THEMA

*Cyber*sicherheit

Bedrohung, Verwundbarkeit, Werte und Schaden

Cyberattacken bedrohen eine Infrastruktur, ohne die moderne Gesellschaften kaum funktionieren können. Doch die Gewährleistung von Cybersicherheit kann zu Zielkonflikten führen: Je mehr Gesellschaften auf funktionierende Informations- und Kommunikationstechnologie angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen. Ein TATuP-Thema herausgegeben von Karsten Weber, Markus Christen und Dominik Herrmann.

https://doi.org/10.14512/tatup.29.1.10

Bedrohung, Verwundbarkeit, Werte und Schaden

Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung

Karsten Weber, *Institut für Sozialforschung und Technikfolgenabschätzung, Ostbayerische Technische Hochschule Regensburg, Galgenbergstraße 24, 93053 Regensburg (Karsten.Weber@oth-regensburg.de)* *https://orcid.org/0000-0001-8875-2386*
Markus Christen, *Digital Society Initiative, Universität Zürich (christen@ifi.uzh.ch)*
Dominik Herrmann, *Lehrstuhl Privatsphäre und Sicherheit in Informationssystemen, Fakultät Wirtschaftsinformatik und Angewandte Informatik, Otto-Friedrich-Universität Bamberg (dominik.herrmann@uni-bamberg.de)*

Die monetären Kosten, die jährlich weltweit durch Cyberattacken entstehen, wachsen stetig und bewegen sich in Dimensionen, die mit öffentlichen Haushalten ganzer Staaten verglichen werden können. Cyberattacken treffen Individuen, Unternehmen, öffentliche Einrichtungen, Behörden und Regierungen; sie treffen eine Infrastruktur, ohne die moderne Gesellschaften kaum mehr funktionieren. Doch die Gewährleistung von Cybersicherheit kann zu Zielkonflikten führen. Die Technologien zur Herstellung von Sicherheit und Resilienz dieser Infrastruktur sollten daher Gegenstand der Technikfolgenabschätzung sein.

Threat, vulnerability, values, and damage
Cyberattacks and cybersecurity as a subject of technology assessment

The annual monetary costs incurred worldwide by cyberattacks are growing steadily and are on a scale comparable to the budgets of entire countries. Cyberattacks affect individuals, businesses, public institutions, authorities, and governments; they affect an infrastructure without which modern societies can hardly function. But ensuring cybersecurity can lead to conflicts of interest. Technologies used to ensure the security and resilience of this infrastructure should therefore be a subject of technology assessment.

Keywords: *cybersecurity, cyberattacks, critical infrastructures, resilience*

https://doi.org/10.14512/tatup.29.1.11

Digitalisierung allerorts

Spätestens mit der weltweiten Verbreitung von Social Media und Smartphones, welche die Nutzung von Plattformen sowie des Internets allgemein zu jeder Zeit an jedem Ort ermöglichen, haben Informations- und Kommunikationstechnologien (IKT) fast alle gesellschaftlichen Lebensbereiche und Praktiken weithin sichtbar durchdrungen. Dies betrifft nicht nur alltägliche Lebensvollzüge wie Information, Konsum oder Bankgeschäfte einzelner Personen, auch die globale Verknüpfung wirtschaftlicher Prozesse – von Produktion über Logistik bis hin zum internationalen Finanzwesen – stützt sich heutzutage entscheidend auf IKT ab. Immer mehr, früher informell ablaufende wirtschaftliche und gesellschaftliche Prozesse werden in digitalen Systemen abgebildet und damit steuerbar. Dieser Prozess der Durchdringung wird seit einigen Jahren als Digitalisierung bezeichnet, doch es ist offenkundig, dass die damit benannten Veränderungen lange vor der Entstehung sozialer Medien und der mobilen Internetnutzung begonnen haben: Banken und Versicherungen, Fluggesellschaften und Logistikunternehmen haben bereits in den 1960er- und 1970er-Jahren, also vor mehr als einem halben Jahrhundert, damit begonnen, Geschäftsprozesse zu digitalisieren – nur nannte man dies noch nicht so. Handel, Industrie und Verkehr, aber auch die Gesundheitswirtschaft, die öffentlichen Verwaltungen, das Militär und die Sicherheitsbehörden sowie viele andere Sektoren der Wirtschaft und des öffentlichen Lebens nutzen schon lange IKT zur Verwaltung von Datenbeständen, die für die Funktion der entsprechenden Organisationen essentiell sind.

Vergleichsweise neu ist dagegen die massive Vernetzung all dieser IKT-Systeme. Zwar sind sehr große oder gar globale Computernetzwerke ebenfalls nichts wirklich Neues; man denke an das in den 1950er-Jahren entstehende vernetzte SAGE-Computersystem in den USA zur Steuerung der kontinentalen Flug-

abwehr (Redmond und Smith 2000) oder an die sowjetischen Pendants, die allerdings in westlicher wissenschaftlicher Literatur kaum behandelt werden (Gerovitch 2004). Im zivilen Bereich wären die großen Flugbuchungssysteme wie Sabre und Apollo zu nennen, die bereits in den 1960er- und 1970er-Jahren entstanden (Copeland et al. 1995). Doch diese Systeme nutzten Vernetzungstechnologien, die mit dem, was wir heute als Internet kennen, wenig bis nichts gemeinsam hatten. Ihre Zugänglichkeit war daher sehr eingeschränkt; in Hinblick auf Sicherheitserwägungen war dies vermutlich ein erheblicher Vorteil.

Unser heutiges Bild vernetzter Computer ist durch Ubiquität, allgemeine Zugänglichkeit, Mobilität und nicht zuletzt durch geringe Kosten der Vernetzung geprägt; auch wenn zunehmend der Energiebedarf der digitalen Transformation kritischer diskutiert wird (Jones 2018). Vielleicht aber noch mehr spielt eine Rolle, dass die meisten Menschen das Internet mit dem WWW und sozialen Medien gleichsetzen und deren Entertainmentfunktionen betonen. Damit gerät jedoch in den Hintergrund, dass diese Dienste längst zu einer Infrastruktur geworden sind, von deren korrekter Funktion ein erheblicher Teil der globalen Wertschöpfung abhängig ist.

Unabhängig davon, wie jemand auf vernetzte IKT schaut: Diese Technologie beeinflusst unsere Denkweise, unsere Interaktionen mit anderen Personen sowie mit Organisationen und Institutionen; sie verändert unsere Rollen als Bürgerinnen und Bürger, Arbeitnehmerinnen und Arbeitnehmer oder auch als Verbraucherinnen und Verbraucher. IKT als komplexe und vernetzte Basistechnologie des 21. Jahrhunderts macht unsere Welt zu einem wohlhabenderen, effizienteren und sehr interaktiven Ort – IKT kann die Kommunikation und Interaktion zwischen Menschen über Staats- und Kulturgrenzen hinweg erleichtern oder gar erst ermöglichen. Doch gleichzeitig machen Komplexität und hochgradige Vernetzung IKT anfällig für technisches Versagen sowie für kriminelle, terroristische oder gar kriegerische Attacken, sodass es mit zunehmender Komplexität und Vernetzung immer schwieriger wird, die Funktionsfähigkeit von Industrien oder Versorgungsinfrastrukturen aufrechtzuerhalten. Moderne Gesellschaften, deren Funktionsfähigkeit auf IKT beruht, sind daher – mit Ulrich Beck (1986) gesprochen – „gefährdete Gesellschaften“. Das ist der Ausgangspunkt des TATuP-Themas „Cybersicherheit“.

Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen.

Cyberspace, Cyberkriminalität, Cyberterror: Unsicherheit

Die durch Cyberattacken weltweit verursachten Kosten sind enorm: „Our current estimate is that cybercrime may now cost the world almost $ 600 billion, or 0.8 % of global GDP“ (CSIS 2018, S. 4). Andere Kennzahlen sind ebenso beindruckend wie erschreckend: „One major internet service provider (ISP) reports that it sees 80 billion malicious scans a day, the result of automated efforts by cybercriminals to identify vulnerable targets. Many researchers track the quantity of new malware released, with estimates ranging from 300,000 to a million viruses and other malicious software products created every day“ (CSIS 2018, S. 4). Aus gesellschaftlicher Sicht sind nicht nur die direkten Kosten (z. B. Reparaturkosten, betrugsbedingte Verluste), sondern auch indirekte Kosten (beispielsweise Kosten von Präventivmaßnahmen) und implizite Kosten (u. a. geringere Produktivitätssteigerungen durch geringeres Vertrauen in digitale Transaktionen) auf Verletzungen der Cybersicherheit zurückzuführen (Bauer und van Eeten 2009). Angesichts solcher Zahlen ist es wenig überraschend, wenn das Center for Strategic and International Studies schreibt: „Over the last 20 years, we have seen cybercrime become professionalized and sophisticated. Cybercrime is a business with flourishing markets offering a range of tools and services for the criminally inclined“ (CSIS 2018, S. 12). Wer weiß, wo man suchen muss, findet im Netz all die Werkzeuge, die notwendig sind, um selbst Cyberattacken zu verüben, ohne dass dabei ein besonderes Wissen notwendig wäre; man kauft sich einfach *Cybercrime-as-a-Service*.

Es kann somit kaum verwundern, dass aktuelle Cybersicherheitsdebatten geprägt sind von der Betonung immer größerer und vielfältiger werdender Bedrohungsformen, die von Cyberkriminalität und Cyberspionage bis hin zu Cyberterror und Cyberwar (Dunn Cavelty 2014) reichen. Cybersicherheit ist dadurch auch zu einer Angelegenheit staatlicher Akteure geworden; die Ausgaben für verteidigungsbezogene Aspekte von Cybersicherheit steigen (Brito und Watkins 2011; Boulanin 2013).

Schon dieser kurze Überblick weist auf die Gefahr hin, Diskurse über Cybersicherheit thematisch einzuengen: Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, Sicherheit über alle anderen Werte zu stellen, auf denen unsere Gesellschaften aufbauen. Infolgedessen werden Grenzen, die bisher unsere soziale, institutionelle, rechtliche und moralische Welt konstituiert haben, infrage gestellt, kompromittiert oder relativiert. Traditionelle Differenzierungen und Abgrenzungen getrennter sozialer Bereiche wie Familie und Freundschaft, Arbeit, Politik, Bildung, kommerzielle Aktivität und Produktion, Gesundheitswesen, Forschung usw., die jeweils durch kontextbezogene Normen und Regeln bestimmt sind, werden durch IKT bedroht. Betroffen sind beispielsweise Konzepte wie informierte Einwilligung, persönliche Daten oder Anonymität sowie die ihnen zugrundeliegenden Werte wie Autonomie, Fairness, Privatsphäre und Verantwortung. Diese Werte können durch eine übermäßige Betonung des Werts Sicherheit außer

Kraft gesetzt werden; insbesondere wenn Cyberbedrohungen als grundlegende Bedrohung der gegenwärtigen Lebensweise angesehen werden.

In Hinblick auf Privatsphäre, Datenschutz, Computer- und Cybersicherheit sollte allerdings nicht der Eindruck erweckt werden, dass die Debatte erst kürzlich begonnen hätte. Schon 1967 stellt Alan F. Westin in seinem häufig zitierten Buch *Privacy and Freedom* den Zusammenhang zwischen dem Schutz der Privatsphäre (als Schutz privater Daten) und Freiheit her; wenige Jahre später bringen Lance J. Hoffman (1973) und James Martin (1973) Sicherheit und Privatsphäre bei der Verarbeitung von Daten in Computersystemen zusammen. Sicherlich wäre es lohnenswert, die damaligen Diskurse zu rekonstruieren, um zu sehen, inwieweit daraus Lehren zu ziehen sind – vermutlich nicht in einem technischen Sinne, aber doch in politischer Hinsicht.

Wie viel Absicherung gegen Risiken von Cyberattacken – sei es krimineller, terroristischer oder kriegerischer Art – letztlich erforderlich ist, ist umstritten und muss gesellschaftlich stets neu ausgehandelt werden. Es kann gut sein, dass das Repertoire der vorhandenen Maßnahmen und Mechanismen bereits ausreicht, weil Gesellschaften es gewohnt sind, Risiken einzugehen und im Bedarfsfall zu handeln (Odlytzko 2019). Cybersicherheit herzustellen bedeutet nicht nur die Überwindung technischer Hindernisse, sondern benötigt gleichzeitig ein tieferes Verständnis für die Veränderungen, die sich aus der Digitalisierung des modernen Lebens ergeben. Es bedarf einer multiperspektivischen Sichtweise, an der Expertinnen und Experten aus verschiedenen wissenschaftlichen Disziplinen ebenso wie aus unterschiedlichen Professionen beteiligt sein müssen.

Die Beiträge dieser Ausgabe

Der erste Beitrag thematisiert das Problem, dass die Herstellung von Cybersicherheit ganz erhebliche langfristige Herausforderungen mit sich bringen kann. Tim Zander, Pascal Birnstill, Florian Kaiser, Marcus Wiens, Jürgen Beyerer und Frank Schultmann zeigen dies in ihrem Beitrag „IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte“. Zeit ist der Faktor, der Technikfolgenabschätzung so schwierig macht – je weiter in die Zukunft wir zu schauen versuchen, desto unschärfer wird unser Blick. Wenn aber heute Technik in den Verkehr (in diesem Fall im wortwörtlichen Sinne) gebracht wird, die in großer Zahl und langfristig genutzt wird und gleichzeitig auch erhebliche Schäden verursachen kann, dann wäre dem Vorsorgeprinzip zufolge ganz besondere Vorsicht geboten. Dies gilt ganz besonders für das von den Autoren gewählte Beispiel (teil-)autonomer Fahrzeuge mit einer Nutzungsdauer von 20 und mehr Jahren. Doch es gibt nur sehr wenige Einsatzgebiete, in denen es Erfahrung mit der kontinuierlichen Nutzung von IKT-Systemen über mehrere Jahrzehnte hinweg gibt; die oben bereits genannten Banken und Versicherungen haben ihre Computersysteme teilweise solange betrieben oder betreiben sie auch heute noch. Ein Vergleich mit einem großen technischen System wie dem Straßenverkehr würde aber vermutlich zeigen, dass sich die Erfahrungen der Banken und Versicherungen nur bedingt auf (teil-)autonome Fahrzeuge übertragen lassen. Eine Großrechenanlage (*mainframe*) als vergleichsweise geschlossenes System in einem hochkontrollierten Umfeld zu betreiben ist etwas anderes als die Funktionsweise eines aus Millionen Fahrzeugen und einer komplexen Infrastruktur bestehenden großen technischen Systems zu garantieren. Insbesondere, da letzteres unter beileibe nicht vollständig kontrollierten Bedingungen operiert und aus Geräten unterschiedlichster Hersteller besteht. Doch nicht nur die Komplexität unterscheidet sich; auch die Zahl der Stakeholder, deren Homo- bzw. Heterogenität und die Schadensarten unterscheiden sich.

Nachweisbarkeit von Cybersicherheit bedeutet, dass kein einziges Bauteil einer IKT-Infrastruktur Cyberattacken ermöglicht.

Der Beitrag „Building resilient cyber-physical power systems“ von Mariela Tapia, Pablo Thier und Stefan Gößling-Reisemann ist aus Perspektive der Technikfolgenabschätzung sowohl im Hinblick auf die Dimensionen der Zeit als auch des Risikos relevant. Die Stromversorgung gehört zu den kritischen Infrastrukturen, denn die Abhängigkeit der modernen Zivilisation von Elektrizität ist augenfällig. Stromausfälle sind nicht nur lästig, sondern können, wenn großflächig und langandauernd auftretend, Leben, Gesundheit und Eigentum vieler Menschen gefährden, Umweltzerstörung durch sekundäre technische Ausfälle bewirken, die Wirtschaft langfristig schädigen, kurzum: ein Land zum Stillstand bringen. Das Risiko ist also hoch, weil die Schadenshöhe enorm sein kann; das ist an sich nichts Neues. Doch da Stromversorgungssysteme (und andere kritische Infrastrukturen) heute ebenfalls informationstechnisch vernetzt sind, existieren neue Bedrohungen und Angriffsvektoren, die dazu beitragen können, dass nicht nur die Schadenshöhe groß ist, sondern auch die Eintrittswahrscheinlichkeit eines Schadens zunimmt. In solchen Fällen sollten (nicht nur) aus TA-Sicht die Alarmglocken schrillen, denn hier ist besondere Vorsorge notwendig. Insofern liefert der Beitrag Hinweise auf Verfahren, die in den TA-Methodenkoffer gut integriert werden können: Ana-

lysen der Vulnerabilität und Resilienz bedienen die Dimension des Risikos und der Zeit.

Kritische Infrastrukturen spielen in dem Beitrag „Siedlungswasserwirtschaft im Zeitalter der Digitalisierung“ von Martin Zimmermann, Engelbert Schramm und Björn Ebert ebenfalls eine zentrale Rolle; nun sind es aber nicht die Strom-, sondern die Wasserversorger, die in den Blick genommen werden. Im Alltag haben wir uns daran gewöhnt, die Verfügbarkeit von Wasser als etwas Selbstverständliches anzusehen und haben in der Regel vergessen, dass dahinter eine komplexe Infrastruktur steht, auch wenn diese in vielen Fällen regional eingegrenzt ist. Ebenso wie die Stromversorger sind die Wasserversorger zunehmend informationstechnisch vernetzt, sodass neue Angriffs- und Schadensszenarien möglich werden. Meist wäre der Ausfall der Wasserversorgung – sei sie nun durch eine Cyberattacke oder andere Faktoren verursacht – räumlich begrenzt. Allerdings bedeutet dies nicht notwendigerweise eine geringe Schadenshöhe, denn der Ausfall der Wasserversorgung in Großstädten wie Berlin würde möglicherweise Hunderttausende oder gar Millionen Menschen direkt betreffen. Indirekt wäre der Schaden vermutlich noch höher, da eine Attacke auf diese essentielle Versorgungsinfrastruktur psychologisch sehr wirksam wäre.

Diese drei Beiträge verdeutlichen: Es bedarf einer (cyber-)sicheren technischen Infrastruktur nicht nur für den Verkehr, für die Strom- und Wasserversorgung, sondern für alle Bereiche des Einsatzes vernetzter IKT. Entscheidend dabei ist, dass diese Sicherheit nachweisbar ist. Arnd Weber, Gernot Heiser, Dirk Kuhlmann, Martin Schallbruch, Anupam Chattopadhyay, Sylvain Guilley, Michael Kasper, Christoph Krauß, Philipp S. Krüger, Steffen Reith und Jean-Pierre Seifert zeigen in ihrem Beitrag „Sichere IT ohne Schwachstellen und Hintertüren“ auf, wie nachweisbare Sicherheit zu erreichen wäre. Die Größe des Autorenkollektivs deutet bereits an, dass es sich hierbei um keine triviale Aufgabe handelt. Denn letztlich bedeutet Nachweisbarkeit der Sicherheit, dass jedes Bauteil einer IKT-Infrastruktur nachweisbar sicher sein muss in dem Sinne einer (in der Praxis kaum erreichbaren) Zielvorgabe, dass es keine Cyberattacken ermöglicht. Dies gilt für die hochkomplexen Prozessoren und integrierten Schaltkreise, also die Hardware, ebenso wie für die Software, die auf den entsprechenden Geräten ausgeführt wird. Welche Brisanz dieses Thema besitzt, lässt sich an der öffentlich kontrovers diskutierten Frage erkennen, ob Geräte des chinesischen Herstellers Huawei beim Aufbau der nordamerikanischen und europäischen 5G-Netze genutzt werden dürfen, da befürchtet wird, dass die Geräte dieses Unternehmens Hintertüren enthalten, die beispielsweise chinesischen Geheimdiensten einen direkten und verdeckten Zugang zur weltweiten Kommunikation bieten. Hier geht es um Erwägungen individueller, unternehmerischer und staatlicher Sicherheit mit räumlich, zeitlich und risikobezogen weitreichenden Konsequenzen.

Fazit

In der Beschreibung der Beiträge des aktuellen TATuP-Themas war vor allem von Risiken und Schaden die Rede; das muss jedoch ergänzt werden um den Hinweis auf den Nutzen und die Chancen der Vernetzung. Auch beim Thema Cybersicherheit kommen Gesellschaften nicht umhin, eine vernünftige Abwägung von Kosten und Nutzen sowie Risiken und Chancen vorzunehmen.

Alle Beiträge des TATuP-Themas zeigen vor allem aber deutlich auf, dass das Nachdenken über Cybersicherheit ein Bestandteil der Technikfolgenabschätzung sein sollte. Moderne Technik hat heute immer IKT-Anteile; kaum mehr ein Gerät ist nicht vernetzbar. Man mag sich lustig darüber machen, dass Alltagsgegenstände wie Toaster, Küchenmaschinen oder Körperwaagen über WLAN verfügen. Bedenkt man jedoch, dass diese Geräte immer auch einen Zugriffspunkt zu einem WLAN-Netz darstellen, das wiederum den Zugang zum Rest des globalen Internets bieten kann, bekommen diese Alltagsgegenstände und deren Cybersicherheit eine neue Bedeutung. Consumer-Elektronik wird in der Regel nur Monate oder wenige Jahre mit Softwareupdates versorgt – danach werden Sicherheitslücken nicht mehr geschlossen. Diese Tatsache macht solche Geräte zu bevorzugten Angriffspunkten für Hacker, weil man in diesen Geräten beispielsweise unbemerkt Schadsoftware installieren kann, sodass etwa der Kühlschrank plötzlich Teil eines Botnetzes werden kann. Sollte man diese Geräte demnach entsorgen, weil sie ein (Cyber-)Sicherheitsrisiko darstellen? Fallen solche Systeme aus, kann dies eine Kaskade weiterer negativer Auswirkungen nach sich ziehen. Die Krisenfestigkeit ganzer Gesellschaften, das sollten die in den Beiträgen angesprochenen Themen deutlich aufzeigen, steht daher durch die ubiquitäre Nutzung hochkomplexer und vernetzter IKT infrage.

Beim Thema Cybersicherheit kommen Gesellschaften nicht umhin, eine vernünftige Abwägung von Kosten und Nutzen sowie Risiken und Chancen vorzunehmen.

In der Informatik kursiert Gerald Weinbergs – ein vor zwei Jahren verstorbener Computerwissenschaftler – zweites Gesetz: „If builders built buildings the way programmers wrote programs, then the first woodpecker that came along would destroy civilization.“ Sicherlich ist dieser Sinnspruch übertrieben, doch

auch in einer Übertreibung steckt meist ein Quäntchen Wahrheit. In den industrialisierten Staaten dieser Welt funktioniert kaum mehr etwas ohne IKT – das sollte nicht nur, aber auch jenen, die sich mit Technikfolgenabschätzung beschäftigen, zu denken geben.

Danksagung

Die Thema-Herausgeber möchten sich bei den Autorinnen und Autoren sowie den Gutachterinnen und Gutachtern für die gelungene Zusammenarbeit bedanken. Ganz besonderen Dank schulden wir Linda Kokott, die uns bei der Findung der Gutachterinnen und Gutachter unterstützt und bei der ersten Sichtung der eingegangenen Beiträge geholfen hat.

Literatur

Bauer, Johannes; van Eeten, Michel (2009): Cybersecurity. Stakeholder incentives, externalities, and policy options. In: Telecommunications Policy 33 (10–11), S. 706–719. DOI: 10.1016/j.telpol.2009.09.001.

Beck, Ulrich (1986): Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt am Main: Suhrkamp.

Boulanin, Vincent (2013): Cybersecurity and the arms industry. In: SIPRI Yearbook 2013: Armaments, disarmament and international security, S. 218–226.

Brito, Jerry; Watkins, Tate (2011): Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. Mercatus Center, Georg Mason University, Working Paper No. 11–24. Online verfügbar unter https://www.mercatus.org/system/files/Loving-Cyber-Bomb-Brito-Watkins.pdf, zuletzt geprüft am 05. 02. 2020.

Copeland, Duncan; Mason, Richard; McKenney, James (1995): Sabre. The development of information-based competence and execution of information-based competition. In: IEEE Annals of the History of Computing 17 (3), S. 30–57. DOI: 10.1109/85.397059.

CSIS – Center for Strategic and International Studies (2018): Economic impact of cybercrime – no slowing down. Online verfügbar unter https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf, zuletzt geprüft am 05. 02. 2020.

Dunn Caveltry, Miriam (2014): Breaking the cyber-security dilemma. Aligning security needs and removing vulnerabilities. In: Science and Engineering Ethics 20 (3), S. 701–715. DOI: 10.1007/s11948-014-9551-y.

Gerovitch, Slava (2004): From newspeak to cyberspeak. A History of Soviet cybernetics. Cambridge, MA: MIT Press.

Hoffman, Lance (1973): Security and privacy in computer systems. Los Angeles, CA: Melville Publications.

Jones, Nicola (2018): How to stop data centres from gobbling up the world's electricity. Nature 561 (7722), S. 163–166. DOI: 10.1038/d41586-018-06610-y.

Martin, James (1973): Security, accuracy, and privacy in computer systems. Englewood Cliffs: Prentice-Hall.

Odlyzko, Andrew (2019): Cybersecurity is not very important. Working Paper. Online verfügbar unter http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf, zuletzt geprüft am 05. 02. 2020.

Redmond, Kent; Smith, Thomas (2000): From Whirlwind to MITRE. The R & D story of the SAGE air defense computer. Cambridge, MA: MIT Press.

Westin, Alan (1967): Privacy and freedom. New York: Atheneum.

PROF. DR. PHIL. HABIL. KARSTEN WEBER
ist Ko-Leiter des Instituts für Sozialforschung und Technikfolgenabschätzung (IST) der OTH Regensburg und einer der drei Direktoren des Regensburg Center of Health Sciences and Technology (RCHST) sowie Honorarprofessor für Kultur und Technik an der BTU Cottbus-Senftenberg. Er beschäftigt sich derzeit mit individuellen und gesellschaftlichen Auswirkungen von IuK-Technologie sowie mit wertebasierter Gestaltung von Technik insbesondere im Gesundheitsbereich.

PD DR. HABIL. MARKUS CHRISTEN
ist seit 2016 Geschäftsführer der Digital Society Initiative und leitet eine Forschungsgruppe am Institut für Biomedizinische Ethik der Universität Zürich. Seine Forschungsgebiete sind Ethik von Informations- und Kommunikationssystemen, Neuroethik und Empirische Ethik.

PROF. DR. DOMINIK HERRMANN
hat den Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen an der Fakultät für Wirtschaftsinformatik und Angewandte Informatik der Otto-Friedrich-Universität Bamberg inne. Seine Forschungsthemen sind der Entwurf und die Bewertung nutzbarer und unaufdringlicher Technologien zur Verbesserung der Privatsphäre, der Schutz vor unerwünschter Verfolgung von Online- und Mobilnutzern sowie allgemein Sicherheits- und Datenschutzfragen.

IT-Sicherheit im Wettstreit um die erste autonome Fahrzeugflotte

Ein Diffusionsmodell

Tim Zander, *Institut für Anthropomatik und Robotik, Lehrstuhl für Interaktive Echtzeitsysteme Karlsruher Institut für Technologie (KIT), c/o Technologiefabrik, Haid-und-Neu-Str. 7, 76131 Karlsruhe (tim.zander@kit.edu)*
Pascal Birnstill, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (pascal.birnstill@iosb.fraunhofer.de)*
Florian Kaiser, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (florian-klaus.kaiser@kit.edu)*
Marcus Wiens, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (marcus.wiens@kit.edu)*
Jürgen Beyerer, *Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) (juergen.beyerer@iosb.fraunhofer.de)*
Frank Schultmann, *Institut für Industriebetriebslehre und Industrielle Produktion (IIP), Karlsruher Institut für Technologie (KIT) (frank.schultmann@kit.edu)*

In der Fahrzeugindustrie halten aktuell eine Reihe von Neuerungen Einzug. So sorgen neben dem Umstieg auf E-Mobilität hochtechnologische Assistenzsysteme in Fahrzeugen für einschneidende Veränderungen. Eine weitere mit diesen neuen Systemen einhergehende Neuerung ist, dass Autos nun wie Smartphones mit regelmäßigen Updates versorgt werden. Der Hersteller Tesla behauptet sogar, seine Autos in Zukunft per Softwareupdate zum vollautonomen Fahrzeug upgraden zu können. Diese Entwicklung kann zu einer nicht nachhaltigen und risikoreichen Entwicklung der IT-Security und der Umweltbilanz des Fahrzeugsektors führen.

IT security and competition in the automotive industry
A diffusion model

Today's automotive industry is changing rapidly. The slow movement toward electric mobility and highly technical assistant systems challenge old hierarchies. Another innovation associated with the latter is that cars now receive regular software updates, just like smartphones. Tesla even claims to be able to upgrade their cars to fully autonomous driving in the future. This could lead to an unsustainable and risky development of IT security and the environmental performance of the vehicle sector.

Keywords: *IT security; autonomous mobility; diffusion model*

https://doi.org/10.14512/tatup.29.1.16
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 17. 12. 2019

Motivation

Durch den Einzug von Software mit regelmäßigen Updates in Fahrzeugen wird die IT-Security zunehmend relevant für Autobauer. Oftmals fehlt beim Anwender im Diskurs um die Bedeutung der IT-Security das Bewusstsein über die Möglichkeiten, welche Sicherheitslücken einem Angreifer bieten (Bordonali et al. 2017). Entsprechend vulnerabel sind viele modernen Automobile. Dabei sei, glaubt man Elon Musk, ein flottenweiter Hack eines der größten Risiken für die autonome Mobilität. Der Nachrichtendienst heise.de machte in einem Bericht auf die geringen Sicherheitsstandards in der Automobilindustrie aufmerksam, nachdem es einem Hacker gelungen war „weltweit den Verkehr beeinflussen" zu können (Scherschel 2019). Insbesondere die Motivation, eine Vorreiterposition in der autonomen Mobilität einzunehmen und so eine gute Marktposition zu erlangen, kann vor dem Hintergrund der kapitalintensiven Transformation in Richtung Elektromobilität eine weitere Gefahr für die IT-Sicherheit von Automobilen darstellen. Zusammengenommen kann die Verbindung aus Vernetzung, fehlender Erfahrung mit der neuen Technologie und hohem Wettbewerbsdruck potenziell zu hohen systemischen Risiken bzgl. der IT-Sicherheit führen.

Deep und Fleet Learning für autonomes Fahren

In modernen Fahrzeugen stehen sämtliche Fahrer- und Bedienbefehle wie Bremsen, Lenkung, Regelung der Antriebsleistung über ein elektronisches Nachrichtenprotokoll zur Verfügung. Damit sind alle Voraussetzungen erfüllt, um ein Fahrzeug

von einem Computerprogramm autonom steuern zu lassen. Die Frage, die sich nun stellt ist, welche Sensoren und welche Informationsfusion der Daten dieser Sensoren und welche daraus abgeleiteten Steuerbefehle für ein fahrerloses Fahrzeug nötig sind (Paden et al. 2016).

Ein modernes Auto besitzt eine Vielzahl von Sensoren. Als Beispiel dafür kann das seit 2011 vorgeschriebene Electronic Stability Control-System dienen, das durch gezieltes Verzögern einzelner Räder ein Ausbrechen des Wagens zu verhindern versucht. Dafür werden u. a. Sensoren für den Lenkwinkel, Drehrate, Radgeschwindkeits- sowie die Längs- und Gierachsenbeschleunigung benötigt. In einem Auto mit Autonomiestufe 2 (Perret et al. 2018; Gasser et al. 2012; Wood et al. 2019) wird zusätzlich eine Vielzahl von Sensoren für die Beobachtung der Strecke und der anderen Verkehrsteilnehmer benötigt (Gasser et al. 2012).

In der Folge gehen wir exemplarisch auf die Autonomisierungsbemühungen des elektrischen Fahrzeugherstellers Tesla ein. Die einzelnen Wettbewerber unterscheiden sich bezüglich ihres Vorgehens zwar in einigen Aspekten, diese unterschiedlichen Herangehensweisen sind jedoch für unsere Diskussion und für das weitere Verständnis der Thematik nicht weiter relevant. So hat Tesla seit 2016 für den „Autopilot“ acht Kamera-, zwölf Sonar- und einen Radarsensor verbaut (Tesla 2019 b). Die eingehenden Daten dieser Sensoren müssen fusioniert werden, um den für das Fahrzeug relevanten Zustand der Umwelt zu schätzen. Diese Information über die aktuelle Situation und das entsprechende Ziel müssen dann in entsprechende Steuerbefehle umgesetzt werden.

Für die Verarbeitung von Bilddaten hat sich Deep-Learning als zielführend erwiesen. Bei diesen Verfahren werden künstliche neuronale Netze durch Lernbeispiele angepasst. Hierbei werden große Datenmengen analysiert, um Muster zu erkennen nach denen dann Entscheidungen getroffen werden können und nach denen das Verhalten ausgerichtet werden kann. Damit werden Maschinen befähigt, autonom ihr Verhalten zu optimieren. Mithilfe dieses Verfahrens können in neuen Bildern mit hoher Genauigkeit Objekte wie Tiere und Fußgänger erkannt werden. Passende Datensätze von Bildern zu erstellen und dann zu annotieren ist ein zeit- und kostenintensives Problem. Für den Betrieb eines autonomen Fahrzeugs ergeben sich weitere Herausforderungen bei der Sensorfusion. Unter anderem muss erkannt werden, welcher Teil der Fahrbahn wirklich frei befahrbar ist und ob etwaige bewegliche Hindernisse (wie andere Verkehrsteilnehmer) den geplanten Fahrweg versperren könnten.

Deshalb werden große Mengen an Trainingsbeispielen benötigt. Der Ansatz, auf welchen Tesla für dieses Problem zurückgreift, ist das sogenannte *Fleet Learning*. Hierbei trägt jedes Auto der Fahrzeugflotte zum Sammeln der Trainingsbeispiele bei. Als Beispiele dafür wurden am Tesla *Autonomy Investor Day* Trainingsdaten von der Flotte gesammelt und von Menschen annotiert, um richtig zu detektieren, ob Fahrräder an anderen Fahrzeugen befestigt sind oder als eigenständige Verkehrsteilnehmer am Verkehrsgeschehen teilnehmen (Tesla 2019 a). Ein weiteres Beispiel stellte die vollautomatische Generierung von Lerndaten dar, um Spurwechsel und Fahrverhalten anderer Fahrzeuge besser vorherzusagen.

Fleet Learning ermöglicht das Sammeln großer Mengen an Trainingsbeispielen für die Software autonomer Fahrzeuge.

Zusammenfassend kann Tesla durch Abfrage der sensorgenerierten Daten seiner Flotte und die Beobachtung der Tesla-Fahrer automatisiert Trainingsbeispiele sammeln und diese teilweise sogar automatisch annotieren (Eady 2019). Diese werden dann zur Verbesserung der Fahrzeugsoftware genutzt.

Obwohl es trotz dieser genannten Fortschritte zurzeit noch nicht klar ist, wann, bzw. ob überhaupt vollautonome Fahrzeuge existieren werden, sollte man sich darüber klarwerden, dass der Kauf eines vollautonomen Fahrzeugs viele Ähnlichkeiten mit dem Kauf von Softwarepaketen hat. So kostet zum Beispiel bei Tesla das gleiche Auto ohne die Autopilotfunktion 5.000 € weniger. Wie bei anderen Softwarelizenzen kann die kommerzielle Nutzung beschränkt werden. So enthält die Lizenz für den Autopiloten von Tesla eine Exklusivitätsklausel, die besagt, dass mit Autos im vollautonomen Modus nur im Tesla Robotaxi-Netzwerk Geld verdient werden kann (Tesla 2019 a).

IT-Sicherheit autonomer Fahrzeuge

Die Anbindung an das Internet zum Zwecke der Versorgung mit Updates, Verkehrs- und Mediendaten führt zu der Gefahr des Remotezugriffs durch unautorisierte Personen. So konnten Forscher 2014 demonstrieren, wie über das Mobilfunknetz ein Auto von der Ferne aus angegriffen wurde und unter anderem die Bremsen deaktiviert werden konnten (Miller und Valasek 2014). Es ist zu erwarten, dass elementare Funktionen wie Bremsen, Lenken und Beschleunigen evtl. sogar gewollt noch für längere Zeit über das Internet zur Verfügung stehen werden, da autonome Fahrzeuge vermutlich noch lange nicht auf alle Situationen selbstständig reagieren können (Wood et al. 2019). Ein menschlicher Operator müsste somit per Fernzugriff eingreifen, um z. B. ein

Wendemanöver zu vollführen, zu dem das Fahrzeug selbst nicht in der Lage ist.

Ein weiteres Problem ist ein starkes Wachstum der Softwaregröße und damit der Komplexität. So erhöhte sich die durchschnittliche Softwaregröße in Fahrzeugen von ca. 10 Mio. Codezeilen im Jahr 2010 auf ca. 150 Mio. Codezeilen im Jahr 2016. Als Konsequenz wurden in letzter Zeit vermehrt softwarebedingte Rückrufe von ausgelieferten Fahrzeugen durchgeführt. Die Sicherstellung hoher Softwarequalität nimmt insofern eine Schlüsselrolle ein, da sie maßgeblich die Sicherheit des Fahrzeugbetriebs bestimmt und für den breiten Gebrauch unerlässlich ist (Consumer Watchdog 2019). Eine weitere große Gefahr besteht für die Privatheit aller Verkehrsteilnehmer, da Fahrzeuge Kameras, andere Sensoren und entsprechende Hardware haben, mit denen eine Überwachung sowie Verarbeitung der Daten stattfinden kann. Von ihnen geht also mindestens die gleiche Gefahr für Persönlichkeitsrechte (u. a. Recht auf freie Entfaltung der Persönlichkeit sowie informationelle Selbstbestimmung) der Bürger aus wie von Überwachungskameras im öffentlichen Raum, die durch das Internet erreichbar sind. Darüber hinaus sind Datenschutzproblematiken bezüglich der Datenaggregation sowie der Analyse von Daten der gesamten Fahrzeugflotte zu nennen.

Ähnlich wie im Softwaremarkt ist auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.

Auswirkungen auf den wirtschaftlichen Wettbewerb

Der dargestellte technologische Schock in der Automobilbranche durch autonomes Fahren verändert die Wettbewerbssituation erheblich. Hierbei ist die Verlagerung der Differenzierungsmerkmale und Veränderung der Wahrnehmung des Automobils von einer maßgeblich durch ihre Hardware bestimmten Maschine hin zu einer sich durch Software definierenden Maschine von großer Bedeutung (Teece 2018). So verschiebt sich durch autonomes Fahren der Fokus des Kunden vom Fahrerlebnis hin zur fahrzeuginternen Multimediaerfahrung (Aboagye et al. 2017). Dies hat zur Folge, dass sich die Regeln des Wettbewerbs grundlegend verändert und dadurch den Markt für neue Wettbewerber geöffnet haben. Dementsprechend drängen viele neue Wettbewerber auf den Automobilmarkt (Teece 2018). Hierbei ist nicht nur eine vertikale, sondern auch eine horizontale Integration vieler Unternehmen zu beobachten (Burkacky et al. 2018). Dies führt temporär zu einer Steigerung der Wettbewerbsintensität. Ermöglicht wird dies dadurch, dass die etablierten Unternehmen durch die veränderte Bedeutung der Software eines Automobils an Wettbewerbsfähigkeit sowie technologischem Vorsprung verloren haben und somit Markteintrittsbarrieren gesunken sind (Aboagye et al. 2017). Die Auswirkungen des technologischen Schocks verdeutlicht auch die Prognose einer Verringerung des Wertanteils traditioneller Technologien auf dem Automobilmarkt von 98 % im Jahr 2017 auf ca. 50 % im Jahr 2030 (Aboagye et al. 2017).

Die technologischen Rahmenbedingungen der Entwicklung des autonomen Fahrens bestimmen die neue Wettbewerbssituation. Hierbei nimmt die Erlangung eines technologischen Vorsprungs gegenüber den Konkurrenten bei der hohen Komplexität der Software, welche autonomes Fahren ermöglicht, eine entscheidende Rolle ein (Aboagye et al. 2017). Technologischer Vorsprung gegenüber den Wettbewerbern erhöht dabei die Wettbewerbsfähigkeit und damit die potenzielle Marktmacht sowie Marktdurchdringung eines Anbieters. Mit einer gesteigerten Marktdurchdringung verringern sich wiederum die Informationskosten (Charette 2009). Es sei dabei auf das *Fleet Learning* verwiesen, bei dem durch eine größere Marktausbreitung zusammen mit Netzwerkeffekten vereinfacht Trainingsdaten durch sich im Betrieb befindliche Fahrzeuge generiert werden können. Die geringeren Informationskosten gegenüber den Wettbewerbern mit schlechterer Marktposition ermöglichen es den Unternehmen nochmals, ihren technologischen Vorsprung weiter auszubauen (Bertoncello et al. 2016).

Die Entwicklung der Technologie des autonomen Fahrens führt dabei nicht nur zu einem technologischen Vorsprung, sondern verursacht auch hohe Fixkosten. Diese Fixkosten verteilen sich dabei auf alle Fahrzeuge, wodurch sich Skaleneffekte ergeben. Aufgrund der Skaleneffekte (Fixkostendegression) und Netzwerkeffekte (sinkende Informationskosten) steigt der Wert einer Flotte, wie bei Software-Produkten (Anderson 2008), überproportional zu der Zahl seiner Fahrzeuge. Dies wiederum impliziert Lock-In-Effekte, da mit steigender Größe des Netzwerks der Austritt aus dem Netzwerk für jeden Nutzer unattraktiver wird und durch die Exklusivitätsklausel in der Lizenz noch verstärkt wird. Aufgrund der hohen Entwicklungskosten für autonomes Fahren sowie der dargestellten Besonderheiten der Technologie erhöhen sich nun wieder die Markteintrittsbarrieren für neue Marktteilnehmer, welche die Marktposition bestehender Anbieter langfristig sichern. Ähnlich wie im Softwaremarkt (Anderson 2008) ist somit auch eine Monopolisierung des Marktes für autonome Mobilität zu erwarten.

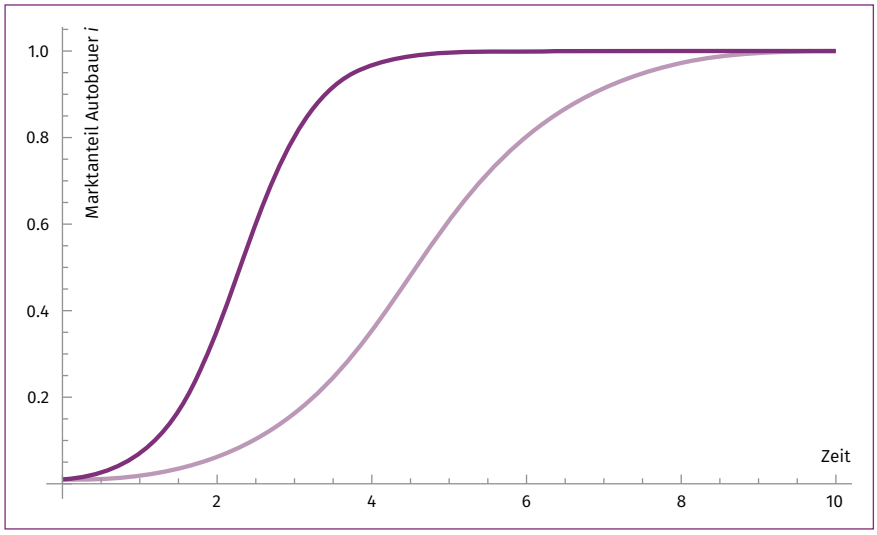


Abb. 1: Marktdurchdringung in Abhängigkeit von IT-Sicherheitsinvestitionen. *Quelle: Eigene Darstellung*

Diffusionsmodell für autonome Fahrzeuge

Um die Marktdurchdringung durch autonome Fahrzeuge und damit den Wettstreit um die erste autonome Fahrzeugflotte zu beschreiben, erscheint die Diffusionstheorie als besonders geeignet, da sie die Adoption neuer Technologien auf einem Markt und damit den Prozess der Marktdurchdringung beschreibt (Geroski 2000). Gemäß Rogers (2010) können die Nutzer neuer Technologien nach dem Grad ihrer Bereitschaft, diese zu nutzen, klassifiziert werden. Hierbei hängen Adoptionsentscheidungen von Informationen über den Nutzen dieser Technologie ab. Die Informationen können dabei aus direktem Erleben aber auch indirekt durch Erzählen erlangt werden. Unter der Annahme einer konstanten Penetrationsrate α kann der Marktanteil $f(t)$ bestimmt werden, der sich als sogenannte Sigmoidfunktion darstellen lässt.

$$f(t) = \frac{1}{1+\frac{1-f(t_0)}{f(t_0)} \cdot e^{-\alpha \cdot (t-t_0)}}$$

Dabei wird für den initialen Marktanteil $f(t_0)$ die Bedingung $f(t_0) > 0$ angenommen, das heißt, das Modell liefert eine Erklärung für die Diffusion autonomer Fahrzeuge nach bereits erfolgtem Markteintritt der Unternehmen. Die Penetrationsrate α beschreibt dabei die Geschwindigkeit der Marktdurchdringung beziehungsweise Diffusion autonomer Fahrzeuge. Sie stellt damit die wichtigste Komponente der Analyse des Wettstreits um die erste autonome Fahrzeugflotte dar.

Davies (1979) bestimmt hierbei als zentrale Determinante den pekuniären Nutzen der Technologie, d. h. die Höhe der Penetrationsrate wird maßgeblich durch den finanziellen Mehrwert durch die Adoption der neuen Technologie bestimmt. Hierbei gilt: je höher der Gewinn für den Nutzer, desto höher seine Priorität der Adoption der neuen Technologie und umso höher die Penetrationsrate. Somit stellt die Erhöhung des Gewinns für den Nutzer beziehungsweise die Vorteilhaftigkeit der neuen Technologie die Priorität für das Handeln der Unternehmen dar, wenn die Erlangung eines möglichst großen Marktanteils in möglichst kurzer Zeit das Ziel ist. Diese Ausrichtung unternehmerischen Handelns scheint in der dargestellten Wettbewerbssituation um die erste autonome Fahrzeugflotte plausibel zu sein.

Das Unternehmen muss also versuchen, autonome Fahrzeuge so günstig wie möglich auf den Markt zu bringen, um in der Phase des intensiven Wettbewerbs möglichst schnell eine ausreichend große Fahrzeugflotte (kritische Schwelle, ab der die Netzwerkeffekte und Skaleneffekte einsetzen) zu erreichen. Unter der Bedingung, dass das Unternehmen kurzfristig keinen Verlust macht, kann die kurzfristige Preisuntergrenze als Veräußerungspreis angenommen werden. Ein tieferer Preis würde das Unternehmen in finanzielle Schieflage bringen, während ein höherer Preis mit dem Unternehmensziel der schnellen Marktdurchdringung nicht konform wäre.

Die Penetrationsrate von Unternehmen i kann bei der Beschränkung der Bestimmung des Nutzens auf den monetären Mehrwert mit der Differenz aus Zahlungsbereitschaft und variablen Kosten gleichgesetzt werden.

$$\alpha_i = Z - k_{v,i}$$

Während im Allgemeinen Ansatz zur Bestimmung der Penetrationsrate ein Nutzenvergleich mit Konkurrenzprodukten erforderlich ist, genügt für den Monopolfall die hier vorgestellte einfache Version, die keine Interaktion mit Konkurrenten erfasst. Unter der Annahme einer konstanten Zahlungsbereitschaft der potenziellen Nutzer stellt sich die Marktdurchdringung in Abhängigkeit von k_v wie in Abb. 1 dar.

Im Hinblick auf die IT-Sicherheit kann es nun erstrebenswert erscheinen Kosten einzusparen, um mit einem geringeren Preis an den Markt zu gehen, insbesondere wenn man die IT-Sicherheit weder als Leistungsmerkmal noch als Begeisterungsmerkmal sieht (Kano et al. 1984). Dies kann am Beispiel der Verbindung von Infotainmentsystemen mit Controller Area Netzwerken erläutert werden, welche sicherheitsrelevante Fahrzeugsysteme steuern (Consumer Watchdog 2019). So stellt das Infotainmentsystem eine Leistungsanforderung und damit ein zentrales Differenzierungsmerkmal dar, während die IT-Sicherheit ein Basismerkmal darstellt. Um eine herausragende Leistung im Bereich des Infotainments zu erreichen, wird hierbei das Controller Area Network zulasten der Sicherheit mit dem Infotainmentsystem verbunden (Consumer Watchdog 2019). Dies hat den Vorteil, dass intelligente Lautstärkeregelungen in Abhängigkeit von

der Geschwindigkeit sowie der Motorgeräusche ermöglicht werden (Consumer Watchdog 2019). Darüber hinaus schränken Sicherheitsmaßnahmen die Funktionalität ein, welches den wahrgenommenen Nutzen bei den Kundinnen und Kunden und damit deren Zahlungsbereitschaft negativ beeinflusst. Es kann für die Firma also sinnvoll sein, in einem kurzfristigen Betrachtungshorizont auf Investitionen in Maßnahmen zur IT-Sicherheit zu verzichten, um eine gute Marktposition zu erreichen (Anderson 2008). Da Kundinnen und Kunden ein sicheres Automobil zunächst nicht von einem nicht sicheren unterscheiden können, kann es aufgrund dieser asymmetrischen Information sogar langfristig zum Marktversagen kommen (Akerlof 1970), wenn zeitversetzt die Sicherheitsdefizite bekannt werden und die Kunden dadurch schließlich verunsichert bzw. abgeschreckt werden. Hierbei unterstreicht das Beispiel der Firma Microsoft, bzw. deren Vorgehen zur Erlangung eines hohen Marktanteils, die angemerkte Ähnlichkeit der Softwarebranche zur Branche der autonomen Mobilität. So hatte Microsoft in den 1990er-Jahren das Motto „Ship it on Tuesday and get it right by version 3“ mit der bekanntermaßen schlechten IT-Sicherheit des Produkts in dieser Zeit. Um eine Monopolstellung zu erreichen war es also nicht nötig, ein von Anfang an sicheres Produkt zu entwerfen (Anderson 2008). Einsparungen bei den Ausgaben für IT-Sicherheit würden also zu einer schnelleren Durchdringung und Beherrschung des Marktes, jedoch langfristig zu steigenden Risiken führen.

Die Wartung von Software in autonomen Fahrzeugen muss langfristig sichergestellt werden.

Auswirkungen auf die IT-Sicherheit

Falls es möglich sein wird, ein vollautonomes Auto zu entwickeln, zur Marktreife zu führen und zeitnah eine entsprechende Marktposition zu erlangen (schnelles Szenario), wird die Bedeutung der IT-Sicherheit durch die große Verbreitung derselben Software an Bedeutung gewinnen. So steigert sich auch die Attraktivität eines Hacks durch die Möglichkeit, mehrere Fahrzeuge zu beeinflussen. Entsprechend wachsen die Anforderungen an die IT-Sicherheit der Fahrzeuge.

Falls sich autonomes Fahren in nächster Zeit nicht verwirklichen lassen sollte, bzw. eine schnelle Marktdurchdringung nicht erreicht werden kann (langsames Szenario) und sich die Investitionen in Techniken des autonomen Fahrens wie *Fleet Learning* als langfristig nicht rentabel erweisen, würden gegensätzliche Effekte eintreten (Porter 2019). So kann das investierte Kapital nicht mehr zurückgewonnen werden, was zur Abwicklung ganzer Unternehmen führen könnte oder diesen zumindest einen rigiden Sparkurs diktieren würde. In diesem Fall könnte es zum Problem werden, dass es dann keinen Verantwortlichen mehr gibt, der die Software warten kann oder will. Diese Gefahr wird durch die steigende Wettbewerbsintensivität in der Automobilbranche sowie durch das Eintreten vieler kleiner Unternehmen immer präsenter. Es wäre also dann unter Umständen unmöglich, etwaige Schwachstellen zu reparieren, da evtl. niemand mehr Zugriff auf den Quelltext der Software hat.

Mindestens würden jedoch Lebenszyklusprobleme auftreten, sollte sich herausstellen, dass die aktuelle Fahrzeuggeneration auch nicht mit Umrüstung für autonomes Fahren geeignet ist. So würde die Softwarewartung bei dieser veraltenden Flotte eine Externalität darstellen, da ökonomische Investitionen ohne zukünftigen Nutzen erforderlich wären. Dies kann damit erklärt werden, dass die Kosten für unterlassene Wartung nicht beim Automobilhersteller anfallen, sondern direkt beim Kunden. Dadurch finden diese Kosten in Marktpreisen keine Berücksichtigung. So wäre es denkbar, dass die Unternehmen den Softwaresupport für Altfahrzeuge einstellen oder den Betrieb derartiger Fahrzeuge künstlich verteuern (Wiens und Chamberlain 2018). Besonders plausibel werden diese Lebenszyklusprobleme, wenn man bedenkt, dass das Durchschnittsalter eines Autos in der Europäischen Union elf Jahre beträgt. So stellt sich die Frage, mit welchen Softwareentwicklungskonzepten man in 20 Jahren Updates für ein heutiges Fahrzeug zur Verfügung stellen kann (Anderson 2018).

Vorschläge zur Vermeidung

Um Bedrohungen durch softwaremäßig nicht mehr gewartete Altfahrzeuge zu vermeiden, wäre es denkbar, diese durch die einschneidende technische Maßnahme des *„Kill Switch“* hart vom Internet zu trennen (Consumer Watchdog 2019). Auch scheint die geforderte Trennung von Infotainment- und Kontrollsystemen in den Fahrzeugen im Hinblick auf die IT-Sicherheit begrüßenswert.

Als Mechanismus für die Erhöhung der IT-Sicherheit könnten Strafen für deren Vernachlässigung dienen. Natürlich stellen sich hier Fragen nach funktionierenden Strafverfahren und Durchsetzbarkeit, die noch überhaupt nicht geklärt sind. Der Vorschlag, sich an den Best Practices der Flugzeugindustrie zu orientieren und sich von allzu komplexer Software zu verabschieden, scheint im Sinne der Wartbarkeit und IT-Sicherheit wünschenswert (Consumer Watchdog 2019). Jedoch steht dies im Gegensatz zum Interesse der Autobauer, die neuesten Assistenzsysteme zu verbauen.

Da Softwarewartung wie gezeigt eine Externalität darstellt, könnten Anbieter zumindest im Falle wirtschaftlicher Schwie-

rigkeiten die Wartung einstellen, den Weiterbetrieb der Fahrzeuge verhindern, die Fähigkeit zur Wartung meistbietend verkaufen oder etwaige Gläubiger des Unternehmens könnten versuchen, durch die künstliche Verteuerung von Updates ihr Kapital zurückzuholen. Dies würde dazu führen, dass sich die Kosten für den Weiterbetrieb eines Fahrzeuges sehr erhöhen oder dieser schlicht unmöglich wird, sodass sich in der Folge die Lebensdauer eines Fahrzeugs verkürzt. Wenn man nun bedenkt, dass ungefähr die Hälfte des gesamten emittierten CO_2 eines Verbrennerfahrzeuges durch die Herstellung erzeugt wird – bei Elektrofahrzeugen ist der absolute Wert und der Anteil noch höher – so ist das vorzeitige Betriebsende eines Automobils aus IT-Sicherheitsproblemen bereits aus ökologischen Gründen untragbar (unter der Vorrausetzung, dass das Fahrzeug dann durch ein neues ersetzt wird). Eine Regulierung, die den Weiterbetrieb der Fahrzeuge über mindestens 20 Jahre sicherstellt, scheint insbesondere aufgrund der gesteigerten Lebenserwartung von Elektroautos wünschenswert. Dass das Interesse an IT-Sicherheit und am günstigen Weiterbetrieb von Altfahrzeugen geringer sein wird als bspw. von Flugzeugen, wird maßgeblich daran liegen, dass es sich bei den Betroffenen um eine deutlich weniger einflussreiche und zahlungskräftige Käufergruppe handelt (Anderson 2008). Da Fahrzeughersteller Gebrauchtwagenmärkte als Wachstumshindernis sehen (Bavier et al. 2019), liegt die Vermutung nahe, dass die mit Kontrolle über die in Fahrzeugen installierte Software einhergehende Macht irgendwann dazu genutzt wird, besonders in wirtschaftlich schwierigen Zeiten den Weiterbetrieb der Fahrzeuge zu erschweren, um damit künstlich Nachfrage zu erzeugen. Zumindest aber sollte nicht darauf gehofft werden, dass die Industrie selbst für eine nachhaltige Softwareentwicklung sorgt und so ein langfristiger Weiterbetrieb der Fahrzeuge mit sicherer Software möglich wird. Ein langfristiger Weiterbetrieb der Fahrzeuge würde einen Teil zur zukünftigen CO_2-Vermeidung beitragen. Aufgrund der bevorstehenden Klimakatastrophe sollten sich Wirtschaft, Wissenschaft und Politik zusammenzuschließen (Anderson 2001), um den IT-Sicherheit und sicheren Weiterbetrieb von Fahrzeugen über die geplante Obsoleszenz hinaus zu gewährleisten.

Literatur

Aboagye, Aaron; Baig, Aamer; Hensley, Russel; Kelly, Richard; Padhi, Asutosh; Shafi, Danish (2017): Facing digital disruption in mobility as a traditional auto player. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Facing%20digital%20disruption%20in%20mobility%20as%20a%20traditional%20auto%20player/Facing-digital-disruption-in-mobility-as-a-traditional-auto-player.ashx, zuletzt geprüft am 17. 12. 2019.

Akerlof, Georg (1970): The market for „lemons". Quality uncertainty and the market mechanism. In: The Quarterly Journal of Economics, 84 (3), S. 488–500.

Anderson, Ross (2001): Why information security is hard. An economic perspective. Seventeenth Annual Computer Security Applications Conference, 10–14 December 2001. New Orleans: IEEE Computer Society. DOI: 10.1109/ACSAC.2001.991552.

Anderson, Ross (2008): Security engineering. A guide to building dependable distributed systems. New York: John Wiley & Sons.

Anderson, Ross (2018): Making security sustainable. In: Communications of the ACM, 61 (3), S. 24–26.

Bavier, Joe; Rumney, Emma; Miriri, Duncan (2019): Auto giants battle used car dealers for Africa's huge market. Online verfügbar unter https://www.reuters.com/article/us-africa-autos/auto-giants-battle-used-car-dealers-for-africas-huge-market-idUSKCN1RO0OJ, zuletzt geprüft am 19. 11. 2019.

Bertoncello, Michele et al. (2016): Monetizing car data new service business opportunities to create new customer benefit. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Monetizing%20car%20data/Monetizing-car-data.ashx, zuletzt geprüft am 19. 11. 2019.

Bordonali, Corrada; Ferraresi, Simone; Richter Wolf (2017): Shifting gears in cyber security for connected cars. Online verfügbar unter https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Shifting%20gears%20in%20cybersecurity%20for%20connected%20cars/Shifting-gears-in-cybersecurity-for-connected-cars.ashx, zuletzt geprüft am 19. 11. 2019.

Burkacky, Ondrej; Deichmann, Johannes; Doll, Georg; Knochenhauer, Christian (2018): Rethinking car software and electronics architecture. Online verfügbar unter https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/rethinking-car-software-and-electronics-architecture, zuletzt geprüft am 19. 11. 2019.

Charette, Robert (2009): This car runs on code. Online verfügbar unter https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, zuletzt geprüft am 19. 11. 2019.

Consumer Watchdog (2019): Kill switch. Why connected cars can be killing machines and how to turn them off. Online verfügbar unter https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19_0.pdf, zuletzt geprüft am 19. 11. 2019.

Davies, Stephen (1979): The diffusion of process innovations. Cambridge, U. K.: Cambridge University Press.

Eady, Trent (2019): Tesla's deep learning at scale. Using billions of miles to train neural networks. What Tesla can do that Waymo can't. Online verfügbar unter https://towardsdatascience.com/teslas-deep-learning-at-scale-7eed85b235d3, zuletzt geprüft am 19. 11. 2019.

Gasser, Tom et al. (2012): Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe. In: Berichte der Bundesanstalt für Straßenwesen. Fahrzeugtechnik Heft F83. Bremerhaven: Wirtschaftsverlag NW. Online verfügbar unter https://bast.opus.hbz-nrw.de/frontdoor/index/index/docId/541, zuletzt geprüft am 14. 01. 2020.

Geroski, Paul (2000): Models of technology diffusion. In: Research Policy 29 (4–5), S. 603–625.

Kano, Noriaki; Seraku, Nobuhiko; Takahashi, Fumio; Tsuji, Shin-Ichi (1984): Attractive quality and must-be quality. In: Journal of the Japanese Society for Quality Control 14 (2), S. 147–156.

Miller, Charlie; Valasek, Chris (2014): Adventures in automotive networks and control units. Online verfügbar unter https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, zuletzt geprüft am 19. 11. 2019.

Paden, Brian; Cap, Michal; Yong, Sze Zheng; Yershov, Dmitry; Frazzoli, Emilio (2016): A survey of motion planning and control techniques for self-driving urban vehicles. In: IEEE Transactions on Intelligent Vehicles1 (1), S. 33–55.

Perret, Fabienne; Fischer, Remo; Frantz, Holger (2018): Automated driving as a challenge to cities and regions. In: TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis 27 (2), S. 31–37. DOI: 10.14512/tatup.27.2.31.

Porter, Jon (2019): Elon Musk says free self-driving chip upgrade could come to older Teslas this year. Online verfügbar unter https://www.theverge.com/2019/7/8/20685873/tesla-fsd-chip-upgrade-2019-install-hw2-full-self-driving, zuletzt geprüft am 19. 11. 2019.

Rogers, Everett (2010): Diffusion of innovations. New York: The Free Press.

Scherschel, Fabian (2019): Hacker knackt Auto-GPS-Tracker. „Ich kann weltweit den Verkehr beeinflussen". Online verfügbar unter https://heise.de/-4408466, zuletzt geprüft am 19. 11. 2019.

Teece, David (2018): Tesla and the reshaping of the auto industry. In: Management and Organization Review 14 (3), S. 501–512.

Tesla (2019 a): Tesla Autonomy Investor Day. Online verfügbar unter https://ir.tesla.com/events/event-details/tesla-autonomy-investor-day, zuletzt geprüft am 19. 11. 2019.

Tesla (2019 b): Support Autopilot. Online verfügbar unter https://www.tesla.com/support/autopilot, zuletzt geprüft am 19. 11. 2019.

Wiens, Kyle; Chamberlain, Elizabeth (2018): John Deere just swindled farmers out of their right to repair. Online verfügbar unter https://www.wired.com/story/john-deere-farmers-right-to-repair, zuletzt geprüft am 19. 11. 2019.

Wood, Matthew et al. (2019): Safety first for automated driving. Online verfügbar unter https://www.daimler.com/documents/innovation/other/safety-first-for-automated-driving.pdf, zuletzt geprüft am 19. 11. 2019.

DR. TIM ZANDER

ist wissenschaftlicher Mitarbeiter des Lehrstuhls für Interaktive Echtzeitsysteme (IES) sowie des Kompetenzzentrums für angewandte Sicherheitstechnologie (KASTEL) und forscht im Bereich der Modellierung und Quantifizierung von IT-Security und Privacy.

DR.-ING. PASCAL BIRNSTILL

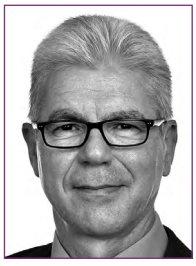
ist wissenschaftlicher Mitarbeiter am Fraunhofer IOSB und KASTEL. Seine Forschungsschwerpunkte liegen im technischen Datenschutz, der Datensouveränität und dem Trusted-Computing.

FLORIAN KAISER

ist wissenschaftlicher Mitarbeiter in der Forschungsgruppe Risikomanagement am Institut für Industriebetriebslehre und Industrielle Produktion (IIP) sowie KASTEL. Er forscht im Bereich des Cyberrisikomanagements und der Analyse sowie Modellierung von Wirtschaftssystemen.

DR. RER. POL. MARCUS WIENS

ist Leiter der Forschungsgruppe Risikomanagement am IIP sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte liegen im Bereich des ökonomischen Risikomanagements, der Analyse von System- und Verhaltensrisiken sowie der Akzeptanz- und Vertrauensforschung.



PROF. DR.-ING. JÜRGEN BEYERER

ist der Leiter des Fraunhofer IOSB sowie des IES Lehrstuhls sowie Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. die Automatischen Sichtprüfung und Bildverarbeitung, die Mustererkennung und die semantische Umweltmodellierung.

PROF. DR. RER. POL. FRANK SCHULTMANN

ist Leiter des IIP, des Deutsch-Französischen Instituts für Umweltforschung sowie Inhaber des Lehrstuhls für Betriebswirtschaftslehre, insbesondere Produktionswirtschaft und Logistik und Mitarbeiter in KASTEL. Seine Forschungsschwerpunkte umfassen u. a. stoffstrombasiertes Produktionsmanagement, Konzeption und Optimierung industrieller Kreislauwirtschaftssysteme sowie die techno-ökonomische Bewertung nachhaltig orientierter Investitionen und Innovationen.

Building resilient cyber-physical power systems

An approach using vulnerability assessment and resilience management

Mariela Tapia, *Research Group Resilient Energy Systems, University of Bremen, Enrique-Schmidt-Str. 7, 28359 Bremen (mariela.tapia@uni-bremen.de)*
Pablo Thier, *Research Group Resilient Energy Systems, University of Bremen (thier@uni-bremen.de)*
Stefan Gößling-Reisemann, *Research Group Resilient Energy Systems, University of Bremen*

Power systems are undergoing a profound transformation towards cyber-physical systems. Disruptive changes due to energy system transition and the complexity of the interconnected systems expose the power system to new, unknown, and unpredictable risks. To identify the critical points, a vulnerability assessment was conducted, involving experts from the power as well as the information and communication technologies (ICT) sectors. Weaknesses were identified, e. g., the lack of policy enforcement, which are worsened by the unreadiness of the actors involved. Due to the complex dynamics of ICT, it is infeasible to keep a complete inventory of potential stressors to define appropriate preparation and prevention mechanisms. Therefore, we suggest applying a resilience management approach to increase the resilience of the system. It aims at better riding through failures rather than building higher walls. We conclude that building resilience in cyber-physical power systems is feasible and helps in preparing for the unexpected.

Die Gestaltung resilienter cyber-physischer Energiesysteme
Ein Ansatz basierend auf Vulnerabilitätsanalyse und Resilienzmanagement

Energiesysteme befinden sich in einem tiefgreifenden Wandel hin zu cyber-physischen Systemen. Disruptive Veränderungen, die von der Transformation des Energiesystems und der Komplexität der miteinander verbundenen Systeme herrühren, setzen das Stromnetz neuen, unbekannten Risiken aus. Mit einer Vulnerabilitätsanalyse unter Einbeziehung von Experten aus den Bereichen Energie und Informations- und Kommunikationstechnologien (IKT) wurden Schwachstellen identifiziert, z. B. Nachteile durch die fehlende Durchsetzung von Regulierungen, und eine mangelnde Anpassungsbereitschaft der beteiligten Akteure. Die komplexe IKT-Dynamik macht es unmöglich, potenzielle Stressoren vollständig zu erfassen, um geeignete Präventionsmechanismen zu definieren. Die vorgeschlagenen Resilienzmanagementmaßnahmen zielen darauf ab, Krisen besser zu bewältigen, anstatt auf höhere Barrieren zu setzen. Die Resilienz cyber-physikalischer Energiesysteme ist möglich.

https://doi.org/10.14512/tatup.29.1.23
Submitted: 23. 09. 2019. Peer reviewed. Accepted: 15. 01. 2020

Keywords: *cyber-physical power systems, resilience management, vulnerability assessment*

Introduction

Power systems are evolving through an extended convergence with information and communication technologies (ICT), leading to complex cyber-physical power systems (CPPS). This has brought opportunities to enhance the systems' performance and provide solutions to cope with the associated challenges of energy supply based on distributed and fluctuating renewable energies. However, cyber-attacks targeting power systems have been growing in number and sophistication in recent years. For instance, the attacks against the Ukrainian power grid in 2015 and 2016 that resulted in power outages (Dragos Inc. 2017). Another incident against a utility in the United States was reported on March 2019 (Sobzak 2019). Several risk and vulnerability assessments for power systems have been published in recent years (e. g. NIST 2014; Rossebo et al. 2017). In these studies, potential impacts and mitigation options were evaluated based on lists of potential threats and their likelihood of occurrence. We argue that due to the dynamic nature of ICT and its complex interdependency with the power infrastructure, we have to expect surprises. It will no longer be possible to identify a comprehensive inventory of potential threats, as is the case in classic risk management.

A reliable power supply is of great importance for almost all areas of life, therefore it is necessary to develop strategies that enable the power system to be prepared for expected and unexpected stressors. In other words, it is essential to apply a resilience management strategy. Many definitions of resilience exist in the scientific community (e. g. Jesse et al. 2019). For this study, we describe resilience as *a (socio-technical) system's ability to maintain its services under stress and in turbulent conditions* (Brand et al. 2017; Gleich et al. 2010). The advantage of using this definition is that it focusses on *the system services,* which must be outlined together with the stakeholders/us-

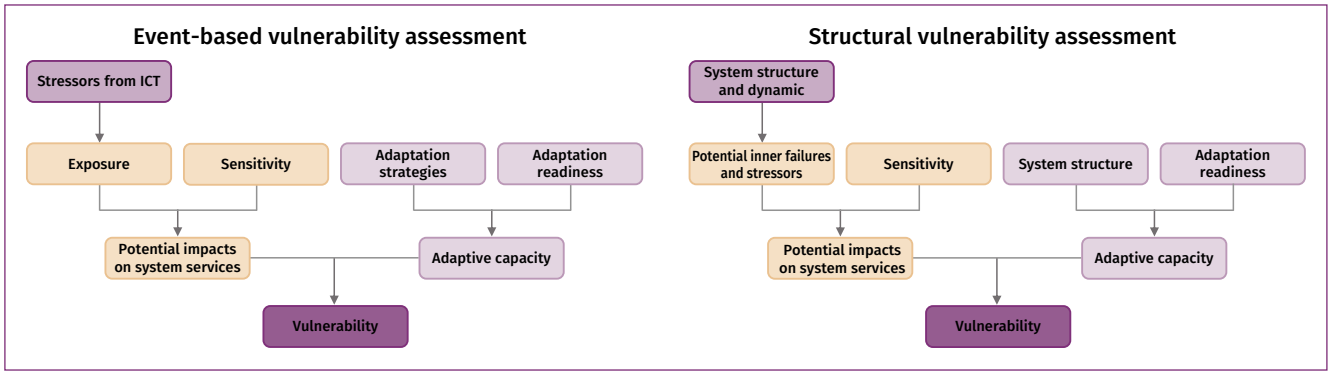


Fig. 1: Schematic representation of the VA methodology. **Left:** Event-based VA. **Right:** Structural VA.
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

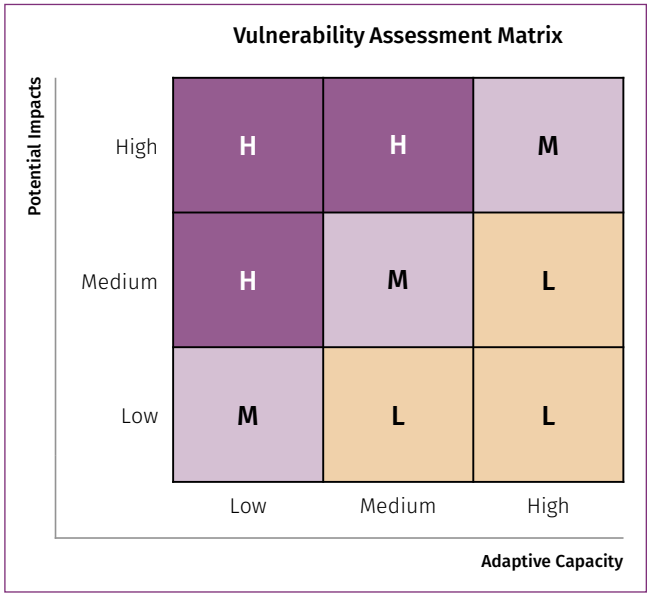


Fig. 2: Vulnerability assessment matrix that considers the level of potential impacts on system services and adaptive capacity. (**H**: High, **M**: Medium, **L**: Low).
Source: Authors' own compilation based on Gleich et al. (2010) and Gößling-Reisemann et al. (2013)

ers. In this way, changes and evolutions of the system are possible, which are core aspects of transitions. The focus lies on the complex nature of interconnectedness and interdependency, and the capability of the system to maintain its *services*.

This article presents the results of an empirical and interdisciplinary base study that involved actors from energy and ICT sectors through interviews and workshops, to get better insights into the vulnerabilities of CPPS. The study consists of two parts. First, a vulnerability assessment (VA) was performed to identify critical points coming from the ICT infrastructure. Second, a resilience strategy was developed by using a resilience management approach to identify how CPPS can be better prepared for any stressor.

Methodology

Vulnerability Assessment Approach

The event-based and structural VA methods (Fig. 1) carried out in Gleich et al. (2010) and Gößling-Reisemann et al. (2013) were used as reference for this study.

The potential impacts were evaluated based on their effect on the *system services,* which were defined in this case according to parameters for both the electric and ICT infrastructures. Regarding the electric infrastructure, the quantity criteria are determined by the system's ability to supply the connected load. The quality criteria are defined by direct technical parameters, such as power quality or reliability indices, and by indirect parameters, such as socio-economic and socioecological impacts. Regarding the ICT infrastructure, the approach considers the effect on the security requirements, i. e. confidentiality, integrity, availability and non-repudiation of data in transit or at rest (e. g. control commands, firmware, software, etc.).

The study focused on the German and European power system covering the complete electrical energy conversion chain and was limited to evaluate stressors from the ICT infrastructure. The component layer of the Smart Grid Architecture Model[1] was used as a reference architecture model. Two workshops and 19 semi-structured interviews were conducted with experts from the sectors: energy, industrial automation, ICT, and public bodies in the period between June 2016 to March 2017. The expert statements were evaluated by means of a comprehensive qualitative content analysis methodology based on Mayring (2014).

Combining the experts' opinions, relevant literature, and our own judgement, the potential impacts were qualitatively rated as high, medium or low according to the effects of stressors and structural weaknesses on the quality and quantity criteria of the system services. In order to determine the adaptive capacity, inputs from experts and literature were considered regarding existing or foreseen adaptation mechanisms and the readiness of the concerned actors to implement them. They were also qualita-

1 http://smartgridstandardsmap.com/

tively rated as high, medium or low. Consequently, the vulnerability level was the result of combining potential impacts and adaptive capacity according to the matrix showed in Fig. 2. A more detailed description on the VA methodology can be found in Tapia et al. (in press)

Resilience Management Approach

Resilient CPPS should have a diverse set of capabilities such as resistance/robustness, adaptation, innovation and improvisation to overcome known and unknown stressors. They help the systems to maintain their *system services* (see definition above). In this study, the resilience management approach described in Acatech et al. (2017) and Goessling-Reisemann and Thier (2019) was used as reference. It comprises a four-phase approach: (1) Prepare and prevent, (2) Implement robust and precautionary design, (3) Manage and recover from crises, and (4) Learn for the future. The suggested measures for each step were developed based on the VA results, the resilience design principles/elements described in Brand et al. (2017) and Goessling-Reisemann and Thier (2019), the statements of the interviewed experts, and our own judgments (Fig. 3).

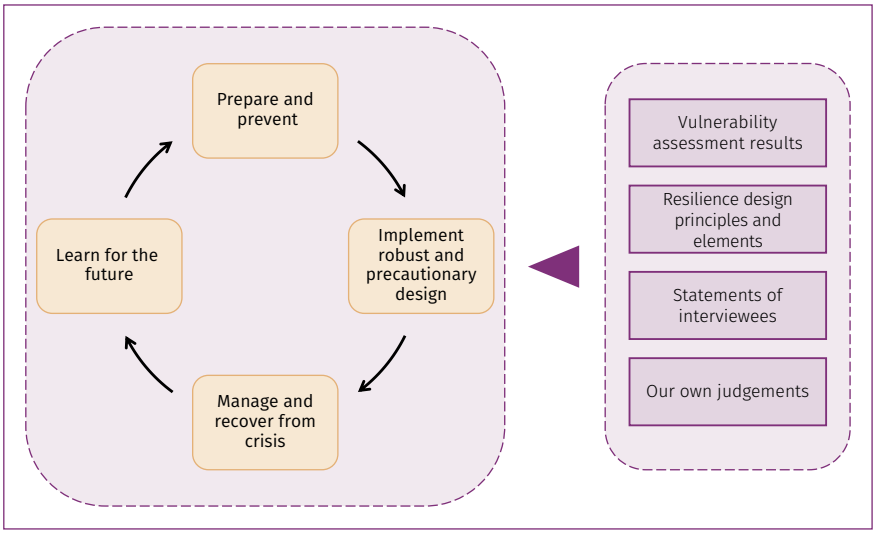


Fig. 3: Four phases of the resilient management approach scheme and the sources for determining the suggested measures for each phase. *Source: Authors' own compilation based on Acatech et al. (2017) and Goessling-Reisemann and Thier (2019)*

Vulnerability Assessment Results

The VA identified critical properties, structures and elements contributing to the vulnerability of the CPPS. Based on the qualitative content analysis results, the findings were sorted into the following four categories: (a) technology, (b) organizational security policies and procedures, (c) the human factor, and (d) regulations. Each category included subcategories and they were assessed individually using the VA methodology described above. All subcategories resulted in *high* vulnerability ratings following the combination of *medium to high* potential impacts with *medium or low* adaptive capacities (Tab. 1). The list of categories and subcategories is not intended to be comprehensive. However, it reflects the fact that the interviewees were queried about what the critical points are according to their opinion, which led to a list of high vulnerabilities. In the following section, the findings for each category will briefly be described.

Technology

The increased number of systems, endpoints and actors involved in the CPPS leads to a higher number of interconnections and communications. If these communications use unencrypted or

Category	Subcategory	Potential Impacts	Adaptive Capacity	Vulnerability
Technology	Insecure endpoints	M–H	M	**H**
	Insecure communications	M–H	M	**H**
Organizational security policies and procedures	Improper patch management	M–H	M	**H**
	Lack of interdisciplinary IT-OT knowledge	M–H	M	**H**
The human factor	Lack of security awareness in organizations	M–H	M	**H**
	Lack of security awareness among consumers	M–H	L	**H**
Regulations	Lack of effective implementation of standards and regulations	M–H	M	**H**
	Lack of coordinated effort to improve security	M–H	M	**H**

Tab. 1: Categories and subcategories that reflect critical properties, structures and elements of CPPS and the corresponding ratings of Potential Impacts, Adaptive Capacity and Vulnerability on the scale **L**: Low, **M**: Medium, **H**: High. *Source: Authors' own compilation based on Tapia et al. (in press)*

weakly encrypted network protocols, authentication keys and data payload are exposed (NIST 2014). Using Man-in-the-Middle attacks, threat agents will be able to listen, inject or manipulate messages between nodes. From one side, legacy communication protocols used in Industrial Control Systems (ICS) in the generation, transmission and distribution domains have evolved from proprietary point-to-point links and isolated from external networks to open and standard protocols. According to the experts, this represents a high security problem. The *'Crashoverride'* malware, which seems to have been used in the Ukraine blackout in 2016, is a good illustration of an advanced malware that leverages the weaknesses of certain ICS protocols (Dragos Inc. 2017).

From the other side, experts also stated that the more distributed and closer to the end-consumer the communication occurs, the more vulnerable it gets. The reason is that devices located at the customer premises (e. g. Internet-of-Things devices) are deployed with poor security features and furthermore, they are not regulated. In most of the cases, they do not have capabilities for secure key management, control access, or patch management. Security challenges and threats of smart home devices are discussed in Lee et al. (2014).

Organizational Security Policies and Procedures

Experts agreed that due to the increasing complexity and interdependencies between IT and Operation Technology (OT) infrastructures, the knowledge needed to address the new challenges has changed. In most of the cases, interdisciplinary knowledge is missing or limited, and therefore it is difficult to properly understand, design, implement and operate the complete complex system. Normally, OT assets are maintained by ICS operators and engineers rather than experienced IT professionals, which can result in common mistakes in maintenance, configuration, and lack of hardening (Bodungen et al. 2017). Moreover, typical IT systems security measures cannot be directly applied in ICS environments, because the process stability or availability could be affected. Therefore, specific and tailored security measures are needed.

As experts stated, ICS usually tend to be outdated, either because vendors do not provide security patches or because the particular system is time-critical. As a consequence, attackers are able to gain access to different system components by exploiting known security-gaps that have not yet been patched. Nevertheless, even if all patches and mitigations are kept up-to-date, attacks are becoming more sophisticated and adversaries use unknown zero-day exploits (McLaughlin et al. 2015), i. e. attacks based on previously unidentified and unpatched cyber-security gaps.

The Human Factor

The lack of effective security trainings and awareness programs in power sector organizations can lead to insufficiently trained or engaged personnel in cyber-security aspects (NIST 2014). Applying social engineering, threat agents are exploring new attack mechanisms targeting different levels in the organization. This is one of the fastest growing security problems according to the experts. In the Ukrainian blackout in 2015, attackers developed the *Blackenergy 3* tool malware and performed a phishing campaign targeting employees from the electricity distributor (Styzcynski and Beach-Westmoreland 2019).

Disgruntled employees, or ex-employees, who are not properly managed when leaving the company, may represent further potential threat actors. They could have detailed knowledge of the systems and access to critical data, allowing them to identify weak internal structures and methods to compromise the systems. Furthermore, critical information about the system configuration could be even publicly available through vendors' or asset owners' websites, employees' social media sites, or from other sources. Attackers can leverage this information for planning the attack.

Additionally, experts mentioned also that end users represent another vulnerable point because of their lack of awareness or understanding of the consequences of eventually low security of their smart devices. A more complex problem derives from end-users being prosumers, who may not have the expert-knowledge to implement and maintain appropriate security measures for Distributed Energy Resource (DER) systems (e. g. smart inverters).

Regulations

The lack of an effective implementation of security standards and regulations represents another critical point for CPPS. Experts considered that the absence of mandatory regulations to enforce power system operators to implement minimum required security standards, or vendors to provide the necessary security requirements in their products expose the system to possible cyber-attacks, for instance man-in-the-middle attacks on non-upgraded ICS systems running the IEC 60870-5 protocol (Maynard et al. 2014).

Different technical and organizational standards have been developed to address cyber-security requirements in smart grids (ENISA 2012; NIST 2014). Nevertheless, as experts stated, in most of the cases, these are only recommendations and the compliance to a minimum-security level is not enforced by regulations. Furthermore, the experts mentioned that there are no economic incentives for grid operators to invest in cyber-security enhancements. The decision to upgrade legacy ICS in order to implement the security measures could be delayed until the next planned lifecycle equipment replacement, not only because of the processes' criticality, but due to the additional associated costs. Another critical point, as experts remarked, is the missing effective coordination to improve security for the overall system.

The critical points discussed in this section are related to all categories mentioned above. The relationship is seen as lack of readiness of the involved actors to implement existing adaptation strategies. Thus, increasing the vulnerability level of each category itself.

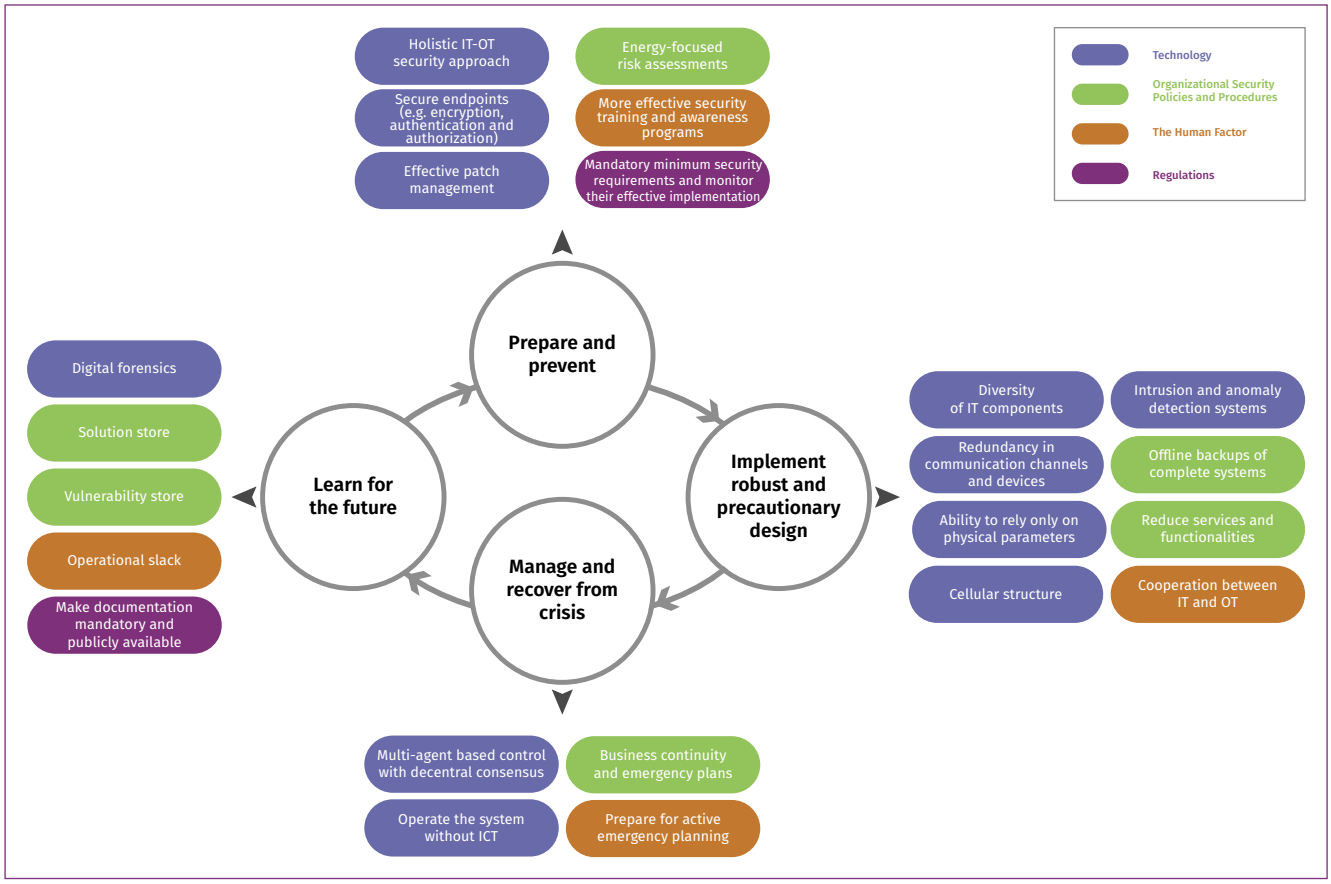


Fig. 4: Selection of resilience-enhancing measures and elements, sorted by the categories: Technology (blue), Organizational Security Policies and Procedures (green), the Human Factor (orange) and Regulations (grey), according to the Resilient Management approach phases.

Source: Authors' own compilation based on Tapia et al. (in press)

Resilience management strategy

The VA unveiled the critical vulnerable points. Security measures, if applied, have great potential to reduce some vulnerabilities. However, they focus mainly on trying to keep the malicious attackers outside of the system. Therefore, one of the biggest challenges is to find a way to broaden the horizon in handling known and unknown stressors by including recovering, adapting and learning mechanism after successful attacks, instead of only focusing on prevention and detection. This is the objective of the second part of the study. Our main concern is how to increase the resilience in CPPS. This requires the understanding that resilience is more than just eliminating identified vulnerabilities. The applied resilience management approach consists of four phases (Fig. 3).

During the **preparation and prevention** phase, weak points in the CPPS are identified and effective prevention measures must be derived. The focus here is on known stressors, thus a holistic security approach between IT-OT (IEC 2016), and energy-focused risk analysis and management strategies (Fischer et al. 2018) are needed. Experts also stressed the importance of scalable and regularly tested security measures at endpoints (e. g. encryption, authentication, authorization), intrusion detection systems, patch management, network segmentation, as well as more effective and engaging security trainings and awareness programs. Technology-wise, the implementation of additional measures for data storage and preserving of unused resources – operational slack – to better deal with surprises are helpful (Fischer and Lehnhoff 2018).

In order to enhance resilience, a **robust and precautionary system design should be implemented** from the beginning. This will empower the system to maintain its services even under stress or disturbances. The system should have a high diversity of IT components and redundancy in communication channels and devices (BNetzA 2019). Maintaining the ability to rely only on physical parameters for operation as well as hardware-based security are helpful. Furthermore, implementing a cellular structure in order to secure a minimum and stable power supply in case of a failing central ICT infrastructure appears beneficial (VDE 2015). Other suggestions supported by the experts are the implementation of real-time monitoring, intrusion and bad data detection schemes (Iturbe et al. 2016; McCarthy

et al. 2018), as well as periodic backups, and reducing services and functionalities in terms of data, ports, libraries, etc. (Fischer and Lehnhoff 2018).

A resilient power system is able to ride through failures in order to **manage and recover from crises.** While the stability and security in this phase could be enhanced by multi-agent based control with decentral consensus finding (Lehnhoff and Krause 2013), attention should also be paid to the ability to operate the system without ICT, i. e. manually, or to at least secure a *soft landing,* as experts stated. In addition, the provision of business continuity and emergency plans on a regional and local level, e. g. through *supplying islands* at least in and around public properties/buildings, and the preparation for active emergency planning and exercises based on realistic cyber-attacks have a high priority (Arghandeh et al. 2016).

Past and avoided disasters should be used in phase four **to learn for the future** in order to improve the adaptive capacity of the system. In this sense, digital forensic would allow to investigate incidents and near incidents in-depth and identify lessons. This should include the documentation of weaknesses that led to failures *(Vulnerability store)* (Gößling-Reisemann 2016). Furthermore, strengths that avoided crises in the past or enhanced recovery are equally worth identifying, as they form the basis for planning strategies and emergency scenarios *(Solution store)* (Gößling-Reisemann 2016). This documentation must be mandatory and publicly available.

Fig. 4 shows the summary of selected resilience-enhancing measures and elements for each phase of the resilience management approach. More details on the specific resilience management strategy described here can be found in Tapia et al. (in press).

Conclusions

In this study, critical properties, structures and elements contributing to the vulnerability of CPPS were identified. On one side, insecure communications or insecure end points, especially at the customer premises, resulted in a high vulnerability due to poor security features on the devices. On the other side, social engineering is a quickly growing security problem that enables threat agents to exploit one of the weaknesses present in every organization: the human factor. In spite of the existence of adaptation mechanisms that could minimize the impact, it was found that their implementation could be hindered by the lack of policy enforcement or the unreadiness of the involved actors to implement these measures. To address cybersecurity challenges, an integrated assessment considering physical, cyber and social perspectives is necessary. The aim is not only to try to keep attackers outside the system, but to design the system in a way that enables it to transform and adapt in order to cope with any kind of stressor. In other words, a resilience management strategy is needed that considers that resilience is more than just eliminating identified vulnerabilities. This article illustrated resilience enhancing measures assigned to the four phases of the resilience management cycle. One important measure is to establish an adequate cyber security regulation framework and monitor its effective implementation. Regarding the system architecture, a cellular structure and physical backup would build resilience in case of successful attacks. We conclude that introducing resilience principles/elements to the system and using a resilience management approach is a suitable way to prepare systems for the unexpected.

Acknowledgments

We acknowledge our beloved supervisor Prof. Dr. Stefan Gößling-Reisemann for his highly valuable insights and contributions during the research project Strom-Resilienz. We are very thankful to Prof. Dr. em. Arnim von Gleich for fruitful discussions and review of this manuscript, to Max Spengler for his support on the interview analysis, to Katja Hessenkämper, Katrina Stollmann and Cécile Pot d'or for proofreading.

Funding declaration

Project funded by the German Federal Ministry of Education and Research within the program Innovation and Technology Analysis, FKZ 16I1678.
http://www.stromresilienz.de

References

Acatech; Deutsche Akademie der Naturforscher Leopoldina e. V.; Akademienunion; Union der deutschen Akademien der Wissenschaften e. V. (2017): Das Energiesystem resilient gestalten. Maßnahmen für eine gesicherte Versorgung. Berlin: Acatech, Leopoldina, Akademienunion.

Arghandeh, Reza; Meier, Alexandra von; Mehrmanesh, Laura; Mili, Lamine (2016): On the definition of cyber-physical resilience in power systems. In: Renewable and Sustainable Energy Reviews 58, pp. 1060–1069.

BNetzA – Bundesnetzagentur (2019): Aktualisierung Sicherheitsanforderungen. Available online at https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html, last accessed on 20. 12. 2019.

Bodungen, Clint; Singer, Bryan; Hilt, Stephen; Shbeeb, Aaron; Wilhoit, Kyle (2017): Hacking exposed industrial control systems. ICS and SCADA security secrets and solutions. New York: McGraw-Hill Education.

Brand, Urte et al. (2017): Resiliente Gestaltung des Energiesystems am Beispiel der Transformationsoptionen „EE-Methan-System" und „Regionale Selbstversorgung". Schlussbericht des vom BMBF geförderten Projektes RESYSTRA. Bremen: Universität Bremen. DOI: 10.2314/KXP:1667649884.

Dragos Inc. (2017): Crashoverride. Analyzing the threat to electric grid operations. Available online at https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, last accessed on 21. 01. 2020.

ENISA – The European Network and Information Security Agency (2012): Smart grid security. Security related standards, guidelines and regulatory documents. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/smart-grid-security-related-standards-guidelines-and-regulatory-documents/view, last accessed on 21. 01. 2020.

Fischer, Lars; Lehnhoff, Sebastian (2018): IT-Security for functional resilience in energy systems. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.):

Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 316–340.

Fischer, Lars; Uslar, Mathias; Morrill, Doug; Döring, Michael; Haesen, Edwin (2018): Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector. Final Report. Available online at https://ec.europa.eu/energy/sites/ener/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf, last accessed on 21. 01. 2020.

Gleich, Arnim von; Gößling-Reisemann, Stefan; Stührmann, Sönke; Woizeschke, Peer; Lutz-Kunisch, Birgitt (2010): Resilienz als Leitkonzept. Vulnerabilität als analytische Kategorie. In: Klaus Fichter, Arnim von Gleich, Reinhard Pfriem and Bernd Siebenhüner (eds.): Theoretische Grundlagen für erfolgreiche Klimaanpassungsstrategien. Delmenhorst: Projektkonsortium ‚nordwest2050', pp. 13–49.

Goessling-Reisemann, Stefan; Thier, Pablo (2019): On the difference between risk management and resilience management for critical infrastructures. In: Matthias Ruth and Stefan Goessling-Reisemann (eds.): Handbook on resilience of socio-technical systems. Croydon: Edward Elgar Publishing Limited, pp. 117–135.

Gößling-Reisemann, Stefan (2016): Resilience. Preparing energy systems for the unexpected. In: Igor Link and Valentine Florin (eds.): IRGC Resource Guide on Resilience. Lausanne: EPFL International Risk Governance Center.

Gößling-Reisemann, Stefan; Wachsmuth, Jakob; Stührmann, Sönke; Gleich, Arnim von (2013): Climate change and structural vulnerability of a metropolitan energy system. The case of Bremen-Oldenburg in Northwest Germany. In: Journal of Industrial Ecology 17 (6), pp. 846–858.

IEC – International Electrotechnical Commission (2016): Power systems management and associated information exchange. Data and communications security. Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems. 1.0. Geneva: IEC.

Iturbe, Mikel; Camacho, Jose; Garitano, Iñaki; Zurutuza, Urko; Uribeetxeberria, Roberto (2016): On the feasibility of distinguishing between process disturbances and intrusions in process control systems using multivariate statistical process control. In: Proceedings of the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, pp. 155–160.

Jesse, Bernhard-Johannes; Heinrichs, Heidi; Kuckshinrichs, Wilhelm (2019): Adapting the theory of resilience to energy systems. A review and outlook. In: Energy, Sustainability and Society 9 (1), p. 27. DOI: 10.1186/s13705-019-0210-7.

Lee, Changmin; Zappaterra, Luca; Choi, Kwanghee; Choi, Hyeong-Ah (2014): Securing smart home. Technologies, security challenges, and security requirements. Proceedings of the 2014 IEEE Conference on Communications and Network Security. San Francisco: IEEE, pp. 67–72. DOI: 10.1109/CNS.2014.6997467.

Lehnhoff, Sebastian; Krause, Olav (2013): Agentenbasierte Verteilnetzautomatisierung. In: Peter Göhner (ed.): Agentensysteme in der Automatisierungstechnik. Berlin: Xpert.press Springer-Verlag, pp. 207–223.

Maynard, Peter; Mclaughlin, Kieran; Haberler, Berthold (2014): Towards understanding man-in-the-middle attacks on IEC 60870-5-104 SCADA Networks. Proceedings of the 2nd International Symposium for ICS & SCADA Cyber Security Research, pp. 30–42. Swindon, U. K.: BCS Learning & Development.

Mayring, Philipp (2014): Qualitative content analysis. Theoretical foundation, basic procedures and software solution. Available online at https://nbn-resolving.org/urn:nbn:de:0168-ssoar-395173, last accessed on 21. 01. 2020.

McCarthy, James et al. (2018): Securing manufacturing industrial control systems. Behavioral anomaly detection. NISTIR 8219. Gaithersburg: National Institute of Standards and Technology. Available online at https://www.nccoe.nist.gov/sites/default/files/library/mf-ics-nistir-8219.pdf, last accessed on 21. 01. 2020.

McLaughlin, Kieran; Friedberg, Ivo; Kang, BooJoong; Maynard, Peter; Sezer, Sakir; McWilliams, Gavin (2015): Secure communications in smart grid. Networking and protocols. In: Smart Grid Security Book 2015, pp. 113–148.

NIST – National Institute of Standards and Technology Interagency (2014): Guidelines for smart grid cybersecurity. Vol. 1: Smart Grid cybersecurity strategy, architecture, and high-level requirements. Report 7628 Rev. 1. Gaithersburg: National Institute of Standards and Technology. DOI: 10.6028/NIST.IR.7628r1.

Rossebo, Judith; Wolthuis, Reinder; Fransen, Frank; Bjorkman, Gunnar; Medeiros, Nuno (2017): An enhanced risk-assessment methodology for smart grids. In: Computer 50 (4), pp. 62–71.

Sobczak, Blake (2019): Experts assess damage after first cyberattack on U. S. grid. Security. In: E & E News. Available online at https://www.eenews.net/stories/1060281821, last accessed on 21. 01. 2020.

Styzcynski, Jake; Beach-Westmoreland, Nate (2019): When the lights went out. A comprehensive review of the 2015 attacks on Ukrainian critical infrastructure. n. p.: Booze Allen Hamilton Inc. Available online at https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf, last accessed on 21. 01. 2020.

Tapia, Mariela; Thier, Pablo; Gößling-Reisemann, Stefan (in press): artec Paper No. 222: Vulnerability and resilience of cyber-physical power system. Results from an empirical-based study.

VDE – Verband der Elektrotechnik Elektronik und Informationstechnik (2015): Der Zellulare Ansatz. Grundlage einer erfolgreichen, regionenübergreifenden Energiewende. Frankfurt a. M.: VDE ETG.

MARIELA TAPIA

holds a M. Sc. in Renewable Energy. Since 2016, she is working as research associate in the research group *Resilient Energy Systems* at the University of Bremen. Her research focus is resilient transformation of power supply in developing countries.

PABLO THIER

has a background in experimental physics. Since 2015, he has been working in different projects at the University of Bremen in the research group *Resilient Energy Systems,* where he is developing a framework for making resilient decisions for energy systems.

PROF. DR. RER. NAT. STEFAN GÖßLING-REISEMANN (1968–2018)

was a theoretical physicist. He was the chair of the research group *Resilience Energy System* and the speaker of the *Advanced Energy Systems Institute* at the University of Bremen. His research aimed at solving the substantial problems of this planet. His last projects aimed at designing resilient and sustainable energy systems.

Sichere IT ohne Schwachstellen und Hintertüren

Arnd Weber, *Hexentalstr. 31, 79283 Bollschweil (arnd.weber@alumni.kit.edu)*
Gernot Heiser, *UNSW Sydney (gernot@unsw.edu.au)*
Dirk Kuhlmann, *Fraunhofer-Institut für System- und Innovationsforschung (dirk.kuhlmann@alumni.tu-berlin.de)*
Martin Schallbruch, *Digital Society Institute, European School of Management and Technology (ESMT) (martin.schallbruch@esmt.org)*
Anupam Chattopadhyay, *Nanyang Technical University (anupam@ntu.edu.sg)*
Sylvain Guilley, *Télécom ParisTech (sylvain.guilley@telecom-paristech.fr)*
Michael Kasper, *Fraunhofer Singapore (michael.kasper@fraunhofer.sg)*
Christoph Krauß, *Fraunhofer-Institut für sichere Informationstechnologie (christoph.krauss@sit.fraunhofer.de)*
Philipp S. Krüger, *Digital Hub Cybersecurity (philipp.krueger@alumni.digitalhub-cybersecurity.com)*
Steffen Reith, *Hochschule RheinMain (Steffen.Reith@hs-rm.de)*
Jean-Pierre Seifert, *Technische Universität Berlin (jpseifert@sect.tu-berlin.de)*

Unsere zunehmende Abhängigkeit von Informationstechnik erhöht kontinuierlich die Safety- und Security-Anforderungen bei deren Einsatz. Ein zentrales Problem hierbei sind Schwachstellen von Hard- und Software. Marktkräfte konnten diese Situation bislang nicht grundsätzlich beheben. Eine Gegenstrategie sollte deshalb folgende Optionen erwägen: (1) private und staatliche Förderung offener und sicherer IT-Produktion, (2) Verbesserung der souveränen Kontrolle bei der Produktion aller kritischen IT-Komponenten innerhalb eines Wirtschaftsraumes sowie (3) verbesserte und durchgesetzte Regulierung. Dieser Beitrag analysiert Vor- und Nachteile dieser Optionen. Es wird vorgeschlagen, die Sicherheit der Schlüsselkomponenten einer Lieferkette durch weltweit verteilte, offene und ggf. mathematisch bewiesene Komponenten zu gewährleisten. Der beschriebene Ansatz erlaubt die Nutzung existierender und neuer proprietärer Komponenten.

Secure IT without vulnerabilities and back doors

Increasing dependence on information technology calls for strengthening the requirements on their safety and security. Vulnerabilities that result from flaws in hardware and software are a core problem which market mechanisms have failed to eliminate. A strategy for resolving this issue should consider the following options: (1) private- and public-sector funding for open and secure production, (2) strengthening the sovereign control over the production of critical IT components within an economic zone, and (3) improving and enforcing regulation. This paper analyses the strengths and weaknesses of these options and proposes a globally distributed, secure supply chain based on open and mathematically proved components. The approach supports the integration of legacy and new proprietary components.

https://doi.org/10.14512/tatup.29.1.30
Submitted: 22. 09. 2019. Peer reviewed. Accepted: 08. 01. 2020

Keywords: *cybersecurity, sovereignty, open source, verification, supply chain risks*

Probleme

Die Abhängigkeit der Industriegesellschaft von Informationstechnik führt zu hohen Anforderungen an den sicheren Betrieb dieser Technik – sowohl im Sinne der funktionellen Verlässlichkeit *(Safety)* als auch der IT-Sicherheit im Sinne von Vertrauenswürdigkeit, Integrität, Verfügbarkeit (*confidentiality*, *integrity*, *availability*, CIA). Beide Anforderungen können, insbesondere in Kombination, durch derzeit produzierte IT-Systeme nur bedingt sichergestellt werden. Infolgedessen können Infrastrukturen ausfallen, Betriebsgeheimnisse entwendet, Autos ferngesteuert, Vermögensschäden verursacht und politische Institutionen ausgespäht werden (Weber et al. 2018 a, 2018 b).

Wesentliche Ursache für die Angriffsmöglichkeiten sind vielfältige Schwächen in Hard- und Software. Sie beginnen bei einfachen Fehlern in der Anwendungssoftware wie etwa dem *Heartbleed-Bug* innerhalb einer Komponente, die zur Verschlüsselung im World Wide Web genutzt wurde. Sie setzen sich fort in Angriffen wie durch die Erpressersoftware *WannaCry*, die den Geheimdiensten bekannte, aber nicht beseitigte Schwächen in Betriebssystemen ausnutzte. Neueren Datums sind Hardware-Trojaner (Becker et al. 2014), deren Existenz in elektronischen Halbleiterbauelementen, z. B. FPGA-Chips, und militärischen Radaranlagen in Syrien bereits behauptet wurde. Von zunehmender Bedeutung ist auch die Möglichkeit von Angriffen auf IT-Lieferketten (Huang 2019).

Eine substanzielle Verbesserung der Situation im Bereich IT-Sicherheit konnte in den letzten Jahren nicht erreicht werden, wie die Statistik der *Computer Vulnerabilities and Expo-*

sures zeigt (MITRE 2019). Spätestens seit den Snowden-Veröffentlichungen im Jahr 2013 muss davon ausgegangen werden, dass nationale Nachrichtendienste Schwachstellen gezielt herstellen oder ankaufen (Abb. 1). Offenkundig betrifft dies nicht nur die Dienste der USA: Auch Russland ist stark im *Cyberspace* aktiv, gleiches gilt für China. Offiziere der chinesischen Volksbefreiungsarmee haben bereits vor zwei Jahrzehnten die Herstellung „logischer Bomben" für Computernetzwerke vorgeschlagen (Liang und Wang 1999). Die aus strategischer Motivation geheim gehaltenen Hintertüren können unter Umständen von Kriminellen ausgenutzt werden, wie das Beispiel *WannaCry* belegt.

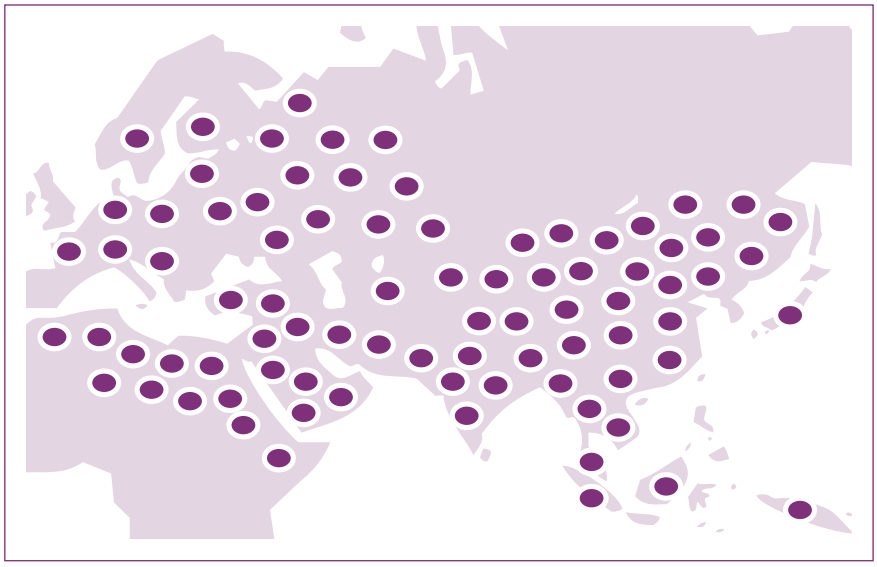


Abb. 1: Von der US-amerikanischen National Security Agency (NSA) kompromittierte Computer. Jeder Punkt repräsentiert > 500 Geräte. Der Whistleblower Edward Snowden veröffentlichte, dass z. B. Maschinen von HP, Dell und Cisco unterminiert und die Firmen Belgacom und Gemalto gehackt wurden.
Quelle: Angepasster Ausschnitt aus Snowden 2013

Nahezu täglich werden neue Schwachstellen entdeckt, die von Fehlern in der Programmierung bis zu ausnutzbaren Seiteneffekten spekulativer Programmausführung in der Hardware reichen (*Spectre* und *Meltdown*). Inzwischen muss selbst die Möglichkeit einer aktiven Einschleusung von Schwachstellen durch die verwendeten Entwicklungswerkzeuge in Erwägung gezogen werden. Die meisten Komponenten für Computer, einschließlich Softwaremodule und Chips, werden inzwischen in einer komplexen weltweiten Arbeitsteilung erstellt. Dabei sind viele Details der Implementierungen selbst für große industrielle Kunden intransparent. Dies gilt für integrierte komplexe Softwaremodule ebenso wie für einzelne Hardwarekomponenten. Daraus ergeben sich vielfältige Angriffsmöglichkeiten (Weber et al. 2018 a).

Zertifizierungen haben bislang lediglich begrenzte Aussagekraft für die IT-Sicherheit.

Angesichts der Abhängigkeit von digitalen Systemen und den Auseinandersetzungen im Cyberraum erscheint es unzureichend, das Risiko von schwerwiegenden Sicherheitsverletzungen ausschließlich mit Methoden des Risikomanagements und inkrementellen Updates anzugehen (Odlyzko 2019). In Ergänzung hierzu ist es erforderlich, einen grundlegenden Wandel in die Wege zu leiten, der informationstechnische Sicherheit mittels ökonomisch vertretbarer Verfahren fundamental verbessert und zwar unter Berücksichtigung der weltweit steigenden Konzentration von Kompetenzen und Wertschöpfung (Müller-Quade et al. 2017).

Entwicklungsoptionen

Die grundsätzliche Vermeidung von Schwachstellen in Hardware und Software wird im Allgemeinen als nahezu unlösbares Problem angesehen. So wird geltend gemacht, Soft- und Hardware seien zu kompliziert, verifizierte Lösungen teuer und unflexibel und hundertprozentige Sicherheit ohnehin nicht erreichbar. Obwohl aus empirischer und historischer Sicht einiges für diese Einschätzungen spricht, bleibt es Aufgabe der Forschung, die Prämissen dieser Argumente zu ermitteln, sie infrage zu stellen und nach realisierbaren Ansätzen zu suchen.

Herkömmliche Ansätze wie umfangreicheres Testen und *Patching* haben sich bisher als nicht ausreichend erwiesen (Weber et al. 2018 a). So helfen gegen mögliche Systemschwächen und durch finanzstarke Akteure gesponserte Angriffe graduelle Verbesserungen, wie Updates oder neue Systemschichten, bestenfalls graduell. Auch zusätzliche eingeführte Kontrollkomponenten bieten nur begrenzte Möglichkeiten, weil sie ihrerseits für Angriffe ausgenutzt oder umgangen werden können und zudem selbst mit unterminierten Werkzeugen entwickelt worden sein könnten.

Auf europäischer Ebene wird derzeit diskutiert, ob IT-Sicherheit durch Regulierung der Hard- und Software verbessert werden kann, etwa indem Zertifizierungen nach den *Common Criteria* oder dem *EU Cybersecurity Act* von 2019 vorgeschrieben werden. Derartige Zertifizierungen haben bislang lediglich begrenzte Aussagekraft, zumal bestehende Verfahren die Korrektheit der Implementierung meist nur mit Tests prüfen. Selbst wenn alle zertifizierten Software-Komponenten bewiesenermaßen sicher wären, besteht die Frage nach möglichen Hard-

ware-Schwächen fort, etwa wenn das Design oder der Produktionsprozess geändert wird. Überprüfungen werden z. B. dort kompliziert, wo Hardware-Hersteller Teile des Designs geheim halten, um Angriffe zu erschweren oder sie durch Prozessfestlegungen dazu verpflichtet sind. Hierdurch wird die Sicherheit tendenziell reduziert, da diese Komponenten nicht unabhängig nachprüfbar sind (Saltzer und Schroeder 1975; Eurosmart 2014). Ein Kunde kann ein solches Produkt nicht selbst beurteilen. Hinzu kommt, dass die Durchführung der anspruchsvolleren Zertifizierungsstufen sehr kostenintensiv ist.

Ehrgeiziger sind Versuche, die Kontrolle der IT Produktion auf nationaler Ebene sicherzustellen und kritische Systeme ausschließlich im Inland zu produzieren. So verfügt z. B. China über Durchgriffsmöglichkeiten, mit denen im Prinzip die gesamte Wertschöpfungskette kontrolliert werden kann. Vollständige Autonomie ist bei IT-Systemen allerdings schwer zu erreichen, sobald Hersteller für den Weltmarkt produzieren und Komponenten anderer Anbieter beziehen, deren Designfehler oder absichtlich eingefügte Hintertüren jedes IT-System beeinflussen können, in das sie verbaut sind.

Eine Herausforderung für die Forschung besteht darin, Verfahren zu entwickeln, die komplexere Systeme kostengünstig verifizieren können.

Option offene, verifizierte Lieferketten

Der im Folgenden vorgestellte Ansatz kombiniert offene Produktion, verifizierte Hard- und Software und sichere Lieferketten. Wir schlagen vor, offene Produktionsverfahren über die gesamte Lieferkette einzuführen, die Inputs und Werkzeuge ebenso wie die Produkte selbst umfasst. Hierzu ist zunächst die Schlüsselfrage zu beantworten: Wie können Schwächen und Hintertüren tatsächlich eliminiert werden? Danach ist zu fragen, wie der Ansatz zu finanzieren und mit der privatwirtschaftlichen Amortisation von Entwicklungsaufwänden für neue Produkte vereinbaren wäre.

Offenheit

Aus Sicherheitsperspektive haben offene Systeme einige grundsätzliche Vorteile gegenüber vertraulichen Systemen. So konstatiert das US Department of Defence im Rahmen einer Ausschreibung für Projekte zur Cybersicherheit: „Current commodity computer hardware and software are proprietary. A thorough security review cannot be performed on systems with undisclosed components." (SBIR 2018) Beispiele für offene Systeme sind das Betriebssystem Linux und das davon abgeleitete Android, die sich erfolgreich am Markt etabliert haben. Eine ähnliche Entwicklung könnte sich im Hardware-Bereich hinsichtlich des RISC-V Prozessor-Designs anbahnen. Diese offene Prozessorarchitektur, die an der Universität Berkeley unter Förderung durch die Defense Advanced Research Projects Agency (DARPA) und in Kooperation mit der Industrie entwickelt wurde, ermöglicht freie Inspektion und lizenzkostenfreie Weiterentwicklung.

Open source ist per se nicht mit Fehlerfreiheit gleichzusetzen. Dies belegt z. B. der bereits angesprochene *Heartbleed-Bug,* der auf einem jahrelang unentdeckten Implementierungsfehler beruhte. Hier sind Verbesserungen bei der Kontrolle von Spezifikationen und Designs etwa durch Intensivierung automatischer statischer und dynamischer Analyse von Programmen und Testen durch unabhängig arbeitende Gruppen denkbar (Kiss et al. 2015). Durch diesen Mehraufwand könnte die Sicherheit von Open-Source-Komponenten erheblich verbessert werden, doch intensiveres Testen allein kann nie ausschließen, dass unentdeckte Fehler verbleiben.

Formale Verifikation

Gegen unentdeckte Schwächen können offene Systeme Abhilfe schaffen, deren korrektes Funktionieren in Bezug auf Vertraulichkeit und Integrität der verarbeiteten Nutzerdaten mathematisch bewiesen ist („formal verifiziert"). Ein Vorreiter bei der praktischen Realisierung solcher Systeme ist *seL4,* ein Mitglied der L4-Familie von Betriebssystem-Mikrokernen (Klein et al. 2014, vgl. Abb. 2).

Ausgelöst vom Gleitkomma-Divisions-Fehler in Intel-Prozessoren im Jahr 1994 wird seit Jahrzehnten eine formale Verifikation von Teilen der CPU-Designs durchgeführt. Entsprechende Bestrebungen existieren zur Überprüfung kompletter RISC-V Prozessoren (Chlipala 2017). Die zugrundeliegenden formalen Spezifikationen und Beweise sind jedoch aufwändig und verlieren i. d. R. ihre Gültigkeit, sobald am verifizierten Objekt auch nur geringfügige Änderungen vorgenommen werden.

Eine Herausforderung für die Forschung besteht deshalb darin, Verfahren zu entwickeln, die komplexere Systeme kostengünstig verifizieren können. Die Schwierigkeiten für Korrektheitsbeweise komplexer Prozessoren steigen mit der Anzahl der Transistoren, Prozessorkerne, etc. jedoch stark an. Bislang ist unklar, ob man angesichts der wachsenden Integrationsdichte und Transistoranzahl der neuesten Prozessorgenerationen deren Design je zu vertretbaren Kosten beweisen können wird oder ob der Beweisaufwand durch grundsätzliche Änderungen des CPU- und Rechnerdesigns radikal gesenkt werden kann.

Abb. 2: Diese Entwicklungen zeigen beispielhaft, dass die neuen Ansätze in der Forschung, in Prototypen und in Produkten angewendet werden. *(V. l. n. r.:)* [1] Apples A11-Chip mit Secure Element, in dem der L4 Betriebssystemkern verwendet wird; [2] Unbemannter Boeing Hubschrauber kontrolliert durch das offene, bewiesene seL4; [3] Sicherheitsmodul mit dem offenen LEON-SPARC-v8-Prozessor; [4] Prototyp eines offenen Sicherheitsmoduls mit dem offenen VexRiscv Prozessor, mit einem Hardwarebeschleuniger für die ChaCha Stromverschlüsselung, ausschließlich mit offenen Entwurfswerkzeugen erstellt (auf einem FPGA-Chip laufend). *Quellen: [1] Wikipedia (2020); [2] Data61 (2020); [3] Sylvain Guilley, Secure-IC; [4] Steffen Reith*

Sicherung der Lieferkette

Die Lieferkette für IT kann an nahezu jedem Punkt erfolgreich angegriffen werden – Modifikation des Designs und Beeinflussung des Produktionsprozesses sind ebenso möglich wie die Subversion von Test- und Validierungsverfahren oder Austausch von Systemelementen während der Auslieferung. Es ist damit zu rechnen, dass die Sicherung einiger Komponenten, wie etwa Betriebssysteme oder Prozessoren, dazu führt, dass andere Komponenten angegriffen werden, z. B. Kommunikationschips oder verwendete Softwarewerkzeuge. Ein umfassender Ansatz hätte demzufolge möglichst große Teile dieser Kette zu sichern. Dort, wo auf geschlossene, nicht verifizierte Anwendungen, z. B. traditionelle Betriebssysteme, zurückgegriffen werden muss, sollten diese durch Mechanismen gekapselt werden, die sie vom vertrauenswürdigen Teil des Systems trennen.

Eine zentrale Herausforderung betrifft die Sicherung der Produktion der Halbleiter in den *Fabs* genannten Produktionsanlagen. Diese erfordern Milliardeninvestitionen und sind, neben den USA und Israel, auf wenige fernöstliche Länder konzentriert. Eine Strategie zur besseren Absicherung der Chip-Produktion kann sich unter anderem folgender Optionen bedienen:

- Lokale Fertigung durch als vertrauenswürdig betrachtete Betreiber und Mitarbeiter (*Trusted Fab*), eventuell auf eine Reihe kritischer Schritte am Schluss der Fertigung beschränkt (Sengupta et al. 2019).
- Kontrolle der Chips durch mathematische Verfahren, wie Verschlüsselung (Šišejković et al. 2019) oder zusätzliche Leiterbahnen (Seifert und Bayer 2015).
- Stichprobenartige Inspektion von Chips durch optische Prüfung. Aus praktischer Sicht funktioniert dies am besten bei einfachen Chips mit vergleichsweise großen Strukturen, deren Herstellung für Enthusiasten aus dem Open-Source-Umfeld machbar ist, wie durch das *Libre Silicon*-Projekt angestrebt (Libre Silicon 2020).

Die genannten Optionen müssen teils erst noch entwickelt und erprobt werden. Gleiches gilt für Ansätze zur Absicherung von Softwarewerkzeugen, die in der Herstellung von Hard- oder Software verwendet werden. Die drei zu untersuchenden Hauptoptionen sind hier:

- entweder ein offenes System von Werkzeugen zu schaffen und durch intensive Überprüfung die Gefahr von Schwachstellen oder Hintertüren zu minimieren
- oder den Output eines offenen Werkzeugs formal zu verifizieren
- oder den Output mit jenen proprietärer Werkzeuge auf funktionale Äquivalenz zu vergleichen.

Natürlich muss in allen Fällen die Integrität der Prüfumgebung sichergestellt werden, was evtl. nur langfristig geschehen kann. Der Vollständigkeit halber sei noch darauf hingewiesen, dass die Mathematik dabei helfen kann, die Authentizität von Chips sicherzustellen, z. B. durch Verwendung von *physically unclonable functions,* die physikalische Implementierungscharakteristika nutzen (Bruneau et al. 2019).

Kosten

Ein wichtiger Faktor für die Realisierung eines offenen Ansatzes ist die Finanzierbarkeit. Derzeit kommen die vorgeschlagenen formalen Verfahren aus Aufwandsgründen zumeist nicht in Betracht. Die Open-Source-Community beispielsweise setzt derzeit selten Instrumente zur formalen Spezifikation oder Verifikation ein. Einerseits wird dies als zu aufwändig angesehen, andererseits schränkt eine formal orientierte Vorgehensweise die Flexibilität bei der Weiterentwicklung erheblich ein. Es besteht also Forschungs- und Handlungsbedarf, um formale Beweise leichter und kostengünstiger durchführen zu können.

Die Stückkosten für formal verifizierte, offene Komponenten könnten verringert werden, wenn man höhere Losgrößen erreicht, die Entwicklungskosten global auf die Forschungsetats mehrerer Länder und Unternehmen verteilt, dem Beispiel der Kooperation von US-Firmen mit der DARPA folgend, und geringere Lizenzkosten als für proprietäre Tools einbezieht. Durch formal verifizierte Systeme entstehen zudem niedrigere Kosten für Sicherheitsmaßnahmen und für Schadensbehebung. Zudem könnten solche Komponenten wegen der hohen Qualität einen

Vorteil im Wettbewerb darstellen und regulatorischen Anforderungen leichter gerecht werden. Eine belastbare Schätzung der Kosten ist wegen der Vielzahl von Variablen derzeit schwer möglich.

Stand des Übergangs zu offenen, bewiesenen Systemen

Eine strategische Initiative für offene, formal bewiesene Komponenten und Systeme könnte auf einer Reihe von Vorarbeiten aufbauen, die seit längerem u. a. von der DARPA gefördert werden. Angesichts der wachsenden Abhängigkeit der US-amerikanischen IT-Wirtschaft von internationalen IT-Zulieferern folgerte die Agentur bereits 2017: „The Open-Source community needs to develop a complete infrastructure" (Salmon 2017, S. 9). Inzwischen hat auch die Industrie in den USA, Asien und Europa begonnen, sich intensiver mit dieser Thematik auseinanderzusetzen und bspw. hochleistungsfähige Multicore-CPUs auf RISC-V Basis zu entwickeln oder auf Softwareseite auf das verifizierte Mikrokernel-Betriebssystem seL4 zurückzugreifen (Sauter 2019; Hettinga 2019; hartpunkt.de 2018).

Durch diese Initiativen werden bereits heute öffentliche und private Gelder in Beweis-basierte, offene Architekturen investiert, die etwa im Bereich von Grafikkarten, Speichermedien oder eingebetteten Systemen zur Anwendung kommen sollen. Wie im Falle von Linux/Android in der Vergangenheit bereits beobachtbar, kann eine solche Entwicklung bewirken, dass sich der Einsatz derartiger Systeme von ihren ursprünglichen Einsatzfeldern (hochsichere Anwendungen, wie Luftfahrt, Verteidigung und IT-Sicherheitsmodule) auf andere Geräteklassen ausweitet.

Fazit zur globalen Implementierung offener Verifizierung

Im Sinne eines *constructive technology assessment* lassen sich Risiken für den deutschen, europäischen und letztlich globalen Raum nur dann substanziell verringern, wenn Mechanismen entwickelt werden, die die Anzahl von Schwachstellen, Fehlern und Hintertüren nachweislich reduzieren, idealerweise auf null: *Secure IT* statt *IT security*. Eine beträchtliche Zahl technischer Grundlagen für die Entwicklung offener, verifizierter Systeme ist bereits gelegt. Um diesen Ansatz jedoch systematisch auszubauen, bedarf es erheblicher Investitionsmittel. Nötig wären hier forschungs- und industriepolitische Programme zur Frage, wie komplette Wertschöpfungsketten von IT-Systemen offen und sicher gestaltet und verbreitet werden können. In den USA hat die DARPA hierzu einen Investitions- und Forschungsplan entwickelt (*Electronic Resurgence Initiative)*, der die lokale, sichere Produktion von IT-Komponenten zum Ziel hat. Dieser ist jedoch stark auf den militärischen Bereich fokussiert und bezieht US-Hersteller mit vertraulichen Produkten und Prozessen ein. Für den zivilen Bereich, gerade auch außerhalb der USA, sind folgende Programmelemente vonnöten:

1. Initiierung von Pilotprojekten und Prototypen, die die gesamte Wertschöpfungskette umfassen,
2. Weiterentwicklung und *Tooling* von Methoden der formalen Verifikation mit dem Ziel leichterer Anwendbarkeit sowie Ausweitung der Forschung zur formalen Analyse auf komplexere Systeme,
3. Techniken zur redundanten formalen Verifizierung durch geografisch verteilte, unabhängig arbeitende Teams, insbesondere zur Aufgabenverteilung und Zusammenführung der Ergebnisse,
4. Untersuchung von Techniken zur Zertifizierung, die nicht auf der Vertraulichkeit der Produktion und der Verifizierungstechniken beruhen,
5. Training einer ausreichenden Anzahl von fachlich qualifiziertem Personal sowie
6. Entwicklung und Erprobung von Methoden zur Kontrolle geografisch entfernter *Fabs* und weltweiter Lieferwege.

Parallel hierzu müssten Geschäftsmodelle mit dem Ziel erarbeitet werden, die anfänglichen Kosten möglichst global zu verteilen. Ähnlich der Förderung von RISC-V wäre hier eine Kostenteilung zwischen privaten und öffentlichen Trägern naheliegend. Preiswerte, verifizierte Werkzeuge und Komponenten könnten Innovationen in vielen Branchen erleichtern und für viele Länder die „Souveränität" im IT-Bereich stärken.

Ferner sollte untersucht werden, ob und wie eine derartige Zielstellung effizient durch politische oder durch regulatorische Maßnahmen flankiert werden sollte. Die Koordination des beschriebenen Vorhabens könnte dabei in Deutschland z. B. durch zwei in neuerer Zeit gegründete Regierungsinstitutionen gefördert werden: die Agentur für Innovation in der Cybersicherheit und die Agentur zur Förderung von Sprunginnovationen.

Das Ziel „Secure IT" statt „IT security" lässt sich nur erreichen, wenn die Anzahl von Schwachstellen, Fehlern und Hintertüren idealerweise auf null reduziert wird.

Der vorgeschlagene Ansatz hat die Absicherung der gesamten Produktions- und Lieferkette zum Ziel und erfordert deshalb abgestimmte Anstrengungen über eine Vielzahl von Arbeitsgebieten. Die Komplexität eines solchen Vorhabens dürfte jener der derzeitigen Pilot-Initiativen zur Etablierung europäischer *Cyber Competence Networks* nicht nachstehen. Deren Finanzierungsrahmen liegt zwischen 10 und 20 Millionen Euro und ein entsprechender Aufwand sollte auch für die Entwicklung eines technischen und organisatorischen Rahmens veranschlagt

werden. Echte Produktentwicklung für den zivilen Bereich würden allerdings deutlich höhere Aufwendungen erfordern (die DARPA hat hierfür derzeit für fünf Jahre ca. US-$ 1,5 Mrd. eingeplant). Die Umsetzung würde ein umfangreiches Public-Private-Partnership-Programm mit vielen Akteuren oder auch den Aufbau eines nationalen oder europäischen „Champions" unter Mobilisierung von Risikokapital erfordern, ggf. in Kooperation mit Akteuren aus anderen Ländern.

Aus politischer und ökonomischer Perspektive sollten parallele und alternative Entwicklungen auf globaler Ebene beobachtet und deren Ansätze und Risiken weiter analysiert werden. Hierzu gehören etwa Versuche, Lieferketten auf rein nationaler Ebene zu etablieren (USA, China, Indien) oder die Entwicklung und der Einsatz offener, aber bislang unbewiesener Hardware-Komponenten durch etablierte IT-Unternehmen.

Danksagung

Die Autoren danken G. Müller-Datz und A. Saffari für die Begutachtung sowie Vertretern US-amerikanischer und deutscher Unternehmen für Anregungen.

Literatur

Becker, Georg; Regazzoni, Francesco; Paar, Christof; Burleson, Wayne (2014): Stealthy dopant-level hardware Trojans. Extended version. In: Journal of Cryptographic Engineering 1 (4), S. 19–31.

Bruneau, Nicolas et al. (2019): Development of the unified security requirements of PUFs during the standardization process. In: Jean-Louis Lanet und Cristian Toma (Hg.): Innovative Security Solutions for Information Technology and Communications. Cham: Springer, S. 314–330.

Chlipala, Adam (2017): Coming soon. Machine-checked mathematical proofs in everyday software and hardware development. Chaos Communication Congress. Leipzig, Deutschland, 27.–30. 12. 2017. Online verfügbar unter https://events.ccc.de/congress/2017/Fahrplan/events/9105.html, zuletzt geprüft am 06. 11. 2019.

Data61 (2020): The HACMS project @ Data61. Online verfügbar unter https://ts.data61.csiro.au/projects/TS/SMACCM/, zuletzt geprüft am 08. 01. 2020.

Eurosmart – European Smart Card Association (2014): Security IC platform protection profile with augmentation packages. Version 1.0. Online verfügbar unter https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf, zuletzt geprüft am 06. 11. 2019.

hartpunkt.de (2018): Hensoldt kooperiert mit CSIROs Data61. Online verfügbar unter https://www.hartpunkt.de/hensoldt-kooperiert-mit-csiros-data61/, zuletzt geprüft am 08. 01. 2020

Hettinga, Wisse (2019): Sixteen core RISC-V processor Xuan Tie 910. Alibaba. In: EENewsEurope, 25. 07. 2019. Online verfügbar unter https://www.eenewseurope.com/news/sixteen-core-risc-v-processor-xuan-tie-910-alibaba, zuletzt geprüft am 06. 11. 2019.

Huang, Andrew (2019): Supply chain security. „If I were a Nation State". BlueHat IL 2019. Israel, Tel Aviv, 06.–07. 02. 2019. Online verfügbar unter https://www.youtube.com/watch?v=RqQhWitJ1As&list=UUp892CjX6wps88JivisRMtA&index=6&t=0s, zuletzt geprüft am 21. 01. 2020.

Kiss, Balázs; Kosmatov, Nikolai; Pariente, Dillon; Puccetti, Armand (2015): Combining static and dynamic analyses for vulnerability detection. Illustration on Heartbleed. In: Nir, Piterman (Hg.): Hardware and software. Verification and testing. Cham: Springer, S. 39–50.

Klein, Gerwin et al. (2014): Comprehensive formal verification of an OS microkernel. In: ACM Transactions on Computer Systems 32 (1), S. 2:1–2:70.

Liang, Qiao; Wang, Xiangsui (1999): Unrestricted warfare. Beijing: PLA Literature and Arts Publishing House. Online verfügbar unter https://www.oodaloop.com/documents/unrestricted.pdf, zuletzt geprüft am 06. 11. 2019.

Libre Silicon (2020): Libre Silicon. Free semiconductors for everyone. Online verfügbar unter https://libresilicon.com/, zuletzt geprüft am 08. 01. 2020.

MITRE (2019): CVE Details. Online verfügbar unter https://www.cvedetails.com/browse-by-date.php, zuletzt geprüft am 06. 11. 2019.

Müller-Quade, Jörn; Reussner, Ralf; Beyerer, Jürgen (2017): Karlsruher Thesen zur Digitalen Souveränität Europas. Online verfügbar unter https://www.fzi.de/fileadmin/user_upload/PDF/2017-10-30_KA-Thesen-Digitale-Souveraenitaet-Europas_Web.pdf, zuletzt geprüft am 21. 01. 2020.

Odlyzko, Andrew (2019): Cybersecurity is not very important. In: Ubiquity, Issue June, S. 1–23. DOI: 10.1145/3333611.

Salmon, Linton (2017): A perspective on the role of open-source IP in government electronic systems. 7th RISC-V Workshop. Milpitas, USA, 28.–30. 11. 2017. Online verfügbar unter https://content.riscv.org/wp-content/uploads/2017/12/Wed-1042-RISCV-Open-Source-LintonSalmon.pdf, zuletzt geprüft am 21. 01. 2020.

Saltzer, Jerome; Schroeder, Michael (1975): The protection of information in computer systems. In: Proceedings of the IEEE 63 (19), S. 1278–1308.

Sauter, Marc (2019): Wieso RISC-V sich durchsetzen wird. In: golem.de, 17. 10. 2019. Online verfügbar unter https://www.golem.de/news/offene-prozessor-isa-wieso-risc-v-sich-durchsetzen-wird-1910-141978.html, zuletzt geprüft am 21. 01. 2020

SBIR – The Small Business Innovation Research Program (2018): Open source high assurance system. Online verfügbar unter https://www.sbir.gov/sbirsearch/detail/1508741, zuletzt geprüft am 06. 11. 2019.

Seifert, Jean-Pierre; Bayer, Christoph (2015): Trojan-resilient circuits. In: Al-Sakib Pathan (Hg.): Securing cyber-physical systems. Boca Raton: CRC Press, S. 349–370.

Sengupta, Abhrajit; Nabeel, Mohammed; Knechtel, Johann; Sinanoglu, Ozgur (2019): A new paradigm in split manufacturing. Lock the FEOL, unlock at the BEOL. In: Proceedings der Design, Automation & Test in Europe Conference & Exhibition 2019.

Šišejković, Dominik; Merchant, Farhad; Leupers, Rainer; Ascheid, Gerd; Kegreiss, Sascha (2019): Control-lock. Securing processor cores against software-controlled hardware Trojans. In: Proceedings des ACM Great Lakes Symposium on VLSI, S. 27–32.

Snowden, Edward (2013): Worldwide SIGINT. Online verfügbar unter https://edwardsnowden.com/wp-content/uploads/2013/11/nsa1024.jpg, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 a): Sovereignty in information technology. Security, safety and fair market access by openness and control of the supply chain. Karlsruhe: KIT-ITAS. Online verfügbar unter http://www.itas.kit.edu/pub/v/2018/weua18a.pdf, zuletzt geprüft am 21. 01. 2020.

Weber, Arnd; Reith, Steffen; Kasper, Michael; Kuhlmann, Dirk; Seifert, Jean-Pierre; Krauß, Christoph (2018 b): Open source value chains for addressing security issues efficiently. In: Proceedings der IEEE International Conference on Software Quality, Reliability and Security Companion 2018, S. 599–606.

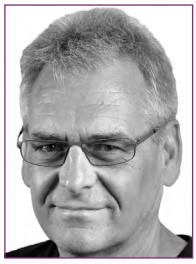
Wikipedia (2020): Apple A11 Bionic. Online verfügbar unter https://de.wikipedia.org/wiki/Apple_A11_Bionic, zuletzt geprüft am 21. 01. 2020.

PROF. DR.-ING. ANUPAM CHATTOPADHYAY

lehrt am SCSE, Nanyang Technical University, Singapur. An der RWTH Aachen arbeitete er an Chiparchitekturen, an EDA sowie an der Automatisierung der Spezifikation von Chips (RTL).

PROF. DR.-ING. SYLVAIN GUILLEY

ist CTO von Secure-IC, Frankreich, sowie Professor an Télécom-ParisTech, Mitarbeiter der École Normale Supérieure (ENS), Außerordentlicher Professor an der Chinesischen Akademie der Wissenschaften sowie Herausgeber von Standards wie ISO/IEC 20897 (Physically Unclonable Functions).



PROF. DR. GERNOT HEISER

ist leitender Forscher bei CSIRO's Data61 und Scientia Professor an UNSW Sydney (John Lions Chair of Operating Systems). Er war Gründer der Open Kernel Labs, deren L4 Kern u. a. in der Secure Enclave aller iOS-Geräte läuft. Er ist Chief Scientist (Software) bei HENSOLDT Cyber und Fellow der ACM, der IEEE und der australischen Akademie der Technischen Wissenschaften.

MICHAEL KASPER

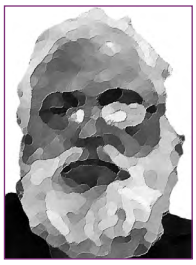
leitet die Arbeitsgruppe „Cyber- und Information Security" bei Fraunhofer Singapore und Mitbegründer von opentrust.ai in Singapur. Er ist assoziierter Senior Researcher beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

PROF. DR. CHRISTOPH KRAUSS

leitet am Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt, die Abteilung Cyber-Physical Systems Security und ist verantwortlich für das Geschäftsfeld Automotive Security. Weiterhin ist er Professor für das Fachgebiet Netzwerksicherheit an der Hochschule Darmstadt.

PHILIPP S. KRÜGER

ist Managing Director von Accenture Security für Deutschland, Schweiz, Österreich und Russland. Er ist Mitbegründer der Digital Hub Cybersecurity, war Berater des Verteidigungsministeriums für Cyberspace und Innovation und ist Leiter der Agile Cyber Deterrence Group des Instituts für Sicherheitspolitik an der Universität Kiel.



DIRK KUHLMANN

ist Senior Researcher am Fraunhofer-Institut für System- und Innovationsforschung (ISI), Karlsruhe. Von 1995 bis 2017 arbeitete er für die Hewlett Packard Laboratories in Bristol in der Forschungsgruppe für IT-Sicherheit mit Schwerpunkt Open-Source-Software.

PROF. DR. STEFFEN REITH

ist Professor für Theoretische Informatik an der Hochschule RheinMain in Wiesbaden. Während seiner Tätigkeit bei Elektrobit Automotive hat er Produkte mit kryptografischen Funktionen für den Serieneinsatz in aktuellen Automobilen entwickelt.

MARTIN SCHALLBRUCH

ist stellvertretender Direktor des Digital Society Institute (DSI) und Senior Researcher an der European School of Management and Technology (ESMT) in Berlin. Gleichzeitig ist er Lehrbeauftragter am Karlsruher Institut für Technologie. Im Bundesinnenministerium war er zuletzt Leiter der Abteilung für Informationstechnik, Digitale Gesellschaft und Cybersicherheit.

PROF. DR. JEAN-PIERRE SEIFERT

ist Einstein Professor für das Fachgebiet „Security in Telecommunications" an der TU Berlin und den Telekom Innovation Laboratories. Er hat u. a. bei Infineon, Intel und Samsung geforscht.

DR. ARND WEBER

ist Volkswirt und Soziologe. Bis zu seiner Pensionierung war er Senior Researcher beim Institut für Technikfolgenabschätzung und Systemanalyse des KIT und hat die EU und die Bundesregierung beraten. Er hat u. a. an der Goethe-Universität Frankfurt und bei NTT Yokosuka geforscht.

Siedlungswasserwirtschaft im Zeitalter der Digitalisierung

Cybersicherheit als Achillesferse

Martin Zimmermann, *Institut für sozial-ökologische Forschung GmbH (ISOE), Hamburger Allee 45, 60486 Frankfurt am Main (zimmermann@isoe.de)*
Engelbert Schramm, *Institut für sozial-ökologische Forschung GmbH (ISOE) (schramm@isoe.de)*
Björn Ebert, *Institut für sozial-ökologische Forschung GmbH (ISOE) (ebert@isoe.de)*

Die Digitalisierung in der Siedlungswasserwirtschaft kann dazu beitragen, die Aufgaben, die sich für Wasserversorgung und Abwasserbeseitigung aufgrund des demografischen und klimatischen Wandels ergeben, besser anzugehen. Gleichzeitig können sich durch Cyberangriffe die Risiken für einen Ausfall dieser Kritischen Infrastrukturen vergrößern. Aspekte der Cybersicherheit werden im Wassersektor jedoch noch nicht hinreichend berücksichtigt. Entsprechende Regularien und Maßnahmen zielen alleine auf die Ausfallsicherheit der Infrastrukturen ab und vernachlässigen dabei die Versorgungssicherheit der Bevölkerung. Die Aufmerksamkeit der Politik auf große Wasserunternehmen und Versorgungsgebiete ignoriert Sicherheitslücken bei kleinen und mittleren Betrieben. Kooperationen zwischen mehreren Wasserunternehmen könnten ein geeignetes Mittel sein, diesbezüglich Synergieeffekte zu erzeugen.

Urban water management in the age of digitalization
Cybersecurity as an Achilles' heel

Digitalization in urban water management can help to better address the challenges for water supply and sanitation due to demographic and climate change. At the same time, cyberattacks can increase the risks for a failure of these critical infrastructures. However, aspects of cybersecurity are not yet sufficiently addressed in the water sector. Corresponding regulations and measures solely aim at the reliability of the infrastructures and neglect the security of supply for the population. Policy attention to large water utilities and supply areas ignores security gaps in small and medium-sized enterprises. Cooperations between several water utilities could be a suitable means of generating synergy effects in this respect.

https://doi.org/10.14512/tatup.29.1.37
Submitted: 26. 09. 2019. Peer reviewed. Accepted: 08. 01. 2020

Keywords: *critical infrastructure, cybersecurity, vulnerability, water infrastructure*

Einleitung

Zu den Funktionen der Siedlungswasserwirtschaft gehören neben dem Hochwasserschutz die öffentliche Trinkwasserversorgung sowie die Abwasserbeseitigung aus Siedlungen. Da deren grundlegende Wasserinfrastrukturen für gesellschaftliche und wirtschaftliche Prozesse unerlässlich sind (u. a. Wahrung der Versorgungssicherheit), können sie entsprechend der EU-Richtlinie 2008/114/EG als Kritische Infrastrukturen eingestuft werden, deren Schutz eine zentrale öffentliche Aufgabe darstellt.

In Deutschland werden 99 % der Bevölkerung über eine öffentliche Wasserversorgung mit Trinkwasser versorgt (Statistisches Bundesamt 2019 b): Insgesamt 4.400 Wasserversorgungsunternehmen befinden sich zumeist in unterschiedlichen Rechts- und Organisationsformen in kommunalem Eigentum. Nur 63 Unternehmen davon lieferten 2016 mehr als 10 Millionen m³ Wasser, davon einige auch ausschließlich als Lieferfirmen (z. B. die Bodenseewasserversorgung, die bis nach Tauber-Franken aktiv ist). Die meisten Unternehmen haben aber eigene Brunnen und operieren direkt in ihren Verteilgebieten, die viel kleiner sind und häufig an der Gemeindegrenze enden. Ähnlich ist die Situation auf der Ablaufseite, wo 97 % der Bevölkerung an die öffentliche Kanalisation mit 9.000 Kläranlagen angeschlossen sind (Statistisches Bundesamt 2019 a). Nur 276 Anlagen waren 2016 so groß, dass sie in mehreren Klärstufen mindestens 6 Millionen m³ Abwasser bearbeiteten, bevor ihr Ablauf in die Gewässer eingeleitet wurde. Beim Abwasser hängen Rechts- und Organisationsformen der Unternehmen sowohl mit der Kapazi-

tät der Kläranlage als auch der Größe und Siedlungsstruktur des Einzugsgebiets zusammen (Pointl et al. 2019).

Die Siedlungswasserwirtschaft steht derzeit vor einer Reihe von Herausforderungen, die sich u. a. aus dem demografischen Wandel und dem Klimawandel ergeben. Die Digitalisierung, beispielsweise in Form von flexibleren Mess-, Steuerungs- und Regelungssystemen (MSR), bietet dabei zum einen die Chance, durch intelligente Betriebsweisen auf außergewöhnliche Ereignisse (z. B. Extremwetterereignisse, kriminelle Gefahren, Stromausfälle) angemessener und schneller reagieren zu können. Zum anderen können Digitalisierungsprozesse durch die so erhöhte Komplexität der Infrastrukturen aber auch die Risiken für menschliches und technisches Versagen oder Sabotage (z. B. Hackerangriff, Terrorismus) vergrößern. Die Konsequenzen sind noch weitreichender, wenn die Abhängigkeiten der Wasserwirtschaft von der Energieversorgung oder Infrastrukturen der Informations- und Kommunikationstechnik (IKT) einbezogen werden. Momentan weist die deutsche Siedlungswasserwirtschaft im Vergleich zu anderen Branchen noch ein moderates Tempo bei der digitalen Transformation auf, u. a. aufgrund hoher Investitionskosten (z. B. Smart Grids und Smart Meters), fehlender Standards, fehlenden Fachpersonals oder Problemen bei Datenschutz und -sicherheit (Graumann 2017).

Digitalisierung innerhalb des Wasserversorgungssystems bringt hohe Anforderungen an IT-Sicherheits- und Datenschutzmaßnahmen für Erzeuger und Verbraucher mit sich.

Derzeit wird in Deutschland eine Novellierung des IT-Sicherheitsgesetzes geplant, mit dem die bestehenden Vorschriften dieses Gesetzes verschärft werden sollen. Im vorliegenden Artikel soll die Frage beantwortet werden, welche Gefährdungen sich für die Siedlungswasserwirtschaft unter Cybersicherheitsaspekten ergeben, ob die diesbezüglichen Regularien und Maßnahmen ausreichend sind und welche Schlussfolgerungen daraus gezogen werden müssen.

Gesetzliche Regelungen zur Cybersicherheit in der Siedlungswasserwirtschaft

Aus den USA wurden vor 2015 vereinzelt Cyberangriffe auf Wasserwerke bekannt. Nach Vorbild der USA (Clark et al. 2017) verabschiedete der Bundestag am 25. Juli 2015 ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme – das IT-Sicherheitsgesetz. Zentralakteur dabei wurde das 1991 gegründete Bundesamt für Sicherheit in der Informationstechnik (BSI); als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen und Nationale Cybersicherheitsbehörde erhielt es zusätzliche Kompetenzen. Unternehmen, die große Kritische Wasserinfrastrukturen betreiben, wurden verpflichtet, eigene IT-Sicherheitsbeauftragte zu benennen, die die Cybersicherheit verantworten.

In der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz für die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung (2016) und der ersten Verordnung zur Änderung der BSI-Kritisverordnung vom 21. Juni 2017 wurden Definitionen getroffen, die die Vorschriften der EU-Richtlinie 2008/114/EG umsetzten, die Einstufung von Anlagen als Kritische Infrastruktur festlegten und den betroffenen Unternehmen Kriterien (sog. „Schwellenwerte“) zur Bewertung ihrer Anlagen zur Verfügung stellten: Anlagen der Trinkwasserversorgung gehören bei mehr als 22 Mio. m³ jährlich verarbeiteter Wassermenge zur Schutzbedarfskategorie „hoch“. Sind 500.000 Einwohner an eine Anlage der Abwasserbeseitigung angeschlossen, so gehört diese in die entsprechende Schutzbedarfskategorie. Sie müssen branchenspezifische Mindeststandards erfüllen, insbesondere die Einführung eines Information Security Management Systems (ISMS), und relevante Vorfälle, die IT-Sicherheit betreffen, an das Bundesamt melden.

Der Schwerpunkt der Debatte hinsichtlich Cyberangriffen liegt in der Wasserwirtschaft derzeit auf den Operativen Technologien (OT) in den industriellen Netzen der Unternehmen, also der Prozessleit- und Automatisierungstechnik (Pointl et al. 2019; Lachance 2016). Die für administrative und organisatorische Aufgaben vorgesehenen Büro-Netze bzw. Informationstechnologien (IT) der Unternehmen werden nur insoweit berücksichtigt, als von ihnen auch Gefährdungen ausgehen können (Fluchs 2017).

Digitalisierung in der Siedlungswasserwirtschaft

In den vergangenen Jahren (2016–2019) haben sich Fachverbände der Wasserwirtschaft in Deutschland zunehmend mit der Frage der Digitalisierung wasserwirtschaftlicher Verfahrensprozesse und Systeme beschäftigt. Dabei wurden bisherige Praxisanwendung, Geschäfts- und gesellschaftliche Nutzen sowie potenzielle Chancen und Herausforderungen von Digitalisierung erörtert. In Anlehnung an „Industrie 4.0“ beschreiben in diesem Kontext Begriffe wie „Wasser 4.0“ (Schaffer et al. 2019) oder „Wasserwirtschaft 4.0“ (Pohl et al. 2017) Systeman-

sätze zur Transformation der Wasserwirtschaft hin zu vernetzten, automatisierten und zukunftsfähigen Systemen mit stärkerer Kundenorientierung und besserer Vernetzung innerhalb der Wertschöpfungskette. Dafür wird ein ganzheitlicher Ansatz aus intelligenten Versorgungsnetzen, sogenannten Smart Grids, gemeinsam mit *Internet of Things and Services* (IoT) zur Bereitstellung und Analyse von Daten sowie *Cyber-Physical-Systems* (CPS) für erforderlich gehalten (Schaffer et al. 2019, S. 6). CPS sind komplexe internetbasierte Datenkommunikationssysteme, die virtuelle und reale Wassersysteme vernetzen und damit Echtzeit-Monitoring sowie Vorhersagemodelle von Produktions-, Frühwarn- und Entscheidungsprozessen in Planung, Bau und Betrieb ermöglichen, was Risiken reduzieren und Kosten vermindern hilft (Schaffer et al. 2019, S. 6). Derartige Systeme sollen Ressourceneffizienz, Flexibilität und Wettbewerbsfähigkeit in der Wasserwirtschaft generieren, wobei der Verbraucherschutz im Vordergrund steht (Schaffer et al. 2019, S. 10; Pohl et al. 2017). Dabei werden eine qualitative Ressourcen- und Prozessoptimierung sowie die Chance auf ein verbessertes Daten- und Schnittstellenmanagement erwartet (Ammermüller und Fälsch 2017). Eine durch die Digitalisierung erbrachte Visualisierung kann ebenfalls zur Erhöhung des Systemverständnisses beitragen und Datenverfügbarkeit optimieren (Schaffer et al. 2019, S. 10). Trotz einer steigenden Bereitschaft zu digitalisieren, zeigt die deutsche Wasserwirtschaft bislang ein moderates Digitalisierungstempo. Sie erzielt einen weit unterdurchschnittlichen Wert ihres Umsatzes mit digitalisierten Produkten und 16 % der Betriebe verfügen über keinerlei digitalisierte Angebote (Graumann 2017).

Digitalisierung innerhalb des Wasserversorgungssystems bringt hohe Anforderungen an IT-Sicherheits- und Datenschutzmaßnahmen für Erzeuger und Verbraucher mit sich (Ammermüller und Fälsch 2017). Besonders CPS bergen durch die direkte Vernetzung virtueller und realer Wasserversorgungssysteme eine mögliche Angriffsstelle in der Cybersicherheit; dennoch setzt bspw. Siemens in Zukunftsprojekten der Abwasser-Steuertechnik auf Gesamtlösungen wie *Totally Integrated Automation* (TIA), bei der die gesamte Antriebs- und Steuerungstechnik von derselben Plattform gesteuert werden (Schaffer et al. 2019, S. 20). Eine Veränderung des Geschäftsmodells hin zu digitalisierten Systemen führt zu Herausforderungen im Personalwesen: Neue Qualifikationen erzeugen einen Mangel an internem Fachpersonal, deren Weiterbildung während des Geschäftsbetriebs zeitaufwändig ist. Der Einfluss branchenfremder qualifizierter Akteure („Disruptoren") hat wiederum Auswirkungen auf das etablierte Geschäftsmodell (Ammermüller und Fälsch 2017; Barjenbruch et al. 2016). Insgesamt erfordert die Digitalisierung einen hohen Investitionsbedarf und Zeitaufwand (Graumann 2017). Da Entscheidungen über Digitalisierungsprozesse meist zentral auf der strategischen Leitungsebene verortet sind, geschieht die Umsetzung in einem „Tone from the Top" (Schaffer et al. 2019, S. 10), was jedoch häufig den Bedürfnissen der einzelnen operativen Organisationseinheiten nicht entspricht. Beim Gesamtblick auf die Aspekte, die in der Siedlungswasserwirtschaft im Zusammenhang mit der Digitalisierung diskutiert werden, kann der Schluss gezogen werden, dass Probleme der Cybersicherheit vergleichsweise unterbelichtet bleiben.

Vulnerable Systembestandteile und Gefährdungen

Vulnerable Systembestandteile der Siedlungswasserwirtschaft

Zu den Operative-Technology-Systemen (OT-Systeme), also (geschlossene bzw. gekapselte Systeme), gehört die Mess-, Steuerungs- und Regelungstechnik (MSR) zur Überwachung und Steuerung technischer Prozesse mittels Computer-Systemen wie SCADA (Supervisory Control and Data Acquisition). In dieser Hinsicht unterscheiden sich die Bereiche der Wasserversorgung und Abwasserbeseitigung nicht grundsätzlich. OT-Systeme kommen hier z. B. zur Steuerung von Ventilen, Schiebern, Pumpen und Aufbereitungsprozessen sowie zur Regelung und Überwachung von Prozesswerten wie z. B. Druck und Durchfluss zum Einsatz. Manuelle Regulation ersetzend werden sie so zu einer entscheidenden Komponente der Wasserinfrastruktur. Dabei müssen die Systeme zur Echtzeitverarbeitung in der Lage sein und mit hoher Zuverlässigkeit und Verfügbarkeit arbeiten. OT-Systeme nutz(t)en im Unterschied zur IT daher oft andere, proprietäre Kommunikationsprotokolle und Standards. Außerdem trugen die Abgeschlossenheit von OT-Systemen und deren damit verbundene Unfähigkeit, PC-basierte Malware auszuführen, maßgeblich zu deren Sicherheit bei. Dadurch, dass die Erreichung funktionaler Ziele im Vordergrund stand, wurden OT-Komponenten oft ohne Berücksichtigung grundlegender IT-Sicherheitsanforderungen konzipiert und eingerichtet.

In jüngster Zeit werden jedoch auch IT-Standard-Netzwerkprotokolle in OT-Systemen eingesetzt, um die Kompatibilität zwischen OT und IT zu erhöhen. Zudem soll die Verknüpfung von IT, OT und Kommunikationsinfrastruktur den Betreibern von Wasserversorgungs- und Abwasserbeseitigungsanlagen die Fernsteuerung und Fernüberwachung ihrer Prozesse ermöglichen. Dies ist jedoch mutmaßlich mit einer Verringerung der Sicherheit von OT-Systemen und der damit gesteuerten und überwachten siedlungswasserwirtschaftlichen Infrastrukturen verbunden, siehe z. B. das Schadprogramm Stuxnet (Gaycken 2010). OT-Systemen kommt damit eine entscheidende Bedeutung für die Verwundbarkeit der Kritischen Infrastruktur Siedlungswasserwirtschaft zu. Informationstechnische Angriffe oder Manipulationsversuche werden mit hoher Wahrscheinlichkeit auf ebendiese Systeme ausgerichtet sein und können zu vorübergehenden Funktionsstörungen einzelner Komponenten bis hin zum Totalausfall der Wasserver- oder -entsorgung führen. Gezielte Attacken setzen jedoch ein hinreichendes Wissen über die Systeme voraus und sind mit einem vergleichsweise hohen Ressourcenaufwand (u. a. Zeit, Personen) verbunden, wobei sich durchaus die Frage stellt, ob der Zweck des Angriffs nicht auch mit anderen Mitteln zu erreichen ist (z. B. durch

unmittelbare Manipulation von Prozessen oder Beschädigung von Geräten).

Zu den vulnerablen Bestandteilen der Wasserversorgung gehören grob die Bereiche Wassergewinnung, Wasseraufbereitung und Wasserverteilung, zu denen der Abwasserbeseitigung die Bereiche Entwässerung, Abwasser- und Klärschlammbehandlung sowie Wasserausleitung (BSI 2014; Zimmermann und Schramm 2019). In allen Bereichen sind IKT-basierte Manipulationsversuche grundsätzlich möglich, wobei in Konsequenz unterschiedliche Schutzgüter (Gesellschaft, Natur) in verschiedenen räumlichen und zeitlichen Ausmaßen gefährdet sein können. Naheliegend wäre zunächst der Fall, dass die Rohwassergewinnung aus Grundwasser, Seen oder Talsperren (seltener direkt aus Fließgewässern) kompromittiert wird, was entsprechende Folgen für die Aufbereitung (z. B. Trockenfallen von Filtern) und Verteilung hätte. Denkbar wäre im umgekehrten Fall aber auch eine unkontrollierte Übernutzung von Grundwasser mit unerwünschten hydrogeologischen Konsequenzen (z. B. Salzwasserintrusionen aus anderen Grundwasserstockwerken). In Fällen, in denen die Ressourcenbasis über eine künstliche Grundwasseranreicherung gesteuert wird, können durch einen unerwünschten Eingriff u. U. Schadstoffe in das Grundwasser gelangen, wodurch sich auch die Gefahr der Erpressbarkeit ergeben kann.

In Bezug auf die Wasseraufbereitung im Wasserwerk sind prinzipiell sämtliche Aufbereitungsprozesse (z. B. Belüftung, Filtration, Enteisenung, Entmanganung, Desinfektion) durch Cyberattacken angreifbar, wodurch abhängig von der Wasserspeicherung die Versorgungssicherheit mengenmäßig oder qualitativ betroffen sein kann. Im Bereich der Wasserverteilung können abgesehen vom Ausfall von Pumpen zur Erhaltung des Versorgungsdrucks auch Smart Grids gestört werden, insbesondere mit Blick auf Aspekte der Netzsteuerung, des Demand Managements oder des Datenschutzes. Smart Grids sind derzeit in der Siedlungswasserwirtschaft noch nicht weit verbreitet. In Zukunft könnten IKT-bezogene Schwachstellen jedoch per Smart Metering bis in die einzelnen Haushalte hineinragen. Besonderheiten stellen soziotechnisch aufwändigere Systeme dar, wie etwa eine Fernwasserversorgung (z. B. Bodensee-Wasserversorgung) oder eine regionale Wasserbeschaffungsgesellschaft (z. B. Hessenwasser).

Darüber hinaus können die innerhäuslichen Versorgungsstrukturen von Wohn- und Bürotürmen durchaus ebenfalls als Teil der Kritischen Infrastruktur gesehen werden. Hier werden Betrieb und Wartung häufig an externe Facility-Management-Dienstleister übertragen, wodurch sich weitere Einfallstore hinsichtlich der Cybersicherheit ergeben. Innerhalb der öffentlichen Wasserversorgung sind daher auch gezielte Cyberattacken auf spezifische Branchen oder begrenzte Gebiete vorstellbar, wie z. B. das Frankfurter Bankenviertel oder Internetknoten und Rechenzentren, deren wasserbasierte Kühlung betroffen sein könnte. Im Gegensatz dazu verfügen große Produktionsstätten (z. B. der Chemie oder Automobilindustrie) oft über eine eigene Wasserversorgung und Abwasserbeseitigung, die gegenüber Cyber-Bedrohungen unterschiedlich gut gewappnet sind.

Das Risiko einer landesweiten Attacke auf die Siedlungswasserwirtschaft ist aufgrund deren Heterogenität und Kleinteiligkeit in Deutschland äußerst gering.

Unabhängig davon, ob öffentliche oder privatwirtschaftliche Wasserversorgungssysteme kompromittiert sind, ist zunächst ein räumlich begrenztes Einzugsgebiet eines Wasserversorgungsunternehmens oder sonstigen Betriebes betroffen. Eine gänzlich andere Bedrohungslage ergibt sich jedoch, wenn beispielsweise mehrere oder sämtliche Wasserwerke eines Landes einer Cyber-Attacke unterliegen. Das Risiko für ein derartiges Szenario kann für Deutschland aufgrund der Kleinteiligkeit und Heterogenität der Siedlungswasserwirtschaft als äußerst gering erachtet werden, ist aber in Ländern mit homogeneren oder zentralisierteren Strukturen grundsätzlich vorstellbar (z. B. Niederlande).

In Bezug auf die Abwasserbeseitigung sind Gefährdungen der Natur unter Cybersicherheitsaspekten als größer zu erachten als solche für die Gesellschaft, z. B. wenn Abwasser im Falle des Ausfalls der Reinigungsanlage unbehandelt in den Vorfluter abläuft. Wo, wie am Rhein, Trinkwasser aus Flusswasser gewonnen wird, kommt es durch das unbehandelt abfließende Abwasser zu Kaskadeneffekten. Aufgrund der gravitären Architektur der Schwemmkanalisation fließt Schmutzwasser ohne äußeren Energieeintrag zumindest bis zur nächsten Pumpstation oder gar bis zur Kläranlage. Die Pumpstation kann damit einen neuralgischen Punkt darstellen. Im schlimmsten Fall kommt es hier zu einem Rückstau des Schmutzwassers bis in die Wohnungen. In Gebieten mit Mischkanalisation gilt dies bei Niederschlag oder Starkregenereignissen auch für Abwasser. Dennoch wird auch in Österreich, wo die Abwasserbeseitigung rechtlich (wie in der EU) nicht als Kritische Infrastruktur gewertet wird, der Ausfallsicherheit von Abwassertransport und -behandlung eine so hohe Priorität beigemessen, dass eine gemeinsame Untersuchung der Cybersicherheit in beiden Bereichen und ein koordiniertes Vorgehen vorgeschlagen wird (Pointl et al. 2019).

Cyber-Gefährdungsszenarien für die Siedlungswasserwirtschaft

Im Kontext der Cybersicherheit in der Siedlungswasserwirtschaft können einerseits bewusst herbeigeführte Gefahren, etwa durch Kriminelle, Terroristen, aber auch Hacker oder Saboteure (Clark et al. 2017), sowie andererseits technisches und menschliches Versagen als Gefahrenkategorien unterschieden werden (Zimmermann und Schramm 2019). Letztere können das Einfallstor für intendierte Attacken darstellen, indem z. B. auf Nachlässigkeiten des Betriebspersonals spekuliert wird oder Fehler bewusst provoziert werden, u. a. ungenügende Zugriffskontrolle, Einschleppen von Schadsoftware oder veraltete Betriebssysteme (Pointl et al. 2019). Intendierte Cyber-Attacken können aus unterschiedlichen Motivationen heraus verübt werden. Klassische Sabotage und Terror wird von organisierten Hackern, sogenannten *Black Hats*, z. B. zum Zweck der Industriesabotage, der Erpressung oder aus ideologischen Gründen betrieben, wobei jeweils Staaten, Unternehmen oder die Öffentlichkeit das Ziel des Angriffs sein können. Dagegen können andere Hacker-Typen (*White Hats* oder *Grey Hats*) das Hacken aber auch als „sportliche Herausforderung" sehen ohne die Absicht, (größeren) Schaden herbeizuführen. Hier dient das Hacken u. a. zur Erlangung von Anerkennung in Hacker-Kreisen; es kann auch mit politischen oder anderen idealistischen Motiven verbunden sein. Schließlich ist aber auch eine interne Sabotage, z. B. verübt durch unzufriedene oder abgewiesene Mitarbeiter, denkbar (Clark et al. 2017). Völkerrechtlich problematisch ist die digitale Kriegsführung, da diese nicht nur auf die militärischen Kombattanten, sondern auch auf die Zivilbevölkerung zielt. Angriffe auf kritische Infrastrukturen finden zudem häufig auch ohne Kriegserklärung statt (Deutscher Bundestag 2015).

Bedingt durch die Abhängigkeit der vulnerablen siedlungswasserwirtschaftlichen Systembestandteile von der Stromversorgung, stellt deren Ausfall ein weiteres Gefährdungsszenario dar (Birkmann et al. 2010). Die Auswirkungen eines durch einen Cyberangriff bedingten Stromausfalls können zum Teil, aber nicht vollständig und nur vorübergehend, durch Notstromaggregate (z. B. zum Betreiben von Pumpen) abgefangen werden. Dieses Szenario wird in dem Roman „Blackout – Morgen ist es zu spät" von Marc Elsberg in einem dystopischen Narrativ illustriert (Koch 2016). Allerdings wird in der Imagination übersehen, dass es in Deutschland bezogen auf die Versorgung mit Trinkwasser in Ballungsgebieten eine Redundanz in einer infrastrukturell unabhängigen Notwasserversorgung gibt (Fischer et al. 2012; BBK 2016).

Regulierungsbedarf und Fazit

Die Praxis hat gezeigt, dass die deutschen Regelungen zur IT-Sicherheit durch eine ausschließliche Fokussierung auf Anlagen an der Wirklichkeit vorbeigehen: Es geht nicht um das reine (Optimierungs-)Geschehen in Wasseraufbereitungsanlagen, Verteilungsnetzen oder Leitzentralen, sondern um komplexe Wechselwirkungen. Mit dem Referentenentwurf für die Novellierung des IT-Sicherheitsgesetzes, dem sog. IT-Sicherheitsgesetz 2.0, verfolgt die Bundesregierung erstmals einen ganzheitlicheren Ansatz. Zudem sollen die für die Betreiber Kritischer Infrastrukturen bestehenden Meldepflichten und Verpflichtungen zur Einhaltung der Mindeststandards auf andere Branchen der Wirtschaft (z. B. die Abfallwirtschaft) ausgeweitet werden, soweit an ihnen besonderes öffentliches Interesse besteht.

„Um Cyber-Sicherheitsvorfällen insgesamt zu begegnen" (Meister und Biselli 2019), sollen nach dem Referentenentwurf aus dem Bundesinnenministerium jedoch nicht nur die Befugnisse der Strafverfolgungs- und Polizeibehörden, sondern auch die des Bundesamtes für Sicherheit in der Informationstechnik erheblich ausgeweitet werden. Da die Bedrohungen des Cyber-Raums unabhängig von den Grenzen der Bundesländer bestehen, sollen die Behörden der Länder durch das Bundesamt unterstützt werden. Ferner sind im Referentenentwurf Ermächtigungen vorgesehen, durch die das Bundesamt selbst fremde Geräte wie PCs oder Internet-Router aus der Ferne prüfen, in die Rolle von Verdächtigen schlüpfen und Internetverkehr manipulieren darf. Weiterhin will der Bund unsichere IT-Technik in den Unternehmen (ohne Ermächtigung und Zustimmung dieser) nachrüsten. Allerdings sind diese Durchgriffsregelungen aktuell höchst umstritten, weil sie Betreiberrechte und Datenschutz einschränken (Meister und Biselli 2019). Zudem wird das beabsichtigte Offenhalten und Nutzen von IT-Schwachstellen durch Sicherheitsbehörden auch innerhalb der Regierungskoalition als „geradezu kontraproduktiv für die IT-Sicherheit" bewertet (Esken 2019).

Mit dem Referentenentwurf für die Novellierung des IT-Sicherheitsgesetzes (IT-Sicherheitsgesetz 2.0) verfolgt die Bundesregierung erstmals einen ganzheitlichen Ansatz.

Nach dem Gesetzentwurf müssen Betreiber Kritischer Infrastrukturen künftig Systeme der Angriffserkennung betreiben. Ein *Intrusion Detection System*, wie es allerdings viele große Betreiber ohnehin bereits als selbstverständlichen Teil ihrer

IT-Sicherheit haben, um illegale Eindringlinge aufzuspüren, wird Pflicht. Zudem dürfen die Betreiber „Kernkomponenten" (also sicherheitsrelevante IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen dienen und für diesen Zweck besonders entwickelt oder geändert wurden) nur noch von Herstellern beziehen, die vorher eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber abgeben haben. Im Zusammenhang mit anderen Kritischen Infrastrukturen (z. B. Telekommunikation) wird aber angezweifelt (Meister und Biselli 2019), dass eine Erklärung über die Vertrauenswürdigkeit des Unternehmens ausreicht, wenn dieses im Ausland produziert und z. B. angenommen werden kann, dass vonseiten der dortigen Geheimdienste ein Zugriff bestehen könnte.

Cybersicherheit muss in Deutschland auch für kleinere und mittlere Unternehmen der Siedlungswasserwirtschaft gewährleistet sein.

Auch sind immer noch Software-Anwendungen von Regulierungen ausgenommen, die nicht nur im Rahmen von Kritischen Infrastrukturen verwendet werden, sondern für darüber hinaus gehende Zwecke entwickelt worden sind. Digitalisierungsbemühungen, bei denen Industrie-4.0-Anwendungen von der Stange gekauft werden, sind also nicht im Visier des staatlichen Versuchs, die Cybersicherheit für die Siedlungswasserwirtschaft zu verbessern.

Angesichts der von uns identifizierten Bedrohungsszenarien reichen die deutschen Regulierungsbemühungen keinesfalls aus. In der Debatte um das IT-Sicherheitsgesetz wird sich völlig falsch auf die großen Wasserunternehmen konzentriert. Aufgrund der größeren Sicherheitslücken, die bei den kleinen Unternehmen bestehen, könnte es jedoch für einen Angreifer auch interessant sein, z. B. viele kleine Wasserunternehmen im Speckgürtel einer Großstadt zu attackieren und dort die Wasserdienstleistungen zu unterbrechen.[1] Gerade in Deutschland sind die Betreiber der Wasserinfrastrukturen stark kommunal orientiert, sodass kleine und mittlere Unternehmen dominieren. Daher sollte das Schutzniveau der Kritischen Infrastrukturen keinesfalls von der Größe des Unternehmens abhängig sein. Wie die Sektor-Studie (BSI 2014) feststellt, ist gerade diese Größenordnung der Versorger aufgrund der Sicherheitsarchitektur besonders anfällig. Lösungen wird es auch für mittlere und kleine Unternehmen geben müssen, wenn nicht ein großer Teil der zu Versorgenden in Deutschland zum Spielball von Cyber-Angreifern gemacht werden soll.

Im Rahmen mehrerer Betreiberbefragungen haben Unternehmen der Siedlungswasserwirtschaft den Wunsch geäußert, externe Unterstützung für Cybersicherheit und den Schutz Kritischer Infrastrukturen einbeziehen zu können (Thim und Pöhls 2018; BSI 2014). Bei aller Vorläufigkeit ihrer Ergebnisse kommt die Sektor-Studie zu dem Ergebnis, dass es insbesondere kleinen und mittleren Wasserunternehmen schwer fällt, Kompetenzen zur IT-Sicherheit bei sich aufzubauen (BSI 2014). Jüngere Auswertungen haben dies bestätigt (Thim und Pöhls 2018). Allerdings könnten Kooperationen zwischen mehreren Unternehmen ein gutes Mittel sein, um hier zu Synergieeffekten zu kommen.

Doch nicht nur für die kleinen Wasserunternehmen bietet eine solche Zusammenarbeit trotz knapper Personaldecke die Möglichkeit, die Herausforderungen sowohl der Digitalisierung als auch der Cybersicherheit gut zu bewältigen. Das BMBF-Projekt „Dienstleistungen und Modelle für die gemeinsame Erbringung von Sicherheitsdienstleistungen", das eine Hochschule und ein Beratungsunternehmen mit dem Wasserunternehmen von Berlin und einem kleinen Zweckverband in Brandenburg durchgeführt hat, macht deutlich, dass auch für große Betreiber Vorteile in einer solchen Zusammenarbeit liegen können (Thim et al. 2012). Ein solcher Verbund könnte z. B. aus einem zentralen Kompetenzzentrum und mehreren regionalen Arbeitsgemeinschaften bestehen, in denen sich gebietsweise z. B. Wasserunternehmen zusammenschließen können, um bedarfsgerechte Schutzkonzepte zu erarbeiten und umzusetzen. Hierbei darf es nicht allein um die Ausfallsicherheit der Infrastrukturen gehen, sondern es muss ebenso auf die Versorgungssicherheit der Bevölkerung geachtet werden.

1 Kleine Wasserwerke können z. B. ein Wasseraufkommen von unter 100.000 m³ pro Jahr haben.

Literatur

Ammermüller, Britta; Fälsch, Marcel (2017): Digitale Wasserwirtschaft. Facts and Figures. Berlin: Verband kommunaler Unternehmen e. V.

Barjenbruch, Matthias et al. (2016): Forschungsbedarf in der Wasserwirtschaft. Water Innovation Circle. Bonn: DWA.

BBK – Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2016): Trinkwassernotversorgung. Bonn: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

Birkmann, Jörn; Bach, Claudia; Guhl, Silvie; Witting, Maximilian; Welle, Torsten; Schmude, Miron (2010): State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom, Stromausfall. Berlin: Freie Universität Berlin.

BSI – Bundesamt für Sicherheit in der Informationstechnik (2014): KRITIS-Sektorstudie. Ernährung und Wasser. Öffentliche Version, Revisionsstand 16. März 2015. Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Clark, Robert; Panguluri, Srinivas; Nelson, Trent; Wyman, Richard (2017): Protecting drinking water utilities from cyberthreats. In: Journal of American Water Works Association 109 (2), S. 50–58.

Deutscher Bundestag (2015): Anwendbarkeit des humanitären Völkerrechts auf Computernetzwerkoperationen und digitale Kriegsführung (Cyber Warfare). Ausarbeitung WD 2-3000-038/15. Berlin: Wissenschaftliche Dienste Deutscher Bundestag.

Esken, Saskia (2019): Zur Sache. Interview mit Saskia Esken. In: Gesellschaft für Informatik e. V. (Hg.): Jahresbericht 2018/19, S. 28. Online verfügbar unter https://gi.de/fileadmin/GI/Hauptseite/Service/Infomaterial/GI_Jahresbericht_19_Web.pdf, zuletzt geprüft am 21. 01. 2020.

Fischer, Peter; Rönnfeldt, Jens; Schindler, Norbert; Nees, Peter (2012): Trinkwassernotversorgung. Betrieb eines Bundes-Notbrunnens in Darmstadt. In: Bevölkerungsschutz (4), S. 23–25.

Fluchs, Sarah (2017): IT-Grundschutz-Pilotprofil bzw. IT-Grundschutz-Profil für die Wasserwirtschaft. Masterarbeit. Aachen: RWTH Aachen.

Gaycken, Sandro (2010): Stuxnet. Wer war's? Und wozu? In: DIE ZEIT, Nr. 48. Online verfügbar unter https://www.zeit.de/2010/48/Computerwurm-Stuxnet/komplettansicht, zuletzt geprüft am 25. 09. 2019.

Graumann, Sabine (2017): Energie- und Wasserversorger noch verhalten bei Digitalisierung. In: energie/wasser-praxis (4), S. 6–9.

Koch, Lars (2016): Heart of Darkness. Über das katastrophische Imaginäre des Blackouts. In: BEHEMOTH – A Journal on Civilisation 9 (1), S. 58–76.

Lachance, Lancen (2016): IT vs. OT für das Industrielle Internet. Zwei Seiten einer Medaille? In: GlobalSign Blog. Online verfügbar unter https://www.globalsign.com/de-de/blog/it-vs-ot-im-industriellen-internet/, zuletzt geprüft am 25. 09. 2019.

Meister, Andre; Biselli, Anna (2019): IT-Sicherheitsgesetz 2.0. Wir veröffentlichen den Entwurf, der das BSI zur Hackerbehörde machen soll. In: Netzpolitik.Org. Online verfügbar unter https://www.netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll, zuletzt geprüft am 25. 09. 2019.

Pohl, Christian; Spinnreker-Czichon, Dominic; Keilholz, Patrick (2017): Wasserwirtschaft 4.0. Voraussetzung für eine intelligente Vernetzung von Bestandssystemen. Bremen: DHI WASY.

Pointl, Michael; Winkelbauer, Andreas; Krampe, Jörg; Fuchs-Hanusch, Daniela (2019): Aspekte der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft. In: Österreichische Wasser- und Abfallwirtschaft 71 (7–8), S. 374–384. DOI: 10.1007/s00506-019-0584-y.

Schaffer, Carsten; Vestner, Richard; Bufler, Ralf; Werner, Uwe; Ziemer, Christian (2019): Wasser 4.0. Berlin: German Water Partnership e. V. (GWP).

Statistisches Bundesamt (2019 a): Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung. Öffentliche Abwasserbehandlung und -entsorgung. Fachserie 19, Reihe 2.1.2. Wiesbaden: Statistisches Bundesamt (Destatis).

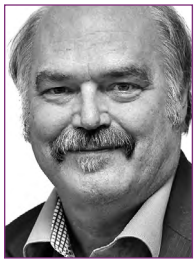
Statistisches Bundesamt (2019 b): Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung. Öffentliche Wasserversorgung. Fachserie 19, Reihe 2.1.1. Wiesbaden: Statistisches Bundesamt (Destatis).

Thim, Christof; Pöhls, Uwe (2018): Stand der IT-Sicherheit in der Wasserversorgung. In: wwt wasserwirtschaft wassertechnik 2018 (1–2), S. 40–42.

Thim, Christof; Röchert-Voigt, Tanja; Proske, Niels; Heine, Moreen; Korte, Edgar (2012): Organisation des Schutzes der Kritischen Infrastruktur Wasserversorgung. Grundlagen und praktische Anwendung für Wasserversorger. Potsdam: Universität Potsdam.

Zimmermann, Martin; Schramm, Engelbert (2019): Digitalisierung als Herausforderung. Die Vulnerabilität Kritischer Infrastrukturen in der Siedlungswasserwirtschaft. In: Transforming Cities 2019 (4), S. 58–62.

DR.-ING. MARTIN ZIMMERMANN
ist wissenschaftlicher Mitarbeiter des ISOE und leitet seit Juli 2018 den Forschungsschwerpunkt Wasserinfrastruktur und Risikoanalysen. Er studierte Wirtschaftsingenieurwesen mit der technischen Fachrichtung Bauingenieurwesen an der TU Darmstadt und promovierte im DFG-Graduiertenkolleg „Topologie der Technik".



DR. ENGELBERT SCHRAMM
ist Mitbegründer des ISOE und war von 2014 bis Juli 2018 Mitglied der Institutsleitung. Er hat ein Studium der Biologie, Chemie und Erziehungswissenschaften an der Universität Frankfurt am Main absolviert. 1995 hat er zur Ideengeschichte des Kreislaufs an der TU Darmstadt promoviert.

BJÖRN EBERT
arbeitet als wissenschaftlicher Mitarbeiter des ISOE im Forschungsschwerpunkt Wasserinfrastruktur und Risikoanalysen. Er studierte Politikwissenschaft und Volkswirtschaftslehre in Frankfurt sowie an der Freien Universität Berlin und promoviert derzeit im Bereich der Technik- und Innovationssoziologie.