Digitalisierung und Energiesicherheit

Wie Cybersicherheit in der Energieversorgung gelingen kann

Cyberangriffe auf die Energieversorgung können verheerende Auswirkungen haben. Doch trotz des bekannten Bedrohungsrisikos offenbart gerade der Energiesektor großen Nachholbedarf. Dabei stehen Technologien und Maßnahmen prinzipiell zur Verfügung. Ihre Einführung sollte nicht nur als Gemeinschaftsaufgabe, sondern vor allem als Chance begriffen werden.

Von Martin Serror und Peter Martini

Die hybride Kriegsführung Russlands in der Ukraine hat auf schmerzliche Weise verdeutlicht, dass die zuverlässige Energieversorgung eines Landes unter anderem maßgeblich von der Cybersicherheit der darunterliegenden Informations- und Kommunikationstechnik (IKT) abhängt. Obwohl die dafür notwendigen Maßnahmen und Technologien prinzipiell bereits seit Jahrzehnten zur Verfügung stehen und kontinuierlich weiterentwickelt werden, scheint die Energieversorgung besonders von fehlender Cybersicherheit betroffen zu sein und einen großen Nachholbedarf bei der entsprechenden Absicherung zu haben. Das liegt zum einen daran, dass Cyberangriffe verheerende Auswirkungen auf die Energieversorgung haben können und dadurch eine erhebliche Bedrohung darstellen. Zum anderen bergen Energienetze besondere Herausforderungen und technische Hürden, die fortlaufend interdisziplinär adressiert werden müssen, damit eine sichere Energieversorgung gelingen kann.

Was bedeutet Cybersicherheit?

Dabei spielen Cyberangriffe auf Energienetze bereits eine Rolle, seitdem der Einzug der Digitalisierung auch in der Energieversorgung begonnen hat. Ein prominentes Beispiel ist das Stuxnet-Schadprogramm, welches seit 2010 gezielt SCADA-Anlagen des Herstellers Siemens befallen hat (Langner 2011). Eine Besonderheit war hierbei, dass Stuxnet sich nicht über das Internet verbreitet hat, sondern seinen Weg alleine über lokale Netzwerke und USB-Speichermedien gefunden hat – und zwar unter anderem auf iranische Atomanlagen. Ein weiteres bekanntes Beispiel ist der Cyberangriff auf das ukrainische Stromnetz in 2015, der zu massiven Stromausfällen geführt hat (Whitehead et al. 2017). Hier spielte das Internet sowohl für die Erlangung eines unberechtigten Zugangs als auch für die Durchführung des Angriffs eine wichtige Rolle. Zukünftig wird die Vernetzung innerhalb des Stromnetzes weiter fortschreiten, beispielsweise durch die Anbindung der vielen verteilten Erneuerbare-Energien-Anlagen an IKT-Netze, was insgesamt zu einer wachsenden Angriffsfläche und somit einem höheren Bedarf an Cybersicherheit führt. Da eine Vielzahl von dezentral eingesetzten Geräten auf identischen Standard-IT-Komponenten aufbaut, sind diese für die gleichen Schwachstellen anfällig, weshalb für die Durchführung eines großflächigen, verteilten Cyberangriffs oftmals eine einzige Sicherheitslücke ausreicht (Pearson et al. 2011).

Um Cybersicherheit zu stärken, muss zunächst definiert werden, was überhaupt schützenswert ist. Daraus ergeben sich Schutzziele, die es systematisch durch technische und organisatorische Maßnahmen zu erreichen gilt. Im Unterschied zu anderen Bereichen steht in der Industrie und insbesondere bei der Energieversorgung die Betriebssicherheit an erster Stelle, also der Schutz von Leib und Leben. Erst dann folgen (mit absteigender Priorität) die gängigeren IT-Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit. Für die Erreichung dieser Schutzziele müssen entsprechende Sicherheitsmaßnahmen implementiert werden. Umgekehrt bedeutet dies aber auch, dass jede (neue) Sicherheitsmaßnahme vor ihrem Einsatz mit den Schutzzielen in Einklang gebracht werden muss. Dieser Umstand in Kombination mit den spezifischen Eigenschaften von Energienetzen hat erheblichen Einfluss auf die Umsetzung konkreter Maßnahmen.

Physische Sicherheit herstellen

Eine wesentliche Herausforderung liegt bereits in der Größe von Energienetzen, die eine physische Überwachung aller dazugehörigen Leitungen, Anlagen und Liegenschaften nahezu unmöglich macht. In der Konsequenz werden dadurch Sabotageaktionen ermöglicht, sowohl von Innentätern, etwa frustrierten Mitarbeitenden, als auch von externen Akteuren (Krause et al. 2021). Solche Aktionen haben häufig cyberphysische Auswirkungen auf das Gesamtsystem, die zum Zeitpunkt der Durchführung unter Umständen noch nicht abzusehen waren. Gerade in der Energieversorgung wird solchen, gezielten oder zufälligen, Ausfällen mit Redundanz begegnet, was unter anderem an der grundsätzlichen Umsetzung des (n-1)-Kriteriums liegt. Allerdings hat beispielsweise die Sabotage der Kommunikationsleitungen der Deutschen Bahn im Oktober 2022 gezeigt, dass versierte Tätergruppen sich durch einfache Redundanzen nicht aufhalten lassen. Deshalb müssen die An-

*Ökologisches*Wirtschaften 2.2023 (38) | DOI 10.14512/OEW380226

griffserkennungssysteme verbessert werden, etwa durch die Einbeziehung von Prozesswissen (Wolsing et al. 2022) oder durch die Kopplung von automatisierter Liegenschaftsüberwachung mit Intrusion-Detection-Systemen (Serror et al. 2022).

Veraltete Systeme und Hardware

Weiterhin zeichnen sich industrielle Netze insgesamt und somit auch Stromnetze durch lange Produktzyklen und teilweise auch veraltete Hardware aus (Serror et al. 2020). Eine Herausforderung bei diesen älteren Systemen ist, dass dort moderne Cybersicherheitsmechanismen fehlen und sie deshalb ein Sicherheitsrisiko für das Gesamtsystem darstellen. Auch eine Modernisierung der Systeme oder zumindest die Nachrüstung entsprechender Sicherheitsmechanismen ist häufig nicht ohne Weiteres möglich, da vorrangig die unterbrechungsfreie Stromversorgung garantiert werden muss und zeitkritische Prozesse somit nicht einfach unterbrochen werden können. Es müssen daher andere Wege gefunden werden, diese veralteten Systeme abzusichern, etwa durch die Anpassung zeitintensiver kryptischer Verfahren, deren Berechnung in die Leerlaufphasen der beteiligten Systeme verlagert wird (Hiller et al. 2018).

Dennoch wird kein Weg daran vorbeiführen, in vielen Bereichen der Energieversorgung die Cybersicherheit grundlegend anzugehen. Hierzu bietet sich ein Security-by-Design-Ansatz an, bei dem die Cybersicherheit bereits in der Entwurfsphase neuer Anlagen und Systeme mitgedacht und somit von Anfang an berücksichtigt wird. Cybersicherheit wird somit nicht mehr nur als optionaler Mehrwert verstanden, sondern als eine zwingend notwendige Anforderung an neue Systeme. Die gute Nachricht ist, dass viele der benötigten Lösungen bereits in Ansätzen existieren und teilweise schon in anderen Bereichen eingesetzt werden. Sie warten also nur noch auf ihre Anpassung und Umsetzung in der Energieversorgung. Allerdings bleibt die Herausforderung, dass neue Sicherheitslösungen vorab getestet werden müssen, was im laufenden Betrieb von Produktivsystemen nicht einfach möglich ist. Es braucht daher sichere Testumgebungen, die die Erprobung neuer Sicherheitsverfahren und gleichzeitig eine Auswirkungsanalyse auf das Gesamtsystem ermöglichen. In diesem Kontext bietet beispielsweise das interdisziplinäre Fraunhofer-Zentrum Digitale Energie flexible Testaufbauten, die sich zu individuellen und nahezu realen Stromnetzen konfigurieren lassen. Zusätzlich können sie durch verschiedene detailgetreue Simulationen erweitert werden, um die nachgebildeten Stromnetze bei Bedarf auch in der Größe zu skalieren und somit neue Fragestellungen zu betrachten.

Cybersicherheit als Chance begreifen

Letztlich können diese Herausforderungen nur interdisziplinär und durch einen gemeinsamen Kraftakt angegangen werden. Hier ist einerseits die Expertise aus Bereichen der Informatik, Elektrotechnik und den Wirtschaftswissenschaften gefragt, andererseits müssen auf der Makroebene Forschung, Industrie und Gesellschaft zusammenarbeiten. Sicherlich spielen bei den Betreibern von Energienetzen auch finanzielle Motive eine Rolle, wenn es darum geht, in die Sicherheit über die gesetzlichen Regelungen hinaus zu investieren. Schließlich lässt sich mit der Erhöhung von Cybersicherheit per se kein Geld verdienen, allenfalls lassen sich die Risiken für Schäden minimieren. Vielleicht kann dieser Entwicklung entgegengewirkt werden, wenn Cybersicherheit nicht mehr nur als regulatorische Auflage begriffen wird, sondern als Chance. Denn eine moderne Sicherheitsarchitektur bei der Energieversorgung legt das Fundament für eine starke und tiefgreifende Vernetzung von Erzeugung, Übertragung und Verbrauch, ganz im Sinne der dringend benötigten Energiewende.

Literatur

Hiller, J./Henze, M./Serror, M./Wagner, E./Richter, J. N./Wehrle, K. (2018): Secure low latency communication for constrained industrial IoT scenarios. In: IEEE 43rd Conference on Local Computer Networks (LCN): 614–622. DOI: 10.1109/LCN.2018.8638027

Krause, T./Ernst, R./Klaer, B./Hacker, I./Henze, M. (2021): Cybersecurity in power grids: Challenges and opportunities. In: Sensors 21/18: 6225. DOI: 10.3390/s21186225

Langner, R. (2011): Stuxnet: Dissecting a Cyberwarfare Weapon. In: IEEE Security & Privacy 9/3: 49–51. DOI: 10.1109/MSP.2011.67

Pearson, I. L. G. (2011): Smart grid cyber security for Europe. In: Energy Policy 39/9: 5211–5218. DOI: 10.1016/j.enpol.2011.05.043

Serror, M./Hack, S./Henze, M./Schuba, M./Wehrle, K. (2020): Challenges and Opportunities in Securing the Industrial Internet of Things. In: IEEE Transactions on Industrial Informatics 17/5: 2985–2996. DOI: 10.1109/TII.2020.3023507

Serror, M./Bader, L./Henze, M./Schwarze, A./Nürnberger, K. (2022): Poster: INSIDE-Enhancing Network Intrusion Detection in Power Grids with Automated Facility Monitoring. In: Conference on Computer and Communications Security: 3463–3465. DOI: 10.1145/3548606.3563500

Whitehead, D. E./Owens, K./Gammel, D./Smith, J. (2017): Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies. In: Conference for Protective Relay Engineers (CPRE). DOI: 10.1109/CPRE.2017.8090056

Wolsing, K./Thiemt, L./Sloun, C. V./Wagner, E./Wehrle, K./Henze, M. (2022): Can Industrial Intrusion Detection Be SIMPLE? In: European Symposium on Research in Computer Security: 574–594. DOI: 10.1007/978-3-031-17143-7_28

AUTOREN + KONTAKT

Dr. Martin Serror ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE und forscht im Bereich der Cybersicherheit für die Energieversorgung.

Fraunhofer FKIE, Abteilung Cyber Analysis & Defense, Zanderstraße 5, 53177 Bonn-Bad Godesberg, Tel.: +49 228 50212-500, E-Mail: martin.serror@fkie.fraunhofer.de.

Dr. Peter Martini ist Leiter des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE sowie Professor des Instituts für Informatik IV an der Rheinischen Friedrich-Wilhelms-Universität Bonn.

Fraunhofer FKIE, Institutsleitung, Fraunhoferstr. 20, 53343 Wachtberg, Tel.: +49 228 9435-217, E-Mail: peter.martini@fkie.fraunhofer.de.