspotenzialen bei Zertifizierungen und ihren Hürden bei der Umsetzung anhand einer Fallstudie erstellt und im August 2025 veröffentlicht.

## Transparenz in der Gesetzgebung erhöhen

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. In Zusammenarbeit mit der intcube GmbH, der Gesellschaft für Informatik e.V. und Cyber Policy Haus BV wurde ein Mentoring für Start-ups und KMUs, die indirekt von NIS2 betroffen sind, durchgeführt sowie eine praxisorientierte Roadmap entwickelt. Die Ergebnisse wurden in einer Studie im August 2025 veröffentlicht.

## **Ausblick auf zukünftige Themen**

Gemeinsam mit dem Partnerkreis und der Gesellschaft für Informatik e.V. werden auf Basis zahlreicher Diskussionen vier neue, verknüpfte Themenfelder definiert, die zukünftig für die Branchenplattform von besonderer Bedeutung sind:

- **Herausforderungen der IT-Sicherheit in Vergaberecht, Einkauf und Lieferkette bündeln:** Das Spannungsfeld von digitaler Souveränität und Abbau von Bürokratie in Vergabeprozessen auflösen.
- **Dezentrale Energieversorgung durch Testlabore sichern:** Evaluation von Testlaboren im Kontext der Dezentralisierung sowie die Betrachtung der Sicherheit von Heim-Photovoltaik-Anlagen.
- **Die interne Organisation, das grundlegende Sicherheitsmanagement und den Fachkräftemangel gemeinsam angehen:** Dabei steht insbesondere die Etablierung einer Cybersicherheitskultur im Fokus.
- **Sektorenkopplung und -erweiterung betrachten:** Die Ausweitung auf andere Sektoren bzw. auf die gesamte Energiewirtschaft inklusive Gas, Wasserstoff und Wärme sowie den Einbezug physischer Sicherheit mit in Betracht ziehen.

---

<sup>1</sup> 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.

# Inhalt

<b>1</b>	<b>Hintergrund</b> .....	<b>6</b>
<b>2</b>	<b>Die Branchenplattform Cybersicherheit in der Stromwirtschaft</b> .....	<b>8</b>
<b>3</b>	<b>Was wir geschafft haben: vier Projekte für mehr Cybersicherheit</b> .....	<b>10</b>
3.1	Führungskräfte sensibilisieren .....	11
3.2	Gemeinsam aus Cyberattacken lernen .....	13
3.3	Herausforderungen vernetzter OT-Systeme angehen und Harmonisierung von Zertifizierungen vorantreiben .....	16
3.4	Transparenz in der Gesetzgebung erhöhen .....	22
<b>4</b>	<b>Was wir mitnehmen: vier zentrale Handlungsfelder</b> .....	<b>27</b>
4.1	Herausforderungen in IT-Sicherheit in Vergaberecht, Einkauf und Lieferkette bündeln .....	27
4.2	Dezentrale Energieversorgung durch Testlabore sichern .....	29
4.3	Die interne Organisation, das grundlegende Sicherheitsmanagement und den Fachkräftemangel gemeinsam angehen .....	29
4.4	Sektorenkopplung und -erweiterung betrachten .....	31
<b>5</b>	<b>Fazit und Empfehlungen</b> .....	<b>33</b>
	<b>Anhang: Der Prozess hinter der Themenroadmap</b> .....	<b>36</b>
	Der Delphi-Ansatz als Inspiration .....	36
	Eine strukturierende Basis mit dem ENISA-Framework .....	37
	Eine Umfrage für ein erstes Meinungsbild .....	38
	Ein Workshop zur Abwägung der Plattform-Themen .....	41
	<b>Abbildungsverzeichnis</b> .....	<b>43</b>
	<b>Literaturverzeichnis</b> .....	<b>44</b>

# 1 Hintergrund

Mit der Energiewende sollen Tausende Photovoltaik- (PV), Wind- oder Biogasanlagen auf nachhaltigerem Wege schaffen, was vorher wenige Kraftwerke geleistet haben. Das Stromnetz wird damit flexibler, aber auch komplexer. Denn diese PV- 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 PV keinen Strom liefert, 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<sup>2</sup> auf oder Störungen in Anlagen oder Systemen könnten über die breite Vernetzung vielen weiteren Akteuren Schaden zufügen und zu großflächigen Stromausfällen führen (Achaal et al., 2024), wie im Mai 2025 auf der iberischen Halbinsel<sup>3</sup>.

Dass Cyberangriffe eine reale Bedrohung darstellen, zeigt die steigende Zahl an registrierten Vorfällen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2024). 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<sup>4</sup>. Ebenso wächst die Sorge vor einem künstlich herbeigeführten Ausfall von PV durch eingebaute Backdoors in Wechselrichtern durch China, Iran oder Nordkorea<sup>5</sup>. „Ein sehr klug geplanter und gezielter Hackerangriff auf PV-Anlagen könnte vermutlich heute schon im ungünstigsten Fall einen europaweiten Blackout verursachen“, sagt Steffen Eyhorn, Experte für Leistungselektronik und Netzintegration am Fraunhofer-Institut für Solare Energiesysteme ISE in Freiburg<sup>6</sup>. Die Gefahr eines Blackouts sieht auch Erika Langerová, Leiterin des Cybersecurity for Energy Research Teams an der Tschechischen Technischen Universität Prag. Sie betont jedoch das Risiko, sich durch Lieferketten in der Stromwirtschaft zu abhängig von China zu machen (Langerová, 2025).

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) mit den EU-Richtlinien NIS2 und CER besondere Anforderungen, die in Deutschland aktuell mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG, Inkrafttreten voraussichtlich

---

<sup>2</sup> Das Kunstwort *Cyber* wird im Sinne von *die Informationstechnik bzw. IT-Systeme betreffend* verwendet.

<sup>3</sup> <https://www.tagesschau.de/ausland/europa/spanien-stromausfall-102.html>, (zuletzt besucht am 13.06.2025)

<sup>4</sup> <https://news.microsoft.com/de-de/autoritaere-staaten-verstaerken-cyber-angriffe-auf-kritische-infrastrukturen/> (zuletzt besucht am 07.10.2024)

<sup>5</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier\\_Cybersicherheit\\_Energiesektor.pdf?\\_\\_blob=publicationFile&v=2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.pdf?__blob=publicationFile&v=2) (zuletzt besucht am 13.06.2025)

<sup>6</sup> <https://www.faz.net/aktuell/wirtschaft/cyberangriffe-auf-solaranlagen-droht-europas-stromnetz-ein-blackout-110520793.html> (zuletzt besucht am 13.06.2025) und <https://www.heise.de/news/Boesartige-Kommunikationsgeraete-in-Solar-Wechselrichtern-in-den-USA-entdeckt-10384536.html> (zuletzt besucht am 09.07.2025)

Ende 2025) sowie dem KRITIS-Dachgesetz (Inkrafttreten voraussichtlich Ende 2025) umgesetzt werden. Viele weitere Stakeholder des Stromsektors (z.B. kleine Unternehmen oder IT-Dienstleister) fallen derzeit unter keine Verordnung. Mit Inkrafttreten der Verordnungen können jedoch für sie teilweise Nachweispflichten entstehen.

Diese und weitere Sicherheitsvorgaben umzusetzen, bedeutet für die Akteure der Stromwirtschaft keine einmalige Anstrengung. Aufgrund sich ständig entwickelnder Software, technologischer Fortschritte, laufend 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 e.V. (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, die in den Kapiteln 3 und 4 vorgestellt werden. Kapitel 5 befasst sich mit den Ergebnissen des letzten Branchenplattform-Treffens 2025. 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 Energie (BMWE) geförderte Branchenplattform Cybersicherheit in der Stromwirtschaft startete im Herbst 2022, 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. So sollen gemeinsam Fortschritte auf dem Weg zu einer cybersicheren und digitalen Energiewirtschaft erzielt werden.

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 Digitalwirtschaft, der Wissenschaft, aus Behörden, Start-ups und der dena. Es liegt ein besonderes Augenmerk darauf, auch kleinere Unternehmen zu involvieren. Beteiligte Akteure / Organisationen (Stand 09/2025):

BayWa r.e. renewable energy GmbH	EnergieDock GmbH
Bitkom e.V.	Energiequelle GmbH
Bundesamt für Sicherheit in der Informationstechnik (BSI)	EWE NETZ GmbH
Bundesministerium für Wirtschaft und Energie (BMWE)	genua GmbH
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA)	intcube GmbH
Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW)	KISTERS AG
Bundesverband Windenergie (BWE)	Next Kraftwerke GmbH
Cloudflare Germany GmbH	performio GmbH
Der Mittelstand BVMW e.V.	Power Plus Communications AG (PPC)
DKE – VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V.	Rhebo GmbH
Dunkelblau GmbH & Co. KG	Rohde & Schwarz GmbH & Co. KG
D-Trust GmbH	SMA Solar Technology AG
eco – Verband der Internetwirtschaft e.V.	solbytech GmbH
EnBW Cyber Security 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 3.4) 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 NIS2UmsuCG bleiben die **Schwellenwerte des BSI-Gesetzes** für KRITIS-Betreiber nach aktuellem Referentenentwurf grundsätzlich gültig. Allerdings gelten durch das neue Gesetz neue Anforderungen für erheblich mehr Organisationen. Rund 30.000 Unternehmen werden voraussichtlich ab diesem Jahr neu reguliert (Stand: Mai 2025, mehr dazu in Kapitel 3.4). 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<sup>7</sup>.

- **Zu den KRITIS-Betreibern** gehören 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 Mitarbeitenden 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 Mitarbeitende und über 10 Millionen Euro Umsatz. Als Sonderfälle zählen größenunabhängig noch Vertrauensdienste und öffentlich bzw. öffentlich zugängliche Telekommunikationsdienste zu den wichtigen Einrichtungen.

<sup>7</sup> <https://www.openkritis.de/it-sicherheitsgesetz/einrichtungen-unternehmensgroesse-nis2.html> (zuletzt besucht am 16.06.2025)

## **3 Was wir geschafft haben: vier Projekte für mehr Cybersicherheit**

Durch den partizipativen Themenroadmap-Prozess (siehe Anhang) konnten initial sieben Themen identifiziert werden. Sie decken sowohl regulatorische und organisatorische als auch technische Probleme ab, die die Stakeholder beschäftigen. Fünf dieser Themen konnten in vier Projekten abgeschlossen werden. Diese Themen und die zugehörigen Projekte werden in diesem Kapitel vorgestellt. Die grau hinterlegten Info-Boxen enthalten ausführlichere Hintergrundinformationen zu einzelnen Aspekten sowie zu den Ergebnissen des Projekts bzw. zum aktuellen Bearbeitungsstand. Die verbleibenden beiden Themen werden in Kapitel 4 zusammen mit weiteren zu vier neuen Handlungsfeldern zusammengefasst.

### 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 Personal Mangels 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. Aufgrund der vorgezogenen Bundestagswahlen 2025 konnte das parlamentarische Verfahren zum NIS2UmsuCG nicht abgeschlossen werden. 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 Bedeutung 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 NIS2UmsuCG wird Cybersicherheit zur Aufgabe von Führungskräften, indem sie für Cybersicherheit offiziell verantwortlich gemacht werden. Ab dem Inkrafttreten des Gesetzes 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.<sup>8</sup> 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 nahezu 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 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.
- Nicht nur Negativszenarien eignen sich, um Führungskräfte zu sensibilisieren, sondern auch die Vorteile von Cybersicherheit für ihr Unternehmen. 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

---

<sup>8</sup> <https://background.tagesspiegel.de/cybersecurity/bei-cybersicherheit-gibt-es-keinen-koenigsweg> (zuletzt besucht am 06.01.2025)

Unternehmen adressiert, um sie schnell und kompakt über aktuelle Themen der Cybersicherheit zu informieren. Ein ähnliches Format mit stromwirtschaftsspezifischen Themen könnte die Branchenplattform aufsetzen.

## 3.2 Gemeinsam aus Cyberattacken lernen

### **Aktueller Stand:** Abgeschlossen

Das Thema „Gemeinsam aus Cyberattacken lernen“ wurde am 11. Juni 2025 mit der Veröffentlichung der Analyse „Gemeinsam lernen. Lern- und Austauschformate zu Cybersicherheit in der Energiewirtschaft“ abgeschlossen.

Ziel der Studie ist es, aufzudecken, welche Probleme einem Austausch zu Cybersicherheit und damit einem gemeinsamen Lernen entgegenstehen. Im Austausch mit Branchenvertreterinnen und -vertretern wurden auf der Grundlage von Theorien aus der Psychologie Handlungsempfehlungen für nachhaltiges Lernen im Bereich Cybersicherheit und konkrete Lern- und Austauschformate zum Teilen von Erfahrungen mit Cybervorfällen entwickelt. Drei dieser Formate wurden während einer Veranstaltung ausprobiert, alle weiteren im Rahmen der Veranstaltung bewertet. Die Bewertung zeigt, dass durch die Etablierung von vier Kernelementen (Verstetigung, Vertrauen, offene Fehlerkultur sowie Wissenstransfer und gemeinsame Sprache) Inhalte effektiv vermittelt werden können und eine positiv wahrgenommene Veranstaltung durchgeführt werden kann.

### **Wesentliche Ergebnisse**

- Eine offene Fehlerkultur ist grundlegend für effektives Lernen: Mitarbeiterinnen und Mitarbeiter müssen sich trauen können, Fragen zu stellen, und Fehler ohne Angst zugeben können. Andernfalls werden Missstände vertuscht und ein gemeinsames Lernen bleibt aus.
- Motivation ist der Schlüssel: Um eine Handlungsänderung zu erzielen, müssen Anlass, Fähigkeit und Motivation gegeben sein. Die Beschäftigten sollten verstehen, welchen Vorteil sie aus der Umsetzung von Cybersicherheitsmaßnahmen ziehen, um eine Verhaltensänderung zu erreichen.
- Austauschformate erfordern Vertrauen: IT-sicherheitsrelevante Details des eigenen Unternehmens zu teilen, kann nur gelingen, wenn die Gesprächsteilnehmerinnen und -teilnehmer in die Integrität des Gegenübers vertrauen können. Dies kann auch mit Non-Disclosure Agreements (NDAs) gewährleistet werden.
- Gemeinsames Verständnis fördern: Die Umsetzung von effektiver Cybersicherheit scheitert auch an fehlendem Wissen auf Leitungsebene. Durch eine Kommunikationsstrategie, die relevante Entscheidungsträgerinnen und -träger da abholt, wo sie stehen, können Entscheidungen leichter umgesetzt werden.

Die Studie wurde in Zusammenarbeit mit der Gesellschaft für Informatik e.V., Prof. Dr. Stefan Sütterlin und Cyber Policy Haus BV erstellt.

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.<sup>9</sup> 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.<sup>10</sup> Andererseits halten mindestens genauso viele Unternehmen es für richtig, transparent mit Cyberangriffen umzugehen.<sup>11</sup> Auch Expertinnen und Experten empfehlen immer wieder Transparenz statt Geheimhaltung.<sup>12</sup>

Die Branchenplattform bietet eine außergewöhnliche Chance, einen Rahmen zu schaffen, in dem sich verschiedene Stakeholder vertrauensvoll und nicht öffentlich zu ihren Cybersicherheitsstrategien und Erfahrungen mit Angriffen austauschen können. Je offener dieser Austausch ist, desto mehr Lernpotenzial ergibt sich für die Beteiligten.<sup>13</sup> 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<sup>14</sup> oder geplant auf EU-Ebene<sup>15</sup>). 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).<sup>16</sup> 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

---

<sup>9</sup> <https://background.tagesspiegel.de/cybersecurity/schweigen-ist-gold> (zuletzt besucht am 12.06.2025)

<sup>10</sup> <https://background.tagesspiegel.de/cybersecurity/unternehmen-scheuen-zusammenarbeit-nach-cyberangriff> (zuletzt besucht am 12.06.2025)

<sup>11</sup> <https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2023.html> (zuletzt besucht am 12.06.2025)

<sup>12</sup> Zum Beispiel <https://background.tagesspiegel.de/cybersecurity/mit-transparenz-erreichen-unternehmen-mehr-als-mit-verschleierungstaktik> (zuletzt besucht am 12.06.2025)

<sup>13</sup> <https://background.tagesspiegel.de/cybersecurity/cyberangriffe-zwei-unternehmen-berichten> (zuletzt besucht am 12.06.2025)

<sup>14</sup> <https://www.itdz-berlin.de/aktuelles/franziska-giffey-eroeffnet-security-operations-center-im-itdz-berlin-1196292.php> (zuletzt besucht am 12.06.2025)

<sup>15</sup> [https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L\\_202500038](https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202500038) (zuletzt besucht am 12.06.2025)

<sup>16</sup> <https://background.tagesspiegel.de/cybersecurity/proaktiver-schutz-mit-einem-cyber-defense-center> (zuletzt besucht am 12.06.2025)

und Mitarbeiter dies tun. Für die Etablierung einer tatsächlichen Cybersicherheitskultur braucht es mitunter eine individuelle Ansprache und niedrighschwellige 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 Teilnehmenden 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 4.2)
- 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 4.1)

### 3.3 Herausforderungen vernetzter OT-Systeme angehen und Harmonisierung von Zertifizierungen vorantreiben

#### **Aktueller Stand:** Abgeschlossen

Die Themen „Herausforderungen vernetzter OT-Systeme angehen“ und „Harmonisierung von Zertifizierungen vorantreiben“ wurden gemeinsam bearbeitet, da sie inhaltlich eng miteinander verknüpft sind. Das Thema wurde mit der Studie „Cybersicherheits-Zertifizierungen vernetzter Systeme in der Energiewirtschaft“ im September 2025 abgeschlossen.

Ziel der Studie ist es, eine praxisorientierte Übersicht über die bestehenden Zertifizierungen im Bereich Cybersicherheit zu geben und daraus mögliche Ansätze zur Harmonisierung und Vereinfachung abzuleiten. Die Übersicht dient den Mitgliedern der Branchenplattform als Orientierungshilfe. Im zweiten Teil der Studie werden konkrete Herausforderungen eines integrierten Stadtwerks vor allem in Bezug auf langfristige Update-Fähigkeit und Sicherheit im Smart-Meter-Bereich systematisch aufbereitet, um ein besseres Verständnis für bestehende Problemstellungen zu schaffen.

#### **Wesentliche Ergebnisse**

- Die Trennung zwischen verschiedenen Zertifizierungsregimen – etwa nach EnWG, § 8a BSIG oder Technischen Richtlinien – führt häufig zu Doppelprüfungen. Ein modular aufgebautes Zertifizierungssystem mit anschlussfähigen Grund- und Zusatzmodulen sowie die gegenseitige Anerkennung etablierter Standards wie ISO/IEC 27001 oder BSI-Grundschutz könnten hier substantielle Entlastung schaffen. Auch die gezielte Wiederverwendung bereits geprüfter Prüfelemente (PE) würde den Aufwand reduzieren.
- Derzeit existieren kaum offizielle Mappings zwischen nationalen (§ 8a BSIG), internationalen (ISO/IEC) und europäischen (z. B. EUCS, EUCC, CRA) Standards. Diese Unverbundenheit erschwert nicht nur die Nachweispraxis, sondern auch die internationale Vergleichbarkeit. Klare Anrechnungstabellen und die verpflichtende Integration sektoraler Normen wie ISO/IEC 27019 würden die Praxisnähe und Kohärenz der Prüfungen erhöhen.
- Viele Unternehmen lassen bereits mehrere Anforderungen in einem kombinierten Audit prüfen – zum Beispiel ISO 27001 und ISO 22301. Allerdings fehlt häufig die regulatorische Anerkennung solcher Kombi-Zertifikate. Eine formelle Zulassung dieser Bündelungen würde Synergien heben und Prüfzyklen reduzieren.

Die Studie wurde in Zusammenarbeit mit der c.con Management Consulting GmbH und dem OFFIS e.V. erstellt.

#### **Herausforderungen von vernetzten OT-Systemen angehen**

Die Digitalisierung im Energiesektor verbindet auch zunehmend IT<sup>17</sup>- mit OT-Komponenten<sup>18</sup>. 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-

<sup>17</sup> IT = Informational Technology; Hardware und Software zur elektronischen Datenverarbeitung (z. B. die Speicherung, Übertragung und Verwendung von digitalen Informationen für Zwecke des Geschäftsbetriebs)

<sup>18</sup> OT = Operational Technology; Hardware und Software zur Steuerung und Kontrolle von physischen Prozessen und Geräten (wie z. B. Anlagen)

Systeme können auch über Schnittstellen zu anderen Systemen verfügen, um etwa zu evaluieren, wie sich Schalthandlungen auf Stromleitungen oder Transformatoren auswirken (acatech/Leopoldina/Akademienunion, 2021).

Die Vielzahl an Optionen, die sich aus vernetzten OT-Systemen ergeben, ist mit weiteren technischen Möglichkeiten, politischen Vorhaben und sicherheitskritischen Herausforderungen verbunden. Dazu gehören die Sektorenkopplung, die Energiewende und die Zunahme an kleinen Energieerzeugern. Beim Übergang zwischen Sektoren treten weitere Herausforderungen auf: Zusätzlich zur Sicherstellung einer Interoperabilität verschiedener IT-Systeme müssen unterschiedliche Sicherheitsanforderungen und Risikobewertungen vereint werden, um die Funktionalität der Sektorenkopplung zu gewährleisten. Über die in diesem Zusammenhang relevanten Themen geben wir in der grau hinterlegten Box einen Überblick.

### **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 Speichereinrichtungen miteinander zu verknüpfen und zu analysieren. Dies wäre hilfreich, um etwa die Energieeffizienz zu steigern sowie Energieüberschüsse und -mängel 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<sup>19</sup> liegt. Seit dem 01.01.2025 hat in Deutschland ein Smart-Meter-Rollout begonnen<sup>20</sup>. Aktuell besteht jedoch durch das Fehlen einer zentralen Lese- und Steuerzentrale die Möglichkeit, großflächigen Schaden zu erzeugen.

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

<sup>19</sup> <https://iot-analytics.com/smart-meter-adoption/> (zuletzt besucht am 07.01.2025)

<sup>20</sup> <https://www.bmwk.de/Redaktion/DE/Infografiken/Energie/infografik-smart-meter-rolloutfahrplan.html> (zuletzt besucht am 12.06.2025)

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-Grundschatz 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.

## Die Harmonisierung von Zertifizierungen vorantreiben

Die Gesetzgebung gibt Betreibern Kritischer Infrastrukturen vor, welche Sicherheitsanforderungen sie zu erfüllen haben (vgl. Kapitel 3.4). 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.<sup>21</sup>

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.<sup>22</sup> 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 Teilnehmenden der Branchenplattform dürfte es besonders interessant sein, sich über Änderungen auszutauschen, die mit dem NIS2UmsuCG 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.
  - 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.

---

<sup>21</sup> <https://background.tagesspiegel.de/cybersecurity/wie-wirksam-sind-die-it-sicherheitsgesetze> (zuletzt besucht am 12.06.2025)

<sup>22</sup> [https://www.openkritis.de/r/OpenKRITIS\\_Mapping\\_KRITIS-Cyber-Security.pdf](https://www.openkritis.de/r/OpenKRITIS_Mapping_KRITIS-Cyber-Security.pdf) (zuletzt besucht am 12.06.2025)

### **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 nur die 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 3.4) 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.

### 3.4 Transparenz in der Gesetzgebung erhöhen

#### **Aktueller Stand:** Abgeschlossen

Das Thema „Transparenz in der Gesetzgebung erhöhen“ wurde im September mit der Studie „NIS2-Roadmap für Energie-Start-ups“ abgeschlossen.

Ziel der Studie ist es, ein besseres Verständnis für die Anforderungen und Herausforderungen der NIS2-Richtlinie zu schaffen, insbesondere für Unternehmen, die durch Lieferkettenabhängigkeiten indirekt betroffen sind. Im Zeitraum Q2 bis Q3 2025 wurde ein zweimonatiges Mentoring-Programm mit sechs Start-ups und KMUs der Stromwirtschaft durchgeführt. Dabei wurden die Maßnahmen der NIS2-Richtlinie erprobt, priorisiert und in praxisorientierte Formate überführt. Darauf aufbauend wurde eine NIS2-Umsetzungs-Roadmap erarbeitet. Sie richtet sich an Start-ups und kleine Unternehmen (KMUs) in der Stromwirtschaft, die nicht direkt unter die NIS2-Richtlinie fallen, jedoch in Zusammenarbeit mit regulierten Akteuren – zum Beispiel als Zulieferer oder Dienstleister – mittelbar betroffen sind. Ziel ist es, diesen Unternehmen eine praxisnahe Orientierungshilfe bereitzustellen, die auf die spezifischen Anforderungen und Herausforderungen in ihrer betrieblichen Realität eingeht.

#### **Wesentliche Ergebnisse**

- 100 Prozent der teilnehmenden Unternehmen gaben an, durch das Mentoring relevante Informationen erhalten zu haben, die eine eigenständige Umsetzung ermöglichen.
- Die Verbindung aus interaktiven Formaten, Gruppenaustausch und technischer Expertise wurde von der Zielgruppe als besonders hilfreich bewertet.
- Abstrakte Anforderungen wurden entmystifiziert und das Sicherheitsbewusstsein und die Umsetzungsfähigkeit der Teilnehmenden gestärkt.
- Es wurde eine Roadmap veröffentlicht, die allen interessierten Akteuren zugänglich ist und praktische Umsetzungstipps bietet.

Die Studie wurde in Zusammenarbeit mit der intcube GmbH, der Gesellschaft für Informatik e.V. und Cyber Policy Haus BV erstellt.

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.

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]“<sup>23</sup>. 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.<sup>24</sup>

<sup>23</sup> <https://www.bundestag.de/resource/blob/984658/767a3abc17eed5a9eae39377204dc052/27-Sitzungsprotokoll-mit-Anlagen-OeA.pdf> (zuletzt besucht am 06.11.2024)

<sup>24</sup> <https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/streit-um-schwellenwerte> (zuletzt besucht am 14.10.2024)

Diesen Wunsch teilen auch Beteiligte am Themenroadmap-Prozess. 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.

## **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 durch das NIS2UmsuCG 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 (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. Die NIS2-Richtlinie weitet Cybersicherheitsvorgaben auf mehr (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 mehr als 30.000. Damit fallen in Deutschland Zehntausende Unternehmen erstmals unter die EU-Regulierung.

Für die Umsetzung der Richtlinie in Deutschland legte das Bundesministeriums des Innern (BMI) im Juni 2025 einen neuen Referentenentwurf für ein NIS2UmsuCG vor, das das BSI-Gesetz erweitern wird. Anfang Juli fand eine Anhörung mit Interessensverbänden zum Referentenentwurf statt. Mit der NIS2-Betroffenheitsprüfung des BSI können Unternehmen in wenigen Schritten schon jetzt herausfinden, inwiefern sie Maßnahmen ergreifen müssen.

Gleichzeitig zur NIS2-Richtlinie 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 (der Referentenentwurf des Bundesministeriums des Innern (BMI) wurde zuletzt im Dezember 2024 im Bundestag beraten).

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 betroffen sein.

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

- Die Teilnehmenden wünschen sich klare Ansprechpersonen auf Behördenseite (BSI, BNetzA). Mit der Branchenplattform könnte eine Übersicht über relevante Anlaufstellen erstellt sowie weitergehende Wünsche der Teilnehmenden 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<sup>26</sup> 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 überarbeitete Whitepaper zu „Sicherheitsanforderungen für IT und Steuerungstechnik in der Energiewirtschaft“, in dem regulatorische Anforderungen aufgeführt und Hilfestellungen für ihre Umsetzung gegeben werden.

<sup>25</sup> <https://www.eco.de/presse/cybersicherheit-nur-wenige-unternehmen-in-deutschland-sind-auf-nis2-vorbereitet/> (zuletzt besucht am 13.06.2025)

<sup>26</sup> <https://inrapol.org/wp-content/uploads/2017/02/Kipker-DuD-2016-Unbestimmte-Rechtsbegriffe.pdf> (zuletzt besucht am 26.10.2024)

- 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. Der Navigator geht aus einem vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR, ehemals Bundesministerium für Bildung und Forschung) 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.

## 4 Was wir mitnehmen: vier zentrale Handlungsfelder

Die Bedeutung von Cybersicherheit in der Stromwirtschaft steigt immer weiter, wie auch das BSI betont: Die fortschreitende Digitalisierung und Dezentralisierung des Energiesektors vergrößert die Angriffsfläche für Cyberbedrohungen<sup>27</sup>. Dementsprechend lang ist die Liste an weiteren Themen, die im Rahmen der Themenroadmap und bei weiteren Treffen der Branchenplattform Cybersicherheit in der Stromwirtschaft erarbeitet wurden. Bei einigen Themen bietet es sich an, sie mit in Projekte zu integrieren, anstatt sie als eigenständiges Thema hervorzuheben:

- **Bedürfnisse kleiner Unternehmen:** Dieser Punkt sollte nicht hintenüberfallen, sondern, wie bereits vorgeschlagen, bei der Umsetzung von Formaten mitgedacht werden. So können beispielsweise bei Veranstaltungen Plätze für KMUs oder Start-ups freigehalten oder solche Unternehmen bei Befragungen berücksichtigt werden.
- **Neue Technologien beachten:** Auch hier empfiehlt es sich, bei der Umsetzung der oben genannten Punkte neue Technologien mitzudenken und wenn möglich einzubinden, anstatt einen gesonderten Schwerpunkt zu setzen.

Die übrigen Themen wurden mit dem Partnerkreis diskutiert und zu vier zentralen Handlungsfeldern zusammengeführt. Im Folgenden stellen wir diese vor und geben einen kurzen Einblick, welche Hintergründe ihnen zugrunde liegen. Die Reihenfolge der Themenfelder entspricht der Priorisierung, die zusammen mit den Partnern der Branchenplattform getroffen wurde.

### 4.1 Herausforderungen in IT-Sicherheit in Vergaberecht, Einkauf und Lieferkette bündeln

Vor dem Hintergrund neuer geopolitischer Gegebenheiten rückt mit der fortschreitenden Dezentralisierung der Stromwirtschaft, unter anderem durch digitale Energiedienste, die Sicherheit der (IT-)Lieferketten in den Fokus. Es gilt, Abhängigkeiten von einzelnen Lieferanten und Ländern sowie das Vertrauen in Zulieferer bereits im Einkauf zu berücksichtigen. Dies lässt sich sowohl unternehmensseitig als auch politisch adressieren. Die Branchenplattform kann eine kritische Reflexion der Anforderungen an die Vergabe bewirken und diese Erkenntnisse nutzen, um Unternehmen in ihrem Einkauf zu unterstützen. Hier kann auch eine technische Wissensbasis zur Bedrohungsclassifikation helfen: Geht von bestimmten Komponenten ein erhöhtes Sicherheitsrisiko aus, können sich Unternehmen besser präventiv gegen mögliche Bedrohungen schützen. In diesem Bereich wird von den Partnern der Branchenplattform der stärkste Handlungsdruck gesehen.

Dieses Handlungsfeld beinhaltet die folgenden Einzelthemen:

#### **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

---

<sup>27</sup> [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier\\_Cybersicherheit\\_Energiesektor.pdf?](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.pdf?)

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. Nach dem Pager-Angriff auf die Hisbollah im September 2024 gilt die Aufmerksamkeit auch zunehmend Hardwarekomponenten. 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. 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.

Ein Unternehmen kann sich mittels eines Supply-Chain-Risikomanagements vor vielen Risiken schützen. 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 diese Diskussion anknüpfend an die ohnehin vom BMWV angestrebte Reform des Vergaberechts aufgreifen. Die Reform befindet sich im Sofortprogramm der neuen Bundesregierung, hat also entsprechende Priorität. Es können Best Practices aus anderen Branchen geprüft und adaptiert werden (z.B. TISAX im Automobilbereich). Der Partnerkreis sprach sich insbesondere auch für Templates für bzw. Standardisierung von Fragenkatalogen im Kontext der Dienstleisterqualifikation aus.

### **Lieferkette und Einkauf als eigene Herausforderung**

Sowohl für Unternehmen, die KRITIS betreiben, als auch für ihre Lieferanten stellt der Einkauf eine eigene Herausforderung dar: Gesetzliche Anforderungen wie der CRA oder NIS2 erzeugen immer wieder Fragen und Unklarheiten. Anbieter, die nicht unmittelbar von gesetzlichen Vorgaben betroffen sind, aber betroffene Unternehmen beliefern, stehen vor der Herausforderung, sich in diversen Paragrafen Antworten suchen zu müssen. Präqualifikation und die zentrale Ablage von Nachweisen könnten helfen, die Lieferkette abzusichern. Die Branchenplattform kann durch Austausch und Wissensaufbereitung Unsicherheiten auf beiden Seiten entgegenwirken und Lösungen aufzeigen. Ähnlich wie beim Handlungsfeld „IT-Sicherheit als Kriterium in Vergabeprozessen aufwerten“ (vgl. Kapitel 4.7) spielen Standardisierung und Zertifizierung eine herausragende Rolle. Insbesondere im Bereich der kritischen Komponenten bestehen aktuell große Unsicherheiten.

### **Komplexe Compliance verständlich machen**

Besonders für kleine und junge Unternehmen mit wenig zeitlichen oder personellen Kapazitäten sind Anforderungen aus neuen Gesetzen schwerer umzusetzen. Sie haben Schwierigkeiten, die für sie relevanten Anforderungen zu identifizieren, und haben die Sorge, bei der Umsetzung Fehler zu machen. Aber auch für etablierte Unternehmen können neue Gesetze schwer zu durchdringen sein. Die Teilnehmenden des Branchenplattform-Treffens wünschen sich daher klare Standards, die sich aus solchen Anforderungen ergeben, und dass diese für sie besser überblickbar gemacht werden. Hierbei können beispielsweise standardisierte Nachweisdokumente zur Erfüllung der Vorgaben der NIS2-Richtlinie dabei helfen, den Aufwand durch individuell erstellte Fragenkataloge zu reduzieren (vgl. Kapitel 4.7). Ebenso wünschen sie sich Formate, die Wissen zur Gesetzgebung zugänglich machen, etwa durch Handreichungen, Checklisten

oder KI-basierte Lösungen, die zentral zur Verfügung stehen. Bei der Ausarbeitung der Inhalte könnte das Fachwissen von Auditoren und Prüfern mit einbezogen werden.

## **4.2 Dezentrale Energieversorgung durch Testlabore sichern**

Aufdach-Photovoltaik-Anlagen liegen weiterhin im Trend, ebenso der Ausbau von Balkonkraftwerken. Auch mit Blick auf den jetzt beginnenden Smart Meter Rollout nimmt die Bedeutung der dezentralen Energieerzeugung und -versorgung weiter zu und sollte daher mit geeigneten Formaten begleitet werden. Mögliche Softwarelösungen zum Schutz vernetzter Systeme in Testlaboren zu untersuchen, bietet die Möglichkeit, eigene Lösungen zu entwickeln und zu erproben: ein weiterer Schritt auch in Richtung einer resilienten und unabhängigen Lieferkette.

Dieses Handlungsfeld beinhaltet die folgenden Einzelthemen:

### **Testmöglichkeiten ausbauen**

Die Beteiligten des Themenroadmap-Prozesses wünschen sich einen Ausbau von Testmöglichkeiten wie in Testlaboren. Innovative Systeme sind oft nicht ausreichend getestet, was ihren Einsatz als Alternative zu alten aber stabil laufenden Systemen erschwert. Die Branchenplattform bietet unterschiedliche Möglichkeiten zur Erweiterung von Testangeboten in der Stromwirtschaft. Es können Anforderungen an Testlabore, insbesondere zur IT-/OT-Schnittstelle, gesammelt und erste Schritte zu deren Einrichtung unternommen werden, was die Plattform zu einem zentralen Instrument für die Weiterentwicklung der Stromwirtschaft macht.

### **Dezentrale Stromversorgung und neue Angriffsvektoren**

Mit der stark gestiegenen Verbreitung von Photovoltaik-Anlagen sowie dem Ausbau digitaler Energiedienste wird die Stromerzeugung zunehmend dezentralisiert. Um eine angemessene Auslastung des Stromnetzes zu erreichen, werden die Erzeuger vor allem digital vernetzt. Diese Dezentralität bringt gleich mehrere Bedrohungsszenarien mit sich, die beim Plattformtreffen genannt wurden: Berichte über Backdoors in Wechselrichtern oder Zugriffsmöglichkeiten über Hersteller-Clouds lassen die Sorge entstehen, sie könnten durch einen gezielten Angriff manipuliert werden und damit das Stromnetz destabilisieren. Eine ähnliche Sorge besteht mit Blick auf smarte Energiekleinanlagen und digitale Energiedienste. Die Branchenplattform kann helfen, indem sie beispielsweise Handreichungen für ihre Mitglieder entwickelt, die über bestehende Risiken aufklären (zum Beispiel in Form eines Gefährdungskatalogs) sowie Schutzmöglichkeiten und Handlungsoptionen aufzeigen.

## **4.3 Die interne Organisation, das grundlegende Sicherheitsmanagement und den Fachkräftemangel gemeinsam angehen**

Mit einer Verbesserung von internen Unternehmensstrukturen können interne Prozesse verbessert werden, sodass die Beschäftigten effektiver arbeiten können. Über die Branchenplattform können neue Impulse zur Unternehmensorganisation ausgetauscht werden: Neben einer Wissensvermittlung durch klassische Seminare kann durch das Miteinander verschiedener Plattform-Teilnehmenden ein horizontaler Wissensaustausch entstehen. Dieser Austausch kann ebenso das grundlegende Sicherheitsmanagement betreffen und dabei Weiterbildungsmöglichkeiten beinhalten. Ein positives Betriebsklima und gute Unternehmensstrukturen machen ein Unternehmen zudem attraktiver für interessierte Fachkräfte.

Dieses Handlungsfeld beinhaltet die folgenden Einzelthemen:

### **Weiterbildungsmöglichkeiten ausbauen**

IT-Sicherheit im eigenen Unternehmen hängt stark mit der Awareness der Beschäftigten für das Thema zusammen. Außerhalb des IT-Sektors finden diese Übungen jedoch selten statt. Auch im Stromsektor und insbesondere in kleineren Unternehmen finden Sicherheitsübungen nur selten oder unregelmäßig statt. Entsprechend wünschten sich die Teilnehmenden mehr regelmäßige Weiterbildungen und Trainings zu Cybersicherheit. Dabei könnten neben klassischen (Online-)Seminaren und Schulungen etwa Security-Awareness- und Phishing-Tests durchgeführt werden. Die Nachhaltigkeit der Lerneffekte wird jedoch selten untersucht.

Cybersicherheitsvorfälle können auch nachgestellt und in inszenierten Situationen geübt werden. Es gibt inzwischen verschiedene Anbieter von Serious Games, die sich an öffentliche oder Unternehmensstrukturen richten und Tabletop Exercises, die auf die speziellen Bedürfnisse von Organisationen eingehen. Solche Krisenübungen können unternehmensintern als auch sektorenübergreifend stattfinden, wie die „Länder- und Ressortübergreifenden Krisenmanagementübungen“ (LÜKEX), die im Abstand von wenigen Jahren stattfinden und bspw. 2023 einen Cyberangriff simulierte. Hierbei sollte geprüft werden, inwiefern auch relevante Dienstleister eingebunden werden können. Mit diesen Übungen testet man die Reaktionsfähigkeit und Resilienz der Teilnehmenden wie Unternehmensmitarbeiterinnen und -mitarbeiter oder andere Akteure wie dem Technischen Hilfswerk auf verschiedenen operativen Ebenen. Solche Übungen bilden die Ausgangslage, um Veränderungen im Umgang mit Cyberrisiken anzustoßen. Ergebnisse und Learnings aus einzelnen Übungen sollten auch einer zentralen Wissensbasis zugeführt werden.

### **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 Teilnehmenden verbanden dieses Thema vor allem mit praktischen Problemen dabei, gesetzliche Anforderungen umzusetzen (vgl. Kapitel 3.4). Umsetzungsprobleme können außerdem einer unzureichenden Sensibilisierung geschuldet sein (vgl. Kapitel 3.1). Hierzu sollte eine Status-Quo-Analyse durchgeführt werden, um Hürden bei der Umsetzung zu identifizieren und Lösungen unter Einbezug bestehender und anerkannter Standards zu entwickeln.

### **Dem Fachkräftemangel begegnen**

Der Fachkräftemangel wird zwar auf politischer Ebene immer wieder thematisiert. 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. Hier 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). Mögliche Fokusthemen sind das Einbinden von

Ausbildungsstätten (Schulen, Universitäten), Einsatz von KI, Aufzeigen von Karrierewegen und Mentoring insbesondere für Quereinsteiger.

### **Interne Organisation verbessern**

Aufgrund der sich stetig verändernden Bedrohungslage und immer schnellerer Innovationsprozesse wünschen sich die Teilnehmenden des Branchenplattform-Treffens bessere Aus- und Weiterbildungsmöglichkeiten. Dabei steht neben technischen Herausforderungen auch die Umsetzung organisatorischer Maßnahmen im Vordergrund: darunter ein Neudenken von Organisationskultur mit dem Ziel, Cybersicherheit nicht als bloße Compliance-Maßnahme zu begreifen, sondern als intrinsische Motivation zu etablieren. Dabei wurden Austauschformate vorgeschlagen, um einen Best-Practice-Austausch (aus beispielsweise ISMS, Change Advisory Board, Business Continuity Management und Prüfzyklen) voranzubringen.

## **4.4 Sektorenkopplung und -erweiterung betrachten**

Die Ausweitung auf andere Sektoren bzw. auf die gesamte Energiewirtschaft inklusive Gas, Wasserstoff und Wärme birgt weitere Herausforderungen von der OT-Security bis zur physischen Sicherheit von Energiespeichern, Energienetzen oder Kraftwerken. Die Energieerzeuger hängen oft miteinander zusammen, wie bei der Produktion von grünem Wasserstoff durch Strom aus erneuerbarer Energie. Mit einer erweiterten Branchenplattform kann der bisher nicht betrachtete Punkt der Sektorenkopplung angegangen werden.

Dieses Handlungsfeld beinhaltet die folgenden Einzelthemen:

### **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 geführte 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 und Synergieeffekte der branchenübergreifenden Zusammenarbeit herauszuarbeiten.

### **Branchenplattform als Austauschort ausbauen und erweitern**

Die Teilnehmenden des Plattformtreffens sind sich einig, dass die Branchenplattform zu einem wichtigen Austauschort und Impulsgeber für sie geworden ist. Die veröffentlichten Studien und weitere Formate konnten ihnen wichtige Informationen und Erkenntnisse vermitteln.

Ebenso wurde die Idee aufgeworfen, die Branchenplattform auf die gesamte Energiewirtschaft auszuweiten, also neben der Stromwirtschaft auch Gas-, Wasserstoff- und Wärmenetze und -anlagen sowie die entsprechende Akteurslandschaft in den Blick zu nehmen. Diese Erweiterung kann sinnvolle Synergien schaffen, um die Energiewirtschaft umfassend resilienter gegen Cyberbedrohungen zu gestalten. Die Teilnehmenden des Treffens wünschen sich, auch mit dieser Vergrößerung die Plattform zu verstetigen und das Engagement auf der Plattform langfristig sicherzustellen. Dabei ist neben einem horizontalen Austausch auch explizit ein vertikaler Austausch, also entlang der Supply Chain, gewünscht. Ebenfalls besteht der Wunsch nach weiteren externen Impulsen wie beispielsweise von Auditoren und Prüfern (vgl. Kapitel 4.11).

### **Schnittstellen zur physischen Sicherheit berücksichtigen**

Auf dem Plattformtreffen wurde schließlich auch der Zusammenhang von Cyber- und physischer Sicherheit für Unternehmen, besonders im KRITIS-Bereich, betont, der zu wenig Beachtung erfährt. Häufig sind die entsprechenden Zuständigkeiten in den Unternehmen gebündelt, sodass sich Synergieeffekte erzielen lassen könnten. Zudem kann eine Cyberbedrohung auch einen Angriff auf physische Infrastruktur beinhalten. Als zentrale Anlaufstelle zwischen Unternehmen könnte die Branchenplattform entsprechende Bedrohungsanalysen und Lösungen sowie Handreichungen und Best Practices insbesondere auch im Kontext ganzheitlicher Resilienzkonzepte erarbeiten und im Austausch mit den Mitgliedern kontinuierlich weiterentwickeln.

## 5 Fazit und Empfehlungen

Die Themenroadmap schafft für die Branchenplattform Cybersicherheit in der Stromwirtschaft eine Grundlage für einen zielgerichteten Multi-Stakeholder-Dialog. In der ersten Fassung wurden mehrere Themen identifiziert, die für die Stromwirtschaft von besonderer Relevanz sind. Basierend darauf wurden vier Projekte durchgeführt (vgl. Kapitel 3). Die Ansatzpunkte der Projekte sind vielfältig und die Ergebnisse wirken auf verschiedenen Ebenen:

- Für Führungskräfte wurde eine Handreichung erarbeitet auf Basis derer Entscheidungen zu Investitionen in Cybersicherheitsmaßnahmen besser bewertet werden können (vgl. Kapitel 3.1).
- Damit sich Unternehmen untereinander und über alle Ebenen hinweg besser austauschen können, wurden Lern- und Austauschformate entwickelt und erprobt (vgl. Kapitel 3.2).
- Um den Zertifizierungsprozess zu erleichtern, wurden Synergiepotenziale in den aktuellen Zertifizierungssystemen herausgearbeitet (vgl. Kapitel 3.3).
- Zur Bewältigung der bevorstehenden Umsetzung der Vorgaben aus der NIS2-Richtlinie wurde gemeinsam mit der Branche eine praxisnahe Roadmap entwickelt (vgl. Kapitel 3.4).

Cybersicherheit ist eine ganzheitliche Herausforderung, die sowohl auf Unternehmens- als auch auf Bundesebene aus unterschiedlichen Perspektiven beleuchtet und im Zusammenspiel vielfältiger Akteure mit unterschiedlichen Rollen und Verantwortlichkeiten gestaltet werden muss. Die Branchenplattform bietet dieser Vielfalt einen Raum und widmet sich neben den prägenden Diskursen etablierter Stimmen auch weniger sichtbaren Akteuren und weniger beachteten, gleichwohl entscheidenden Fragestellungen der Cybersicherheit.

Im Rahmen dieser Arbeit wurden in partizipativen Prozessen viele weitere Themen identifiziert und diskutiert. Diese wurden in vier zentrale Handlungsfelder zusammengefasst und priorisiert (vgl. Kapitel 4). Es spiegelt sich auch darin der Kerngedanke der Branchenplattform wider:

- Das Spannungsfeld von digitaler Souveränität und Abbau von Bürokratie in Vergabeprozessen auflösen (vgl. Kapitel 4.1). Die Branchenplattform kann dabei als Vermittler zwischen Politik und Wirtschaft agieren, um politische Ziele und unternehmerische Realitäten in Einklang zu bringen.
- Testlabore im Kontext der Dezentralisierung evaluieren sowie die Sicherheit von Heim-Photovoltaik-Anlagen untersuchen (vgl. Kapitel 4.2). Hierbei kann die Branchenplattform als Impulsgeber agieren und auf zukünftige Herausforderungen aufmerksam machen.
- Die Verbesserung interner Unternehmensstrukturen anstoßen und bei der Etablierung einer Cybersicherheitskultur mitwirken (vgl. Kapitel 4.3). Die Branchenplattform kann hierfür in einem ganzheitlichen Ansatz verschiedene Akteure mit unterschiedlichen Rollen und Perspektiven zusammenbringen.
- Neue Herausforderungen bei der Sektorenkopplung identifizieren (vgl. Kapitel 4.4). Dabei kann die Branchenplattform an geeigneten Stellen über die Grenzen der Stromwirtschaft hinausschauen und Transferwissen für andere Sektoren der Energiewirtschaft bereitstellen.

In der Gesamtschau wird deutlich, dass die Arbeit der Branchenplattform von drei wesentlichen Treibern geformt wird:

- Die Umsetzung der NIS2-Richtlinie und dessen Implikationen.
- Das Voranschreiten der Energiewende mit Dezentralisierung und Sektorenkopplung.
- Der Kulturwandel beim Thema Cybersicherheit bedingt durch die Zeitenwende.

Diese Treiber sind nicht als einzelne Faktoren zu betrachten, sondern wirken in Realität eng verzahnt ineinander und miteinander. Die Branchenplattform will dieses Momentum nutzen um im Sinne der Vision einer Cybernation Deutschland<sup>28</sup> dabei zu unterstützen „vor die Welle“ zu kommen.

### **Empfehlungen der Gesellschaft für Informatik e.V. für die Branchenplattform**

Für eine noch bessere Wirkung in der Energiebranche ist es sinnvoll, den Kreis der Branchenplattform-Mitglieder auf weitere Formen der Energieversorgung zu erweitern. Mit der erfolgreichen Umsetzung von vier Projekten hat sich die Branchenplattform zum wichtigen Austauschort für ihre Mitglieder in der Energiebranche entwickelt und kann für zukünftige Projekte auf dieser Erfahrung aufbauen. Die Gesellschaft für Informatik e.V. empfiehlt daher, die Bedeutung der Branchenplattform als zentralen Austausch- und Wissensort für die Branche anzuerkennen und weiterhin zu fördern. Die Plattform kann Raum schaffen, sich frühzeitig mit zu erwartenden Veränderungen zu befassen, und damit vielen Beteiligten langfristig Vorteile bringen.

### **Empfehlungen aus drei Jahren Branchenplattform**

- **Unter strategischer Leitung des BSI voranschreiten:** Die Zentralstelle BSI fungiert als Wegweiser durch die facettenreiche Landschaft der Cybersicherheit. In unserer Arbeit konnten wir feststellen, dass das BSI als solche anerkannt und gewürdigt wird. Wir schließen uns dieser Haltung an.
- **Einbezug verschiedener Perspektiven von vielfältigen Akteuren:** Cybersicherheit ist ein ganzheitliches Thema, das weit über die technische Umsetzung hinausgeht. Wir erhalten sehr positives Feedback auf besonders gemischten Veranstaltungen mit dem Hinweis, dass ein interdisziplinärer Austausch als sehr bereichernd wahrgenommen wird. Dieses Feedback möchten wir teilen und bestärken.
- **Den Redebedarf der Branche mit interaktiven Formaten katalysieren:** Veranstaltungen leben von einem aktiven Austausch. Zu keinem Zeitpunkt konnten wir einen Mangel an Wortmeldungen auf unseren Veranstaltungen feststellen. Experimentelle Veranstaltungsformate sind bei unserem Publikum sehr gut angekommen. Wir möchten dazu ermutigen sich von traditionellen Formaten zu lösen und auf das Engagement der Branche zu vertrauen.
- **Konstruktiv kritisch und vertrauensvoll miteinander umgehen:** Sich ehrlich machen, auf Missstände hinweisen, eigene Fehler akzeptieren und gemeinsam nach besseren Lösungen suchen. Das erfordert Mut und eine vertrauensvolle Atmosphäre. Wir plädieren dafür destruktive Schuldzuweisungen zu vermeiden und sich nicht von der Angst vor Reputationsverlust davon abhalten zu lassen eigene Fehler zuzugeben, um anderen diese zu ersparen.

---

<sup>28</sup> [https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation\\_node.html](https://www.bsi.bund.de/DE/Das-BSI/Cybernation/cybernation_node.html)

- **Frauen in der Cybersicherheit sichtbarer machen:** Nicht nur auf unseren Veranstaltungen sind Frauen im Publikum weit in der Unterzahl. Wir empfehlen, Frauen an Mikrofone und auf Bühnen zu holen, um weibliche Vorbilder sichtbarer zu machen.

Diese Empfehlungen formulieren wir nicht nur für die Branche, sondern auch für uns. Wir möchten uns entlang dieser Erkenntnisse weiterentwickeln und noch besser in unsere Arbeit integrieren. Es bleibt viel zu tun, doch die steigende Bedeutung des Themas und die hohe Motivation der Branche bilden eine starke Grundlage für die nächsten Schritte.

## **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 der Stakeholder der Branchenplattform. Sie werden zunächst einzeln zu ihren Einschätzungen befragt. Dies wurde durch eine im Folgenden beschriebene Umfrage umgesetzt. Anschließend wurden 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 erhielten 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.

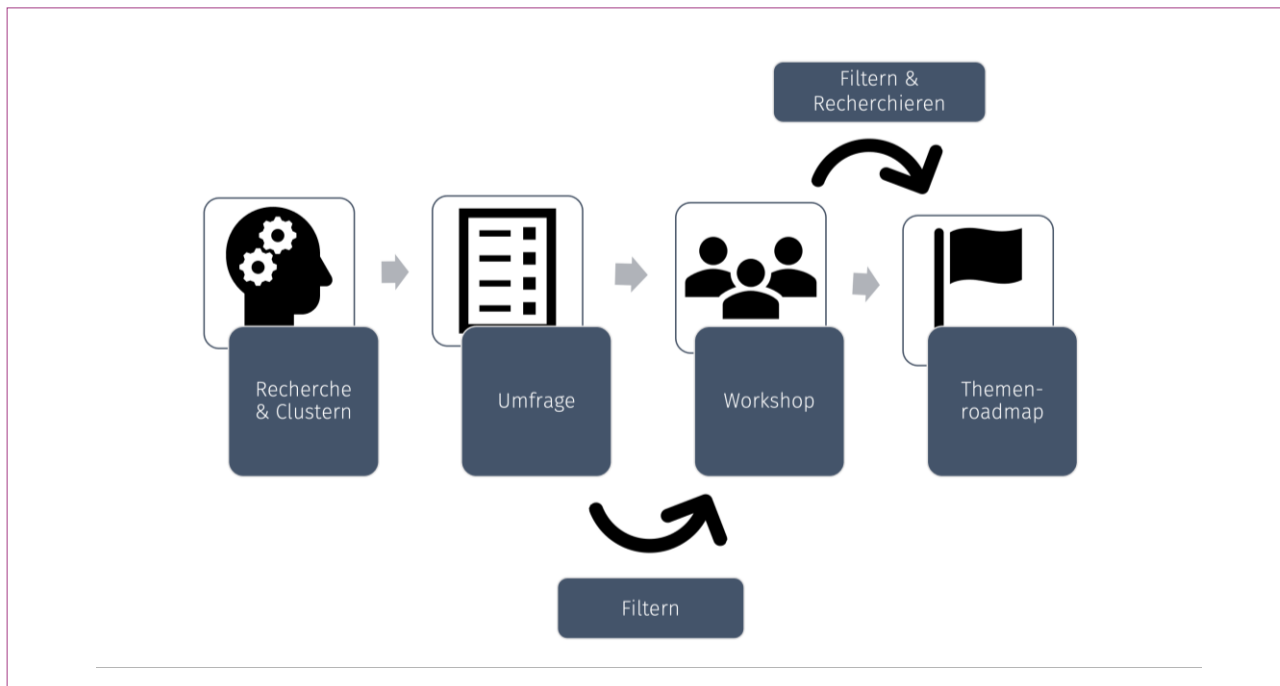


Abbildung 1 Skizzierter Prozess der Themenroadmap

## Eine strukturierende Basis mit dem ENISA-Framework

Zur Strukturierung der Themen haben wir uns an das ENISA-Framework zur Bewertung nationaler IT-Sicherheitsfähigkeiten<sup>29</sup> 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

<sup>29</sup> <https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-de.pdf> (zuletzt besucht am 23.10.2024)

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

- A) Governance und Standards im Bereich der Cybersicherheit
- B) Kapazitätsaufbau 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 „**Kapazitätsaufbau 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 angelegten 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 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 <b>kleine Unternehmen</b> verbindliche Vorgaben zur Cybersicherheit entwickeln und diese kontrollieren.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Meiner Organisation sind die existierenden gesetzlichen <b>Vorgaben zur Cybersicherheit zu unkonkret</b> . Ich wünsche mir präzise Vorgaben.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Die Stromwirtschaft ist nicht auf die erhöhte Gefahr von Cyberangriffen durch den flächendeckenden <b>Einsatz von Smart-Metern</b> vorbereitet.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 Teilnehmende 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.

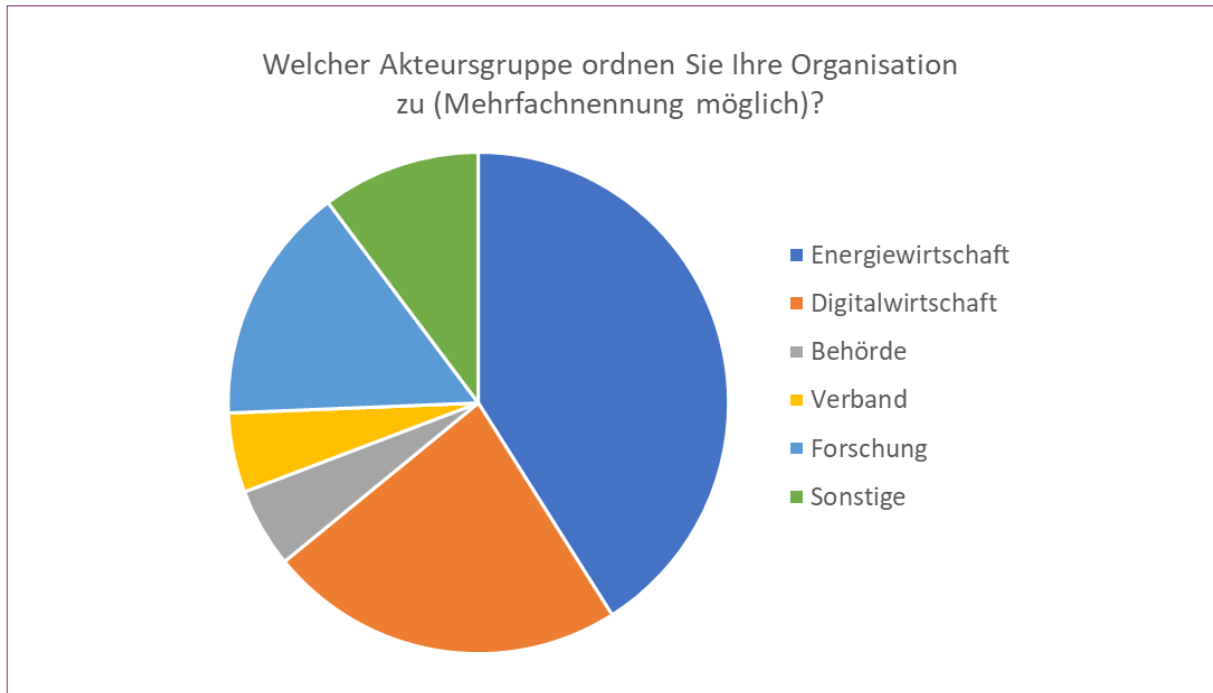


Abbildung 3 Verteilung der Akteursgruppen der 33 Befragten (Mehrfachnennung war möglich)

Die zweite Abfrage zu der Position der Befragten ergab: Mit etwa 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.

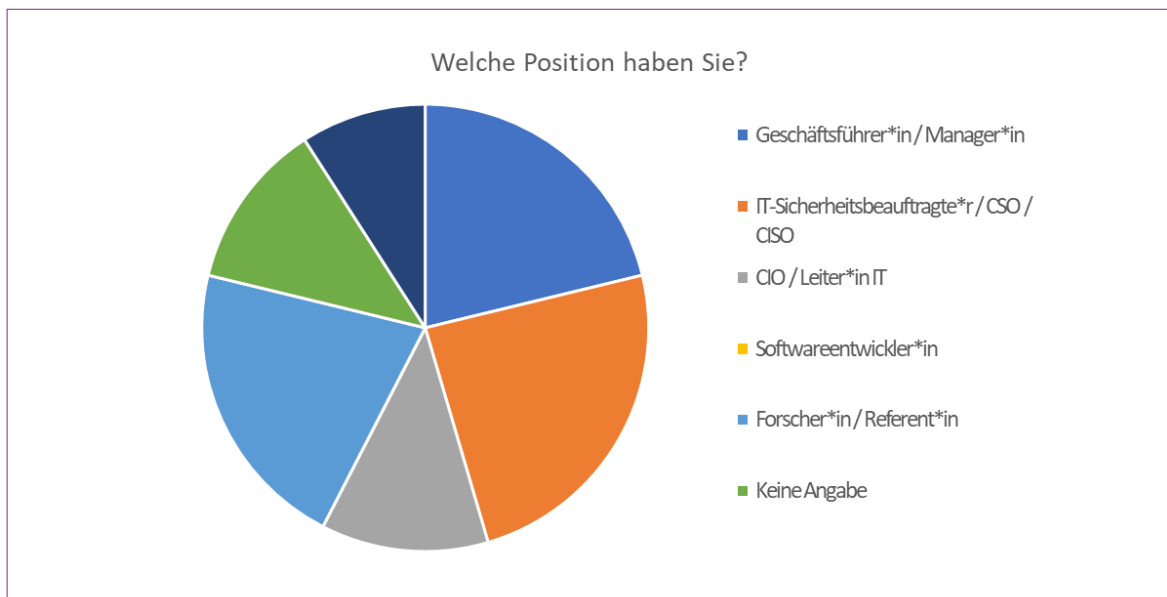


Abbildung 4 Verteilung der Jobpositionen der 33 Befragten (Mehrfachnennung war möglich)

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 Befragten 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 Teilnehmenden haben wir darauf Wert gelegt, dass die Energie- und die Digitalwirtschaft, Behörden und Verbände jeweils gut vertreten sind. Den Teilnehmenden 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 Beteiligten zur weiteren Behandlung in der Branchenplattform empfehlen. Auf Basis dieser Ergebnisse und weiterer Recherchen haben wir die vorliegende Themenroadmap erstellt.

# Abbildungsverzeichnis

Abbildung 1	Skizzierter Prozess der Themenroadmap .....	37
Abbildung 2	Ausschnitt aus der Umfrage zur Themenroadmap der Branchenplattform Cybersicherheit in der Stromwirtschaft (Screenshot).....	39
Abbildung 3	Verteilung der Akteursgruppen der 33 Befragten (Mehrfachnennung war möglich) .....	40

# Literaturverzeichnis

acatech/Leopoldina/Akademienunion (Hrsg.)(2021): Resilienz digitalisierter Energiesysteme. Wie können Blackout-Risiken begrenzt werden? (Schriftenreihe zur wissenschaftsbasierten Politikberatung). Verfügbar unter: <https://www.acatech.de/publikation/rde/>.

Achaal, B., Adda, M., Berger, M. et al. Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges. *Cybersecurity* 7, 10 (2024). <https://doi.org/10.1186/s42400-023-00200-w>.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2023): Die Lage der IT-Sicherheit in Deutschland 2024. Bonn. Verfügbar unter: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?\\_\\_blob=publicationFile&v=5](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5) (abgerufen am: 13. Juni 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](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).

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](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>.

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in Power Grids: Challenges and Opportunities. *Sensors*, 21(18), 6225. <https://doi.org/10.3390/s21186225>

Langerová, E. (2025): Analysing 20 years of China´s power grid hacking research. CTU UCEEB

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.

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](https://www.stiftung-nv.de/sites/default/files/cybersecurity_policy_exercises_in_practice.pdf) (abgerufen am: 4. Februar 2025).

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](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., Müller-Kirchenbauer, J., Kochems, J., Hermann, L., Grosse, B., Nacken, L., Küster, M., Pacem, J., Naumann, D., Kost, C., Kohrs, R., Fahl, U., Schäfer-Stradowsky, S., Timmermann, D., und Albert, D. (2018): Sektorkopplung: Definition, Chancen und Herausforderungen (No. S01/2018). Karlsruhe: Fraunhofer ISI.

