Nr. 5 | Januar 2019

VISE

Virtuelles Institut Smart Energy

Policy Brief

Januar 2019

IT-Sicherheit in der Energiewirtschaft

Autoren

BERGISCHE UNIVERSITÄT WUPPERTAL

SIKoM+ Institut für Systemforschung der Informations-, Kommunikations- und Medientechnologie

Lena Weigelin
Jacqueline Stork

Kontakt

VISE Virtuelles Institut Smart Energy

E-Mail: info@smart-energy.nrw

Website: www.smart-energy.nrw

In Kooperation mit

CPS.HUB /NRW Competence Center for Cyber Physical Systems

Gefördert durch

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

EFRE.NRW
Investitionen in Wachstum
und Beschäftigung

IT-Sicherheit: Zentrale Herausforderung für die Digitalisierung der Energieversorgung

IT-Sicherheit in der Energiewirtschaft

Die Energieversorgung zählt zu den kritischen Infrastrukturen (KRITIS), da sowohl wirtschaftliche als auch gesellschaftliche Sektoren von ihr abhängig sind. Störungen der Energieversorgung können „katastrophale Auswirkungen mit unvorhersehbaren Kaskadeneffekten“[1] mit sich bringen. Die Bedrohungslage für die Energieversorgung hat insbesondere aufgrund der auch in dieser Branche fortschreitenden Digitalisierung zugenommen, hinzu kommt eine bislang unzureichende Fokussierung auf die IT-Sicherheit.[2]

Digitalisierung in der Energiewirtschaft

Mit Hilfe digitaler Technologien im Bereich Energiewirtschaft können u. a. Effizienzsteigerungen bei der Energieversorgung erzielt, Abrechnungsmodelle für den Verbraucher transparenter gestaltet und zahlreiche weitere Anwendungsszenarien genutzt werden. In der Praxis bedeutet das heute, dass z. B. intelligente Messsysteme etabliert und Verbraucherdaten digital an Energieversorger übertragen werden. Kraftwerke werden vernetzt, Anlagen gebündelt und durch ein zentrales Leitsystem wie ein einziges Kraftwerk gesteuert. Mit Hilfe cloudbasierter Plattformen können integrierte Darstellungen von Kundenbeziehungen angeboten werden. Außerdem werden zur Verbesserung der Versorgungssicherheit Netzstationen digitalisiert, die Struktur der Netze und das Lastmanagement durch intelligente Netze, sogenannte Smart Grids, verbessert.[3]

[1] Bartsch, Michael / Frey, Stephanie (2017): Digitalisierung des Bösen: Energiewirtschaft als Cyberopfer, in: Doleski, Oliver D. (Hrsg.): Herausforderungen Utility 4.0. Wie sich die Energiewirtschaft im Zeitalter der Digitalisierung verändert.
[2] Bartsch, Michael / Frey, Stephanie (2017): Digitalisierung des Bösen: Energiewirtschaft als Cyberopfer, in: Doleski, Oliver D. (Hrsg.): Herausforderungen Utility 4.0. Wie sich die Energiewirtschaft im Zeitalter der Digitalisierung verändert.
[3] TÜV Nord Group (2018): Cyber Security im Energiesektor in den Fokus nehmen. Online abrufbar unter: https://www.tuev-nord-group.com/de/newsroom/aktuelle-pressemeldungen/details/article/cyber-security-im-energiesektor-in-den-fokus-nehmen/, Zugriffsdatum: 01.08.2018.

Die Herausforderung, die mit dem Zusammenwachsen der Prozess- und Leittechnik mit Systemen der Informations- und Kommunikationstechnologien einhergeht ist, dass die potenzielle Bedrohungslage durch Cyber-Angriffe steigt. Die Tatsache, dass Hardware-Systeme beispielsweise in Wasser- oder Kernkraftwerken eine sehr hohe Lebensdauer haben und u. a. aus Kostengründen nicht einfach gegen modernere, sicherere Komponenten ausgetauscht werden können verbessert die Voraussetzungen nicht. Die Vielzahl von Akteuren – zentrale und dezentrale Energieproduzenten, Versorger, Netzbetreiber, Messstellenbetreiber, Messdienstleister, Kunden und Verbraucher – in einem Netz bedeutet zahlreiche Angriffsstellen für Cyberangriffe.[4] Gleichzeitig minimiert aber eben dieses komplexe, aber verteilte System die Gefahr eines großflächigen Blackouts bei einem erfolgreichen Cyber-Angriff.

[4] Spiecker, Indra (2017): Smart Home, smart Grid, Smart Meter – digitale Konzepte und das Recht an Daten, in: Doleski, Oliver D. (Hrsg.): Herausforderungen Utility 4.0. Wie sich die Energiewirtschaft im Zeitalter der Digitalisierung verändert.

1 Gefahrenpotenziale

Im Wesentlichen gibt es zwei Angriffsszenarien, die in unterschiedlichen Zusammenhängen sowie auf unterschiedliche Akteure denkbar sind, egal ob Angriffe auf Energieversorger, Smart Grids, Smart Meter Gateways oder ähnliches:

1. Abfangen und Verfälschen von Daten, Missbrauch von sensiblen Kundendaten (Datenschutz und Privacy Problematiken)
2. Sabotage / Störung des Energienetzes (Probleme im sicheren Netzbetrieb)

Der Stuxnet-Angriff im Jahr 2010 sorgte für globales Aufsehen und gilt als Zeitenwende der IT-Sicherheit von Industrieanlagen. Das Schadprogramm war zum Angriff auf das Simatic S7 System von Siemens konzipiert worden, das in zahlreichen Frequenzumrichtern verbaut ist, die unter anderem die Motoren in Wasserwerken und Atomkraftwerken steuern. Der Angriff betraf u. a. das iranische Atomkraftwerk Buschehr. Zeitweise konnte nicht ausgeschlossen werden, dass Stuxnet das gesamte iranische Atomprogramm unter Kontrolle habe. Deshalb gingen Experten zunächst von einem gezielten Angriff auf den Iran aus.[5] Soweit bekannt, waren deutsche Unternehmen von diesem Angriff nicht betroffen.[6]

Ein weiterer Cyber-Angriff erfolgte am 23. Dezember 2015 auf das ukrainische Stromnetz. Insgesamt drei Stromversorger, die einen relativ hohen Automatisierungsgrad in ihren Verteilnetzen hatten, wurden von Umspannstationen abgekoppelt. Dem vorangegangen war monatelange Arbeit der Angreifer, um von der IT-Umgebung der Verwaltung der Stromversorger bis zur Netzleittechnik vorzudringen. Das Ergebnis

[5] Ralph Langner: Stuxnet und die Folgen. Unter: https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf, Zugriffsdatum: 29.08.2018.
[6] Deutscher Bundestag (2010): Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Kathrin Vogler, Dorothee Menzner, Dr. Barbara Höll, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/3253 – Computerschadprogramm stuxnet. Unter: http://dipbt.bundestag.de/doc/btd/17/033/1703388.pdf, Zugriffsdatum: 25.07.2018.

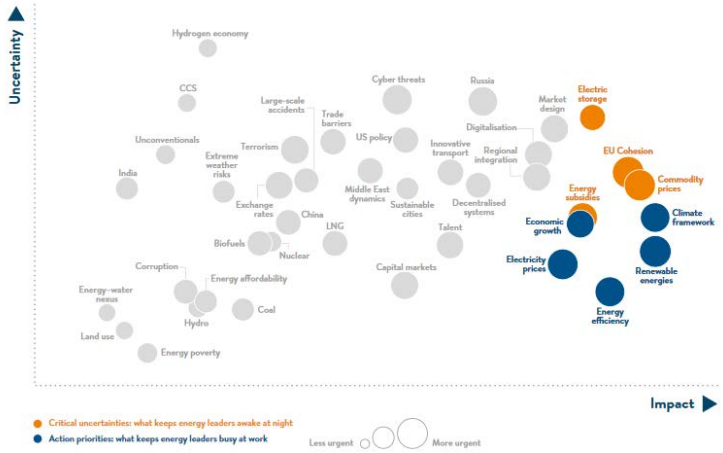
war ein vollständiger Blackout in der West-Ukraine. Rund 225.000 Menschen waren ohne Strom.[7]

[7] Electricity Information Sharing and Analysis Centre (2016): Analysis of the Cyber Attack on the Ukrainian Power Grid. Unter: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Zugriffsdatum: 02.08.2018.

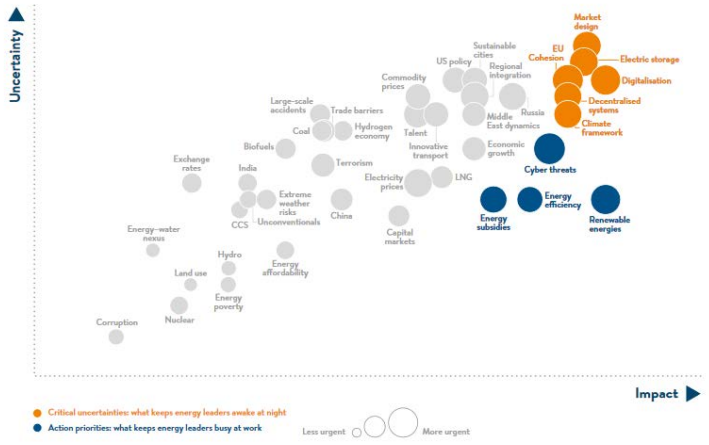
1.1 Einschätzung der Lage

Hohe Erwartungen: Effizienzsteigerungen von bis zu zehn Prozent

Betrachtet man die Einschätzung der Bedrohungslage durch Cyber-Angriffe in unterschiedlichen Ländern, so zeigen sich weltweit große Unterschiede. Der „World Energy Issues Monitor“ zeigt für fast 90 Länder, welche Themen und Fragestellungen die Verantwortlichen in Unternehmen, Ministerien und Experten aus dem Energieumfeld beschäftigen. „Cyber Threats“ werden sehr unterschiedlich wahrgenommen. Das zeigt sich u. a. im Vergleich der Wahrnehmung in der EU insgesamt mit der nationalen Wahrnehmung in Deutschland:



Europäische Union



Deutschland

Abbildung 1 und 2: Wahrnehmung der Cyber-Bedrohungslage von Energie-Unternehmen Eigene Darstellung nach: World Energy Council, "Issue Monitor 2017"

Der Durchschnitt der europaweit Befragten schätzt Cyber-Angriffe als relativ harmlose Gefahr ein. Sie gehören zwar zu den Themen, die großen Einfluss auf den Energiesektor haben, deren Auswirkungen aber

unklar sind. Ein Handlungsdruck wird von den Akteuren der Energiewirtschaft durchaus gesehen, Cyber-Angriffe sind eines der Themen, die intensiv diskutiert und analysiert werden.

Betrachtet man ausschließlich die Antworten der Befragten aus Deutschland zeigt sich ein anderes Bild: Sie betrachten Cyber-Angriffe als eines der drängendsten Themen und schätzen die Auswirkungen auf den Energiesektor als sehr hoch ein. Im Gegensatz zum Durchschnitt der europaweit Befragten sehen deutsche Akteure der Energiewirtschaft einen direkten Handlungsdruck.[8]

1.2 Tatsächliche Bedrohungslage: Weltweit

Zahl der Cyberangriffe steigt weltweit

Das US Department of Homeland Security verzeichnete 2015 insgesamt 295 Cyber-Vorfälle im Energiesektor, eine Steigerung von 20 Prozent im Vergleich zum Vorjahr. Damit entfielen insgesamt 16 Prozent aller Cyber-Angriffe auf den Energiesektor.[9]

Für 2016 ermittelte der IBM X-Force Report rund 39 Millionen IT-Sicherheitsverstöße[10] weltweit im Energiedienstleistungssektor, die Anzahl der ICS-Angriffe (Industrial Control Systems) stieg damit in 2016 im Vergleich zum Vorjahr um 110 Prozent. Für das Jahr 2017 kommt der Bericht zu dem Ergebnis, dass der Energie-Sektor zu den fünf häufigsten Angriffszielen von Cyberkriminellen gehört.[11]

Eine internationale Studie des Ponemon Instituts gemeinsam mit Accenture verdeutlicht, dass die Cyber-Kriminalitätskosten im Energiesektor im Vergleich zu anderen Branchen überdurchschnittlich hoch

[8] World Energy Council (2017): Issue Monitor 2017. Unter: https://www.worldenergy.org/wp-content/uploads/2017/04/1.-World-Energy-Issues-Monitor-2017-Full-Report.pdf, Zugriffsdatum: 02.08.2018.

[9] US Department of Homeland Security (2015): NCCIC/ICS-CERT Year in Review National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team. Unter: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf, Zugriffsdatum: 25.07.2018.

[10] Hierunter fallen laut Definition des Reports Aktivität auf einem System oder Netzwerk, die von einem Sicherheitsgerät oder einer Sicherheitsanwendung erkannt wurden.

[11] IBM X-Force Research (2017): At risk: the energy and utilities sector infrastructure. Unter: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03135USEN&, Zugriffsdatum: 01.08.2018.

sind: So lagen die Kosten in 2017 durch Cyberangriffe bei 17,2 Millionen US-Dollar pro Unternehmen.[12]

1.3 Tatsächliche Bedrohungslage: Deutschland

Deutschland: Hohe Dunkelziffer

Mittlerweile geraten auch deutsche Unternehmen der Energiewirtschaftsbranche vermehrt in den Fokus von Cyber-Angriffen. Bereits 2015 simulierte der TÜV Süd in seinem Honeynet-Experiment mit realer Hard- und Software ein kleines Wasserkraftwerk mit industrieüblichen Schutzmaßnahmen in einer deutschen Kleinstadt. Mit dieser nur im Internet existenten Simulation wollte der TÜV Süd herausfinden, welche Zugriffs- und Angriffsaktionen Hacker verwenden würden und wie groß die tatsächliche Bedrohungslage für ein vergleichsweise unwichtiges Wasserwerk in der Realität ist. Das Ergebnis waren 60.000 Angriffe von Servern aus 150 Ländern mit teilweise verschleierten IP-Adressen innerhalb von acht Monaten.[13]

Die Bedrohung ist mittlerweile aber auch im realen Betrieb angekommen: So zählte das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach Einführung des IT-Sicherheitsgesetzes (Juli 2015), der BSI-Kritisverordnung Teil I (Mai 2016) und Teil II (Juni 2017) insgesamt 34 Meldungen für den Bereich der kritischen Infrastrukturen. Davon fallen 18 in den Sektor Informationstechnik und Telekommunikation, elf in den Sektor Energie, drei in den Sektor Wasser und zwei in den Sektor Ernährung.[14] Im Vergleich zu den globalen Zahlen gibt es scheinbar in Deutschland verhältnismäßig wenige Cyber-Vorfälle – das hat auch mit der Definition bzw. der Meldepflicht gegenüber dem BSI zu tun[15], es

[12] Ponemon Institute / Accenture (2017): Costs of Cyber Crime Study. Insights the security investments that make a difference. Unter: https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50, Zugriffsdatum: 25.07.2018.

[13] TÜV Süd (2015): Das Honeynet-Experiment: Hackerangriffe auf virtuelles Wasserkraftwerk belegen Gefahren für Industrie 4.0. Unter: https://www.tuev-sued.de/management-systeme/newsletter/2015/4/das-honeynet-experiment-hacker-angriffe-auf-virtuelles-wasserkraftwerk-belegen-gefahren-fuer-industrie-4.0, Zugriffsdatum: 26.07.2018.

[14] Bundesamt für Sicherheit in der Informationstechnik (2017): Die Lage der IT-Sicherheit in Deutschland. Unter:https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4, Zugriffsdatum: 25.07.2018.

[15] „Betreiber Kritischer Infrastrukturen, die gemäß der BSI-Kritisverordnung unter das BSI-Gesetz fallen, müssen erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Systeme, IT-Komponenten und IT-Prozesse

wird nicht jede Cyber-Attacke auf deutsche Energieversorger vom BSI erfasst. Die Dunkelziffer dürfte wesentlich höher sein. Der Verfassungsschutz stuft die Dunkelziffer nicht erkannter elektronischer Angriffe als weiterhin „hoch“ ein.[16] In einer Deloitte-Studie gehen 27 Prozent der Befragten davon aus, dass Cyber-Angriffe häufig unentdeckt bleiben.[17]

Im Juni 2018 hat das BSI eine Warnung an mehrere hundert Unternehmen aus der Energiebranche herausgegeben, dass deutsche Unternehmen der Energiewirtschaftsbranche Ziel einer großangelegten weltweiten Cyber-Angriffskampagne seien. Ein Jahr zuvor hatte das BSI bereits eine ähnliche Warnung herausgegeben, die u. a. Handlungsempfehlungen zum Schutz von Netzwerken enthielten.[18] Bei diesem Angriff war unter anderem eine Tochter des Energieversorgers EnBW betroffen: Mutmaßlich russische Hacker sollen in das Netz von Netcom BW eingedrungen sein. Das Unternehmen teilte mit, dass der Angriff in einer frühen Phase abgewehrt werden konnte und keine Gefahr eines Stromausfalls bestanden habe.[19]

(IT-Störung), die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen könnten oder bereits geführt haben, ggf. pseudonymisiert über eine gemeinsame übergeordnete Ansprechstelle (GÜAS), dem BSI melden.“ Gewöhnliche IT-Störungen (laut BSI z. B. bekannte, bereits veröffentlichte Sicherheitslücken, Spam, ungezieltes Phishing), die zu einem Ausfall oder einer Beeinträchtigung führen könnten, werden demnach nicht gemeldet, ebenso wenig IT-Störungen, die zu keinem Ausfall oder Beeinträchtigung führen und keine außergewöhnlichen IT-Störungen (laut BSI z. B. neue, bisher nicht veröffentlichte Sicherheitslücken, unbekannte Schadprogramme), die ebenfalls zu keinem Ausfall oder keiner Beeinträchtigung führen.

[16] Bundesamt für Verfassungsschutz (2014): Elektronische Angriffe mit nachrichtendienstlichem Hintergrund. Unter: https://www.verfassungsschutz.de/embed/broschuere-2014-07-elektronische-angriffe-mit-nachrichtendienstlichem-hintergrund.pdf, Zugriffsdatum: 28.08.2018.

[17] Deloitte (2017): Cyber-Security Report 2017 – Teil 2: Cyber-Risiken in Unternehmen. Unter: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf, Zugriffsdatum: 02.08.2018.

[18] Bundesamt für Sicherheit in der Informationstechnik (2018): Cyber-Angriffe auf deutsche Energieversorger. Unter:https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html, Zugriffsdatum: 25.07.2018.

[19] n-tv (2018): Hacker greifen EnBW-Tochter an. Unter: https://www.n-tv.de/wirtschaft/Hacker-greifen-EnBW-Tochter-an-article20436822.html, Zugriffsdatum: 25.07.2018.

1.4 IT-Sicherheitslage bei deutschen Energieversorgern

Deutsche Stadtwerke sind sich der gestiegenen Gefahren durch Cyber-Angriffe durchaus bewusst: 61 Prozent haben deshalb bereits einen IT-Sicherheitsbeauftragten installiert, 15 Prozent verfügen über ein Informationsmanagementsystem, weitere 46 Prozent etablieren ein solches System gerade. Dennoch geben rund 20 bis 30 Prozent der befragten Netzbetreiber an, IT- und Informationssicherheitsanforderungen für ihr Unternehmen als nicht relevant einzustufen, beziehungsweise keine Angaben hierzu zu machen.[20]

[20] Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft (2017): Stadtwerkestudie 2017. Der Verteilnetzbetreiber der Zukunft – Enabler der Energiewende.

2 Forschungsprojekte

NRW ist einer der Hotspots für die IT-Sicherheit in Deutschland. Zurzeit arbeiten rund 700 Wissenschaftler an 20 Forschungseinrichtungen und Universitäten im Bereich IT-Sicherheit.[21] Gleichzeitig ist Nordrhein-Westfalen „Energieland Nummer 1“: In keinem anderen Bundesland wird so viel Energie erzeugt, aber auch verbraucht. In zahlreichen Forschungsprojekten werden Sicherheitstechnologien für den Energiesektor entwickelt und getestet, von denen hier beispielhaft drei skizziert werden.

2.1 SIDATE – Sichere Informationsnetze bei kleinen und mittleren Energieversorgern

Ziel: Im Projekt SIDATE werden Konzepte und Werkzeuge für eine schnelle Einschätzung und Verbesserung des vorhandenen Sicherheitsniveaus besonders für kleine und mittlere Betreiberfirmen entwickelt. Sie sollen helfen, die Selbsteinschätzung von Unternehmen insbesondere hinsichtlich des vorhandenen Sicherheitsniveaus zu erhalten und so helfen, die IT-Sicherheit kleiner und mittlerer Betreiberfirmen selbst zu verbessern.

Projektpartner: Universität Siegen, TÜV Rheinland i-sec GmbH, regio iT GmbH, Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung im VKU und weitere.

https://sidate.org/

2.2 CONNECT – Innovative smart components, modules and appliances for a truly connected, efficient and secure smart grid

Ziel des Projekts CONNECT ist es, Konzepte, Technologien und Komponenten bereit zu stellen, die die Integration erneuerbarer Energien unterstützen und eine intelligente Speicherung und Steuerung des

[21] Prof. Dr. Pohlmann, Norbert / Prof. Dr. Holz, Thorsten / Barchnicki, Sebastian (2016): IT-Sicherheit für
NRW 4.0. Gemeinsam ins digitale Zeitalter. Aber sicher. https://www.it-sicherheit-nrw.de/download/Strategiepapier_It-Sicherheit_NRW_Web.pdf, Zugriffsdatum: 29.08.2018

Energieflussmanagements ermöglichen, um die Nachfrage nach Primärenergie zu senken und eine dezentrale Energieinfrastruktur zu realisieren. Dabei spielt die Entwicklung fortschrittlicher Sicherheitsmaßnahmen für die Smart-Grid-Kommunikation mit erweiterten hardware- und softwarebasierten Funktionen eine wesentliche Rolle.

Projektpartner: An dem Horizon2020-Projekt mit insgesamt 19 Partnern aus fünf Ländern sind die RWTH Aachen und die Devolo AG beteiligt.

http://www.connect-ecsel.eu/

2.3 E²S²E: Energy Efficient and Secure Smart Environment

Ziel: Im Rahmen des Projekts „Energy Efficient and Secure Smart Environment“ wird ein Cluster von exzellenter Forschung und Innovation in intelligenten Umgebungen (Smart Homes, Smart Cities, Smart Transportation) und verwandten Themen (eHealth, demographischer Wandel) aufgebaut. Im Fokus stehen Fragen der IT-Sicherheit, der Energieeffizienz und der Bedienungsfreundlichkeit verwandter Systeme und decken damit zentrale Fragen in der deutschen und europäischen Forschungsförderung ab.

Projektpartner: Universität Bonn, Fraunhofer FKIE, MBS GmbH und weitere.