

Sieben Handlungsfelder für mehr Cybersicherheit in der Stromwirtschaft

Eine Themenroadmap als Grundlage einer dialogorientierten Branchenplattform

Linda Schwarz¹, Nikolas Becker¹, Marius Dechand², Hannes Federrath³, Tom Petersen³, Jasmin Wagner², Friederike Wenderoth²

Abstract: Über einen partizipativen Prozess haben wir sieben relevante Handlungsfelder für mehr Cybersicherheit in der Stromwirtschaft identifiziert. Ausgangspunkt ist die vom BMWK initiierte „Branchenplattform Cybersicherheit für die Stromwirtschaft“, für die eine Themenroadmap erarbeitet wurde. Die Handlungsfelder werden den Clustern Governance & Standards, Kapazitätsaufbau & Sensibilisierung, Gesetze sowie Zusammenarbeit zugeordnet.

Keywords: Sicherheit Kritischer Infrastrukturen, Stromsektor, Energiewende, Delphi-Methode

1 Einleitung

Mit der Energiewende wird das Stromnetz flexibler, aber auch komplexer. Denn anstelle weniger Kraftwerke sind nun Tausende Solarzellen und Windanlagen an das Stromnetz angeschlossen und digital miteinander vernetzt. Das macht unsere Versorgung stabiler und flexibler, bietet aber auch neue Schwachstellen: Cyberangriffe⁴ auf vereinzelte Anlagen oder Systeme könnten über die breite Vernetzung vielen weiteren Akteuren Schaden zufügen und zu großflächigen Stromausfällen führen (Hecht, Langer und Smith, 2014).

Um Cyberangriffe zu verhindern und deren Folgen abzumildern, müssen Akteure aus Politik, Strom- und Digitalwirtschaft zusammenarbeiten. Die vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderte und von der Deutschen Energie-Agentur (dena) umgesetzte Branchenplattform Cybersicherheit in der Stromwirtschaft⁵ ist 2023 gestartet, um eine solche Zusammenarbeit voranzubringen. Im Folgenden stellen wir sieben Handlungsfelder vor, die im Rahmen der Plattform, angelehnt an die Delphi-Methode, durch Befragung und einen Fokusgruppen-Workshop identifiziert und nach den Clustern des ENISA-Frameworks zur Bewertung nationaler IT-Sicherheitsfähigkeiten⁶ strukturiert wurden.

¹ Gesellschaft für Informatik e.V., Anna-Louisa-Karsch-Str. 2, 10178 Berlin, linda.schwarz@gi.de

² Deutsche Energie-Agentur GmbH (dena), Chausseestrasse 128 a, 10115 Berlin

³ Universität Hamburg, Vogt-Kölln-Straße 30, 22527 Hamburg

⁴ Das Kunstwort „Cyber“ wird im Sinne von „die Informationstechnik bzw. IT-Systeme betreffend“ verwendet.

⁵ <https://future-energy-lab.de/projects/branchenplattform-cybersicherheit/> (zuletzt besucht am 02.11.2023)

⁶ <https://www.enisa.europa.eu/publications/report-files/ncaf-translations/national-capabilities-assessment-framework-de.pdf> (zuletzt besucht am 23.10.2023)

2 Sieben identifizierte Handlungsfelder

Eine Wissensbasis zur Klassifizierung von Bedrohungen und Angriffen schaffen: Es haben sich verschiedene Ansätze etabliert, Cyberbedrohungen zu klassifizieren, etwa das Cyber Kill Chain oder MITRE ATT&CK Framework. Es gibt außerdem zahlreiche weitere Ansätze (z. B. [KiKK19, Pols23]). Stromsektorspezifische Ansätze, um IT-Sicherheitsmaßnahmen und -lösungen zu kategorisieren, sind rar und wenig verbreitet (siehe z. B. [HaSH21, PeSF23, SuHL18, VHKW20]). Viele Akteure der Stromwirtschaft halten es jedoch für sinnvoll, eine zielgruppenspezifische Wissensbasis aufzubauen, um etwa auf spezifische Herausforderungen wie der fortschreitenden Vernetzung zu reagieren. Diese müsste anwendungsnah sein und könnte die Grundlage für eine Meldung von Vorfällen sowie eines gewinnbringenden Austauschs bilden.

Herausforderungen vernetzter OT-Systeme angehen: Bei operativen Technologien (OT) handelt es sich um ursprünglich abgekapselte Systeme. Die Digitalisierung im Energiesektor verbindet nun zunehmend IT- mit OT-Komponenten und macht letztere vulnerabler. Die daraus entstehenden Herausforderungen sind v. a. der im langen Lebensdauer von OT-Systemen (oft über 30–50 Jahre, vgl. [PeSF23]) geschuldet: Heute geeignete Sicherheitsmaßnahmen müssen veraltete, nicht leicht zu ersetzende, verwundbare und teilweise nicht mehr updatebare Systeme schützen. Wenn die Sicherheit von OT-Systemen aufgrund veralteter Software nicht mehr gewährleistet werden kann, müssten diese ausgetauscht werden. Dies verursacht enorme Kosten. Auch die Sicherung alter OT-Systeme mit aktueller Technik ist nicht wirtschaftlich. Da OT-Systeme zudem meist mit jeweils eigenen, sehr verschiedenen proprietären Systemen laufen, sind Standard-Sicherheitslösungen für sie nicht brauchbar.

Test- und Weiterbildungsmöglichkeiten ausbauen: Sicherheitsübungen zur Reaktion auf Cyberangriffe finden bei vielen deutschen Stromnetzbetreibern nicht oder nur unregelmäßig statt [WaCh22]. Auch Testlabore existieren kaum, etwa um den Zwist zwischen stabilen, meist aber alten Systemen auf der einen und innovativen, meist aber noch nicht lange getesteten (und daher unsicheren) Systemen auf der anderen Seite anzugehen. Um für den Ernstfall eines schwerwiegenden Cyberangriffs gerüstet zu sein und auf eine dafür elementare Zusammenarbeit und Vernetzung zurückgreifen zu können, müssen stromwirtschaftsspezifische Weiterbildungs- und Testformate weiterentwickelt und durchgeführt werden.

Führungskräfte sensibilisieren: Da der Stromsektor eine kritische Infrastruktur ist, müssen viele Unternehmen zwar Anforderungen erfüllen, z. B. nach BSI-Gesetz umgesetzte Sicherheitsstrategien nachweisen. Um tagtäglich eine hohe Cybersicherheit zu gewährleisten, sind jedoch noch größere und permanente Anstrengungen erforderlich. Ein Ansatz, um diese Herausforderung zu begegnen, ist es, die Vorteile von Cybersicherheit für Unternehmen herauszustellen. So können Investitionen in Sicherheit Unternehmensbeziehungen stärken, Investitionen in die Digitalisierung und Vernetzung erleichtern und zu höheren Umsätzen führen [Tren23].

Transparenz in der Gesetzgebung erhöhen: Derzeit existieren mehr als 80 Akteure, die Gesetze und Handlungsempfehlungen zum Betrieb Kritischer Infrastrukturen erarbeiten, Informationen bereitstellen oder einen Erfahrungsaustausch zu Cybersicherheit anregen [HeDu23]. Den Betroffenen sind Zuständigkeiten unklar und Regelungen werden als realitätsfern kritisiert [Kipk23]. Es braucht daher mehr Transparenz, um die Akzeptanz von Vorschriften zu gewährleisten.

Die Harmonisierung von Zertifizierungen vorantreiben: Gesetzliche Anforderungen müssen nicht nur umgesetzt, sondern auch nachgewiesen werden. Es existieren jedoch keine einheitlichen Nachweisverfahren⁷. Die daraus entstehende Komplexität verwirrt und es stellt sich bei einigen Nachweisen die Frage nach deren Notwendigkeit. Nationale und internationale Zertifizierungsprozesse sollten vereinheitlichen und harmonisiert werden.

Gemeinsam aus Cyberattacken lernen: Nur wenige Unternehmen, äußern sich Furcht vor einem Reputationsverlust öffentlich zu erfolgreichen Angriffen⁸. Andererseits halten viele Unternehmen es für richtig, transparent mit Cyberangriffen umzugehen.⁹ Auch Expert*innen empfehlen immer wieder Transparenz statt Geheimhaltung, da aus Erfahrungsberichten gelernt werden kann. Es braucht daher einen Rahmen, in dem sich verschiedene Stakeholder vertrauensvoll und (noch) nicht öffentlich zu ihren Cybersicherheitsstrategien und Erfahrungen mit Angriffen austauschen können.

3 Fazit

Die sieben identifizierten Handlungsfelder decken sowohl regulatorische, organisatorische als auch technische Probleme auf, die Stakeholder aus der Stromwirtschaft beschäftigen. Auffällig ist der Fokus auf aktuelle Probleme. Herausforderungen wie ein zu erwartender Fachkräftemangel oder Veränderungen durch neue Technologien wurden im Prozess zwar angesprochen, jedoch nicht als drängendste Probleme identifiziert. Dies unterstreicht einmal mehr den hohen Handlungsbedarf, die aufgeführten Herausforderungen gemeinsam anzugehen.

Literatur

- [HaSH21] HAUG, GERALD H.; SPATH, DIETER; HATT, HANNS: *Resilienz digitalisierter Energiesysteme Wie können Blackout-Risiken begrenzt werden?* Halle (Saale), München, Mainz: Deutsche Akademie der Naturforscher Leopoldina e. V. - Nationale Akademie der Wissenschaften acatech - Deutsche Akademie der Technikwissenschaften e. V. Union der deutschen Akademien der Wissenschaften e. V., 2021

⁷ <https://www.openkritis.de/massnahmen/kritis-isms-standards.html> (zuletzt besucht am 06.11.2023)

⁸ <https://background.tagesspiegel.de/cybersecurity/schweigen-ist-gold> (zuletzt besucht am 23.10.2023)

⁹ <https://www.pwc.ch/en/insights/cybersecurity/global-digital-trust-2023.html> (zuletzt besucht am 23.10.2023)

- [HeDu23] HERPIG, SVEN; DUTKE, FREDERIC: *Deutschlands staatliche Cybersicherheitsarchitektur* (11. Auflage). Berlin : Stiftung neue Verantwortung e.V., 2023
- [HeLS14] HECHT, THOMAS; LANGER, LUCIE; SMITH, PAUL: *Cybersecurity Risk Assessment in Smart Grids* (2014)
- [KiKK19] KIM, HYEON; KWON, HYUKJUN; KIM, KYUNG KYU: Modified cyber kill chain model for multimedia service environments. In: *Multimedia Tools and Applications* Bd. 78 (2019), Nr. 3, S. 3153–3170
- [Kipk23] KIPKER, DENNIS-KENJI: *Schriftliche Stellungnahme „Cybersicherheit – Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland“* (Nr. 27. Sitzung). Berlin: Digitalausschuss des Deutschen Bundestags, 2023
- [PeSF23] PETERSEN, TOM; STOCK, JOSHUA; FEDERRATH, HANNES: *Bedrohungsszenarien für Energieinfrastrukturen*: Universität Hamburg, Norddeutsches Reallabor, 2023
- [Pols23] POLS, PAUL: *The Unified Kill Chain. Raising Resilience against Advanced Cyber Attacks*, 2023
- [SuHL18] SUN, CHIH-CHE; HAHN, ADAM; LIU, CHEN-CHING: Cyber security of a power grid: State-of-the-art. In: *International Journal of Electrical Power & Energy Systems* Bd. 99 (2018), S. 45–56
- [Tren23] TREND MICRO: *IT-Security als Wegbereiter*: Trend Micro Deutschland GmbH, 2023
- [VHKW20] VAN DER VELDE, DENNIS; HENZE, MARTIN ; KATHMANN, PHILIPP ; WASSERMANN, ERIK ; ANDRES, MICHAEL ; BRACHT, DETERT ; ERNST, RAPHAEL ; HALLAK, GEORGE ; U. A.: 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, 2020 — ISBN 978-1-72812-956-3, S. 17–22
- [WaCh22] WAGNER, JASMIN; CHADENAS, OLIVER: *Netzbetreiber-Umfrage Cybersicherheit. Zum Stand der Cybersicherheit im deutschen Stromnetz*: Deutsche Energie-Agentur (dena), 2022