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).

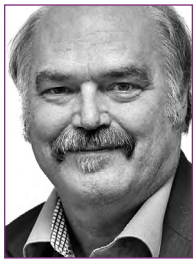
Statistisches Bundesamt (2019 b): Öffentliche Wasserversorgung und öffentliche Abwasserentsorgung. Öffentliche Wasserversorgung. Fachserie 19, Reihe 2.1.1. Wiesbaden: Statistisches Bundesamt (Destatis).

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.