Originalarbeit

Österr Wasser- und Abfallw 2019 · 71:374–384
https://doi.org/10.1007/s00506-019-0584-y

Aspekte der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft

Michael Pointl · Andreas Winkelbauer · Jörg Krampe · Daniela Fuchs-Hanusch

Online publiziert: 9. Mai 2019

Zusammenfassung Durch die fortschreitende Digitalisierung und Automatisierung in der Siedlungswasserwirtschaft kommt den Systemen der Informations- und Kommunikationstechnik (IKT) eine immer größere Bedeutung zu. Während die zunehmende Vernetzung von wasserwirtschaftlichen Anlagen und IKT-Systemen zahlreiche betriebliche und wirtschaftliche Vorteile mit sich bringt, ruft sie auch höheres Potenzial für IKT-Vorfälle hervor. Dabei kann es sich um gezielte Cyberattacken auf die eingesetzten Anlagen oder nicht zielgerichtete, systematische Angriffe von Dritten handeln, die in Störungen des Betriebs oder Ausfällen bei Wasserversorgungsunternehmen (WVU) und Abwasserreinigungsanlagen (ARA) resultieren. Der IKT-Sicherheit, insbesondere bei der Sicherstellung der Versorgungs- und Betriebssicherheit siedlungswasserwirtschaftlicher Betriebe, kommt daher eine entsprechend hohe Bedeutung zu.

Um den Status und die bisherige Rolle der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft zu erheben, wurde im Auftrag des Bundesministeriums für Nachhaltigkeit und Tourismus eine Studie mit einer Reihe beispielhaft ausgewählter und näher untersuchter WVU und ARA durchgeführt. Neben dem institutionellen Umgang mit IKT-Systemen wurden dabei die etablierten und geplanten technischen und organisatorischen Schutzmaßnahmen erhoben. Auf Basis einer systematischen Schwachstellenanalyse wurden Kaskadenwirkungen potenzieller Gefährdungen auf die Versorgungssicherheit bei WVU und die Betriebssicherheit bei ARA analysiert. Die Ergebnisse zeigen einen an sich hohen Standard der IKT-Sicherheit, aber auch eine Reihe nicht unerheblicher, vor allem organisatorischer, Schwachstellen, die einer Nachschärfung im Bereich der Maßnahmensetzung bedürfen. Bei der Mehrheit der Entscheidungsträger ist ein Bewusstsein für auftretende Risiken vorhanden und idealerweise wird versucht, die IKT-Sicherheit der Anlagen einem kontinuierlichen Verbesserungsprozess zu unterwerfen und diesen auch laufend zu evaluieren.

Schlüsselwörter IKT-Systeme · Cybersicherheit · Kritische Infrastrukturen · Wasserversorgung · Abwasserreinigung

DI M. Pointl, BSc (✉) ·
Assoc. Prof. DI. Dr. D. Fuchs-Hanusch
Institut für Siedlungswasserwirtschaft und Landschaftswasserbau, Technische Universität Graz, Stremayrgasse 10/I, 8010 Graz, Österreich
michael.pointl@tugraz.at

Assoc. Prof. DI. Dr. D. Fuchs-Hanusch
fuchs-hanusch@tugraz.at

DI A. Winkelbauer, BSc ·
Univ.-Prof. Dr.-Ing. J. Krampe
Institut für Wassergüte und Ressourcenmanagement, Technische Universität Wien, Karlsplatz 13/2261, 1040 Wien, Österreich

DI A. Winkelbauer, BSc
awinkelbauer@iwag.tuwien.ac.at

Univ.-Prof. Dr.-Ing. J. Krampe
jkrampe@iwag.tuwien.ac.at

Aspects of ICT-Security in the Austrian Water Sector

Abstract Advancements in digitalization and automation in the water sector lead to a continuously increasing role of information and communication technology (ICT). While a more extensive use and further integration of ICT systems induce numerous operational and economic benefits, the vulnerability of water utilities (WU) and wastewater treatment plants (WWTP) to ICT incidents and cyber threats, potentially resulting in damages or disruptions, is arising. Consequently, the security of ICT systems is a key issue of reliable WU and WWTP operation.

In this work, we present the results of a study comissioned by the Federal Ministry of Sustainability and Tourism with the aim of assessing the overall status and implemented efforts to ensure ICT security in the Austrian water sector. In collaboration with several WU and WWTP an in-depth analysis of operational and technical security measures was conducted and the gained results were used for an extensive vulnerability analysis. Based on identified vulnerabilities, key threats to ICT systems were identified and consequences for WU and WWTP operation were assessed. Results show a generally high level of ICT security, but also highlight a number of common, mainly operational, vulnerabilities. The majority of decision makers, managers and personnel are aware of evolving cyber threats and focus on measures to protect and harden their ICT systems.

Keywords ICT-systems · Cyber security · Critical infrastructures · Water distribution · Wastewater treatment

1 Einleitung

Eine möglichst unterbrechungsfreie Versorgung der Bevölkerung mit hochwertigem Trinkwasser und die bestmögliche Reinigung von Abwässern vor deren Rückführung in den Wasserkreislauf stellen zwei der wesentlichen Kernaufgaben der Siedlungswasserwirtschaft dar. Um diesen Aufgaben nachkommen zu können, setzen Wasserversorgungsunternehmen (WVU) und Abwasserreinigungsanlagen (ARA) Informations- und Kommunikationssysteme (IKT) zur Anlagenautomatisierung ein. Innerhalb der IKT dienen dabei Systeme der *Information Technology* (IT) vorwiegend der Administration und Organisation und Systeme der *Operational Technology* (OT) dem Zweck der Prozessüberwachung und -steuerung (Gartner 2018a, b; Lachance 2018).

Die dem Bereich der OT zugerechneten Anlagen, häufig auch als *Prozessleitsysteme* bezeichnet, waren traditionell meist geschlossene bzw. *gekapselte* Systeme, die keine Anbindung zu anderen Netzwerken aufwiesen und mit anderen Systemen häufig auch nicht kompatibel waren. Mit der zunehmenden Digitalisierung und den damit einhergehenden Möglichkeiten, beispielsweise der Möglichkeit von Fernzugriffen auf die OT über Geräte der stationären und mobilen IT, ist diese klare, physische Trennung heute de facto nicht mehr vorhanden. Die Vernetzung von OT und IT nimmt darüber hinaus durch die zunehmende Verfügbarkeit von Technologien wie dem sogenannten *Internet of Things* und die Nutzung eines breiten Spektrums an Applikationen, beispielsweise für den direkten Export und die Analyse von Betriebsdaten der Anlagen, weiter zu.

Neben den zahlreichen operativen und ökonomischen Vorteilen der verstärkten Vernetzung der IKT-Systeme von WVU und ARA stellt diese Behörden, Branchenverbände, Hersteller, Dienstleister und Betreiber vor die Herausforderung, die *IKT-Sicherheit* oder *Cybersicherheit* der Anlagen in weitreichende, strategische Überlegungen einzubeziehen und neue Konzepte im laufenden Betrieb umzusetzen und zu evaluieren. Dabei sind neben gezielten Attacken auf OT oder IT auch deren Trennung sowie Wechselwirkungen zwischen beiden Bereichen bei deren Vernetzung unter ausbleibender Trennung von Bedeutung. Darüber hinaus sind auch nicht-zielgerichtete, systematische Attacken und Bedienfehler zu berücksichtigen.

Zum systematischen Aufbau und der Gestaltung von Maßnahmen zur Sicherstellung eines hohen Schutzniveaus von IKT-Systemen ist eine große Zahl von Normen, Standards und Leitfäden, wie jene des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI, Bundesamt für Sicherheit in der Informationstechnik 2008, 2017a, b, c), sowie Konzepten zur Analyse und Modellierung der Auswirkungen einer Kompromittierung der OT auf den Betrieb von WVU und ARA verfügbar (Morris et al. 2011; Papa et al. 2013; Nazir et al. 2017; Taormina et al. 2017). Empfehlungen zu Maßnahmen der umfassenden Gewährleistung eines geordneten Betriebs der IKT-Anlagen in der Siedlungswasserwirtschaft (Panguluri et al. 2011; Rao und Francis 2015; Alcaraz und Zeadally 2015; Manalo et al. 2015; Clark et al. 2017), die auf Basis von Erhebungen regionaler und nationaler Behörden und Interessens- bzw. Branchenverbände (AWWA, American Water Works Association 2017; DWA, Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall 2017) erstellt wurden, und je nach Zielgruppe unterschiedliche fachliche Tiefe aufweisen, liegen ebenfalls vor. Die große Herausforderung der praktischen Umsetzung liegt im Detail. Umfassend gedachte, überblicksweise Arbeiten geben zum Teil wenig Anhaltspunkte zur Setzung konkreter Maßnahmen und spezialisierte Vorgaben zur Absicherung bestimmter Geräteklassen sind im Kontext der spezialisierten Systeme der Siedlungswasserwirtschaft zum Teil nur schwer umsetzbar.

Auf Ebene der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates (2016) (NIS-RL) sind die Betreiber von als *kritisch* eingestuften Infrastrukturen – worunter, in Abhängigkeit von produzierter Wassermenge sowie Art und Anzahl der versorgten Kunden, Anlagen der *Wassergewinnung, -aufbereitung und -versorgung* fallen können – verpflichtet, Mindeststandards zur Sicherung ihrer IKT-Systeme einzuhalten und diese bei Audits auch nachzuweisen. Zusätzlich wurde eine Meldepflicht von IKT-Vorfällen für diese zu benennenden Unternehmen eingeführt. Infrastrukturbetreiber, deren Anlagen nicht als kritisch eingestuft wurden, können die Meldung von IKT-Vorfällen auf freiwilliger Basis bei derselben Stelle durchführen (Cyber Sicherheit Steuerungsgruppe 2018).

Die Überführung der NIS-RL in nationales Recht (*Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)* (2018)) wurde zum Anlass genommen, den Status quo der IKT-Sicherheit der österreichischen Siedlungswasserwirtschaft durch nähere Untersuchung einer ausgewählten Gruppe von WVU und ARA zu evaluieren. Ausschlaggebend für die Auswahl war dabei die heterogene Struktur der Unternehmen in der Branche.

Obwohl gemäß NISG und dem Österreichischem Programm zum Schutz kritischer Infrastrukturen (Bundeskanzleramt der Republik Österreich 2015) lediglich die Wasserversorgung bzw. bestimmte WVU als kritische Infrastrukturen angesehen werden, muss einer ausfallsicheren Abwasserentsorgung bzw. -reinigung eine hohe Priorität beigemessen werden, weshalb eine gemeinsame Untersuchung und ein akkordiertes Vorgehen bei WVU und ARA als sinnvoll und notwendig angesehen wird.

Gemäß ÖVGW, Österreichische Vereinigung für das Gas- und Wasserfach (2018) werden in Österreich 91,8 % der Bevölkerung über eine zentrale Wasserversorgung mit Trinkwasser versorgt. Die insgesamt rund 5500 WVU in Österreich lassen sich in ca. 3400 Genossenschaften, 1900 kommunale Versorger und etwa 165 Verbände einteilen. Neben Organisations- und Rechtsform der WVU variieren Struktur und Betriebsweise der Anlagen signifikant. Die Art der Wassergewinnung, Topografie und Größe des Versorgungsgebietes sowie die Qualität des Trinkwassers haben wesentlichen Einfluss auf die Größe der Wasserverteilungsanlagen und damit indirekt auch auf die Prozesse, die durch die OT überwacht und gesteuert werden. Neben der notwendigen Steuerung von Pumpen und Schiebern werden in Österreich rund zwei Drittel des gewonnenen Trinkwassers desinfiziert, 6 % einer konventionellen Behandlung (z. B. durch Filtration oder Enteisenung) und etwa 1 % einer weitergehenden Behandlung zugeführt.

Nach Assmann et al. (2016) sind auf Seiten der Abwasserreinigung rund 16.000 Kläranlagen mit einer Ausbaukapazität von 28,3 Mio. Einwohnerwerten (EW) mit direkt in ein Gewässer einleitendem Ablauf in Betrieb. Davon sind rund 14.000 Kleinkläranlagen (bis 50 EW) und rund 1800 kommunale Kläranlagen (51 EW bis über 50.000 EW). Die restlichen Betriebe zählen zu den Industrie- und Gewerbekläranlagen. Rund 70 % der Gesamtausbaukapazität entfällt auf kommunale Kläranlagen mit mehr als 50 EW, 64 % davon auf jene mit mehr als 50.000 EW. Rechts- und Organisationsform der ARA hängen meist direkt mit der Ausbaukapazität der Kläranlagen sowie der Größe und Siedlungsstruktur des Einzugsgebiets zusammen. Kläranlagen sind meist als Genossenschaften, Verbandskläranlagen, Gemeindekläranlagen oder Kommunalunternehmen organisiert. Entsprechend der Ausbaugröße müssen die hydraulischen Abläufe und Reinigungsprozesse geregelt werden. Die OT wird auf den Kläranlagen, Pumpwerke oder aktivierbaren Stau- und Speichervolumina in der an-

geschlossenen Kanalisation zur Überwachung und Steuerung der Prozesse eingesetzt. Darüber hinaus wird die Automatisierungstechnologie für einen integrierten Betrieb unterschiedlicher Verfahren zur Klärschlammstabilisierung, -verwertung und Energiegewinnung auf der Kläranlage eingesetzt.

In dieser Arbeit werden Methodik und Ergebnisse einer Studie zur Evaluierung der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft (Pointl et al. 2018) präsentiert, die im Auftrag des Bundesministeriums für Nachhaltigkeit und Tourismus erstellt wurde. Ziel dieser Studie war es, einen ersten Eindruck vom Status quo der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft zu gewinnen. Über einen mehrstufigen Prozess wurde der institutionelle Umgang mit dem Thema IKT-Sicherheit in den Unternehmen erhoben. In Hinblick auf entsprechende Normen, Richtlinien und unter Berücksichtigung existierender Leitfäden und Mindeststandards, wurde die Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen für die IKT-Systeme einer Gruppe von WVU und ARA erhoben und evaluiert. Die gesammelten Informationen wurden in eine Schwachstellenanalyse übergeführt, die in weiterer Folge als Basis für eine Wirkungsanalyse und Risikobewertung potenzieller Gefährdungen für Versorgungs- und Betriebssicherheit diente.

Im Weiteren folgen nach einer Beschreibung der entwickelten Methodik zur Beurteilung der IKT-Sicherheit von Anlagen der Siedlungswasserwirtschaft eine Zusammenfassung und Diskussion der Ergebnisse sowie darauf aufbauende Schlussfolgerungen und Empfehlungen.

2 Erhebung der IKT-Sicherheit

Ziel der durchgeführten Studie war eine erste Erhebung und Beurteilung des Status quo der IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft. Durch eine integrierte Analyse auf Grundlage von entsprechenden Unterlagen, Befragungen und Besichtigungen der Anlagen vor Ort, wurden die organisatorischen und technischen Rahmenbedingungen der Anlagensicherheit bei einzelnen Betreibern erhoben. Mit einer eigens dafür entwickelten Methodik wurden Schwachstellen in IKT-Systemen systematisch erhoben und auf ein individuelles Modell der IKT-Systeme umgelegt. Darauf aufbauend erfolgte eine Beurteilung, wo und in welchem Ausmaß potenzielle Gefährdungen wirksam werden können und welche Konsequenzen sich dadurch für den geordneten Betrieb von WVU und ARA ergeben.

Der Fokus der Studie lag auf der OT zur Überwachung und Steuerung der Prozesse der Wasserversorgung bzw. der Abwasserreinigung. IT-Systeme wurden lediglich im Kontext der OT analysiert. Dabei standen bei der Berücksichtigung der IT zwei Aspekte im Vordergrund. Zum einen, ob diese beispielsweise durch eine unsichere oder inkonsequente Netzwerktrennung eine Schwachstelle für die OT darstellt und zum anderen, ob und wie die – meist zur Realisierung eines gewissen Bedienkomforts gestalteten – Zugriffe von der IT auf die OT gehandhabt, gesichert und geprüft werden. In der Schnittmenge von OT und IT wurden Bedeutung und potenzielle Risiken neuer Technologien und Konzepte, die häufig mit Begriffen wie *Internet of Things, Industrie 4.0* und *Smart Water* zusammengefasst werden, analysiert.

Neben der Erhebung des aktuellen Umgangs mit und dem Bewusstsein für die IKT-Sicherheit dienen Methodik und Ergebnisse der Studie als Basis für eine systematische, weiterführende Bearbeitung der Thematik für WVU und ARA, besonders Bezug nehmend auf deren unterschiedliche Anlagenstrukturen und personelle und ökonomische Rahmenbedingungen. Die gezielte Entwicklung von Richtlinien und Werkzeugen soll begünstigt werden, um es Anlagenbetreibern zu ermöglichen, Mindeststandards zu implementieren, ihre IKT-Systeme proaktiv und zielgerichtet einzurichten und abzusichern und auf sich laufend verändernde Bedrohungslagen angemessen zu reagieren.

Die Gruppe der untersuchten Anlagenbetreiber umfasst acht WVU und vier ARA, die gemäß der Struktur der österreichischen Siedlungswasserwirtschaft ein breites Spektrum an Anlagengrößen, Mitarbeiterzahl, sowie verschiedener Rechts- und Organisationsformen abdecken. Obwohl es sich bei dieser Gruppe nicht um eine repräsentative Stichprobe handelt, wurden Anlagen bzw. Unternehmen im Hinblick auf eine möglichst gute Abbildung der Situation in der Branche ausgewählt. Die ARA variieren unter anderem hinsichtlich Organisationsform, Einzugsgebiet, angeschlossener Kanalisation sowie Ausbaugröße von Kläranlagen. Bei den WVU wurden Anlagen mit unterschiedlicher Form der Wassergewinnung und Behandlung sowie Gemeindeversorger, Genossenschaften, überregionale Versorgungsverbände und auch klassische Stadtwerke analysiert.

Gemäß der im folgenden Abschnitt beschriebenen Methodik wurden für die Gruppe der Studienteilnehmer umfassende Schwachstellen- und Wirkungsanalysen der IKT-Systeme durchgeführt. Darüber hinaus wurden für einzelne, maßgebende Szenarien Risikobewertungen erstellt und es wurde ein Konzept entwickelt, anhand dessen eine detaillierte Risikoanalyse möglich ist.

Während bei der Wirkungsanalyse und Risikobewertung für die OT bei den WVU die Sicherstellung der Versorgungssicherheit der Kunden als zentrale Prämisse galt, wurde der Fokus bei den ARA auf die Einhaltung von Eliminationsraten und Emissionsgrenzwerten, also auf die anthropogenen Auswirkungen auf die Vorfluter, gelegt.

Zur Gewährung größtmöglicher Anonymität der Betreiber und um die Sicherheit ihrer IKT-Systeme nicht zu gefährden, wird im Folgenden auf unternehmens- oder anlagenspezifische Angaben verzichtet.

2.1 Methodik

Aufgrund des sensiblen Charakters der Studie werden hier lediglich die Grundzüge der angewandten Methodik zur Beurteilung der Sicherheit von IKT-Systemen in der Siedlungswasserwirtschaft beschrieben. Grundsätzlich orientiert sich das Vorgehen und damit die durchzuführenden Analysen an jenen des BSI-Standard 200 (BSI, Bundesamt für Sicherheit in der Informationstechnik, 2017b, c). Abb. 1 stellt eine Übersicht über die entwickelte Methodik dar, deren einzelne Teilschritte nachfolgend detaillierter dargelegt werden.

2.1.1 Datenerhebung und Datenauswertung

Die Datenerhebung erfolgt anhand eines Fragebogens, Interviews mit Anlagenverantwortlichen und Anlagenbetreuern sowie durch Besichtigungen der IKT-Systeme und der jeweiligen Wasserversorgungs- bzw. Abwasserentsorgungsanlagen.

Der eingesetzte Fragebogen umfasst rund 150 Fragen und ist in acht

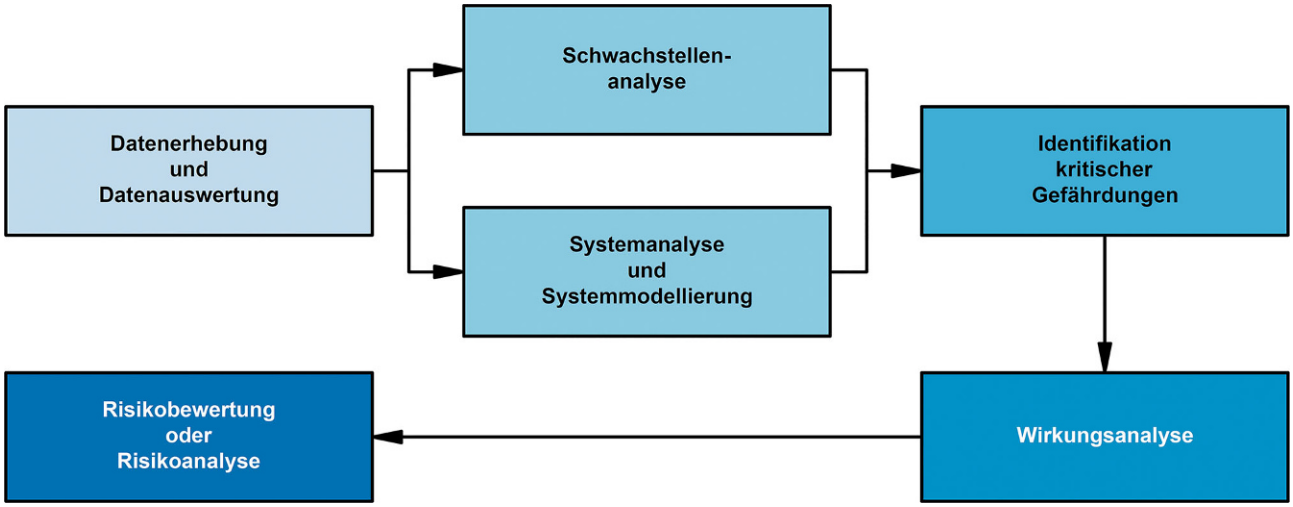

Abb. 1 Teilschritte der Analysemethodik

Themenkomplexe gegliedert (siehe dazu Tab. 1). Er wurde auf Basis eines vergleichbaren Dokuments (Luiijf et al. 2011) erstellt und anhand von Leitfäden zu branchenspezifischen Mindeststandards der IKT-Sicherheit (WaterISAC Security Information Center 2015; EPA, Environmental Protection Agency 2016) sowie aus bekannten IKT-Sicherheitsvorfällen und -Sicherheitsüberprüfungen in der Siedlungswasserwirtschaft gewonnenen Erkenntnissen (Graham et al. 2012; Noble et al. 2017) adaptiert und erweitert. Die Themenkomplexe wurden definiert, um Unterschiede in den Angaben der Studienteilnehmer angemessen berücksichtigen zu können und um die standardisierten Antworten der Fragebogenauswertung um zusätzlich erfasste Angaben aus den Interviews und Informationen aus den erfolgten Besichtigungen ergänzen zu können. Um eine Beeinflussung der Studienteilnehmer durch suggestive Fragestellungen zu vermeiden, wurden unter anderem die Themenkomplexe auf den Fragebögen nicht explizit ausgewiesen. Die Beantwortung des Fragebogens erfolgte im Rahmen der Studie zum Teil unter Einbeziehung von IKT-Anlagenherstellern und -Dienstleistern.

Die vorab ausgefüllten Fragebögen wurden gemeinsam mit Schemadarstellungen der IKT-Systeme und Plänen der Wasserversorgung- und Abwasserreinigungsanlagen analysiert, um auf Basis erster Erkenntnisse zum Anlagenzustand Interviews- und Anlagenbesichtigungen gezielt ausrichten und durchführen zu können. Die gesammelten Daten und Pläne bilden in weiterer Folge die Grundlage umfassender Schwachstellen- und Wirkungsanalysen.

2.1.2 Schwachstellenanalyse

Aufbauend auf den Informationen aus der Auswertung des Fragebogens, der Interviews und Besichtigungen werden die IKT-Schwachstellen jedes Studienteilnehmers identifiziert. Die spezifischen Schwachstellen werden neben einer individuellen Analyse für die Themenkomplexe TK.01 bis TK.07 zusammengeführt (Abb. 2a).

Neben der Bestimmung von Anzahl und Schwere konkreter Schwachstellen wird für jeden Themenkomplex ein *Sicherheitsniveau* abgeleitet. Basis hierfür bildet das sogenannte *grundlegende Sicherheitsniveau* eines Themenkomplexes, in dessen Bewertung unter anderem Umfang, Aktualität und Qualität der umgesetzten Sicherheitsmaßnahmen sowie deren laufende Evaluierung, regelmäßige Audits und kontinuierliche Verbesserungen, jeweils bezogen auf die individuellen Rahmenbedingungen des Anlagenbetreibers, Eingang finden. Es handelt sich um eine Form der Normierung, in die unter anderem Art und Größe des Unternehmens, dessen interne Strukturen sowie technische, wirtschaftliche und personelle Möglichkeiten einfließen. Basis für diese Normierung, die einen Vergleich zwischen den sehr unterschiedlichen Studienteilnehmern ermöglicht, sind die in Themenkomplex TK.00 zusammengefassten Angaben. Ausgehend vom höchsten zum niedrigsten, wird zwischen den vier grundlegenden Sicherheitsniveaus *hoch, mittel, niedrig* und *minimal* unterschieden.

Das grundlegende Sicherheitsniveau eines Themenkomplexes wird anhand der Anzahl (Abb. 2a) und Schwere der identifizierten Schwachstellen reduziert, wodurch sich das *abgeleitete* oder *endgültige Sicherheitsniveau* ergibt (Abb. 2b). Analog zum grundlegenden Sicherheitsniveau wird dabei, vom höchsten zum niedrigsten, zwischen den vier Sicherheitsniveaus hoch, mittel, niedrig und minimal unterschieden. In der Darstellung in Abb. 2b nehmen diese von außen nach innen entsprechend ab.

2.1.3 Systemanalyse und Systemmodellierung

Um die Auswirkungen von IKT-Vorfällen (Angriffe, Stör- und Ausfälle) auf den Betrieb von WVU und ARA bewerten zu können, wurden, in Anlehnung an die Systematik in Fluchs (2017a, b) *Standardbausteine* definiert, die dazu dienen, technische und organisatorische IKT-Komponenten nachzubilden, um individuelle IKT-Infrastrukturen von WVU und ARA, deren Einbindung in die Organisation des Betriebs und ihre Anknüpfungspunkte an die Ver- bzw. Entsorgungsanlagen nachzubilden. So ist es möglich, eine standardisierte Wirkungs- oder Risikoanalyse unter Berücksichtigung individueller Anlagen- und Unternehmensstrukturen, ausgehend von einer gemeinsamen, abstrahierten Anlagenstruktur, durchzuführen.

Bei den *technischen Komponenten* werden die Standardbausteine unter

Tab. 1 Themenkomplexe des Fragebogens

Themenkomplex	Inhalt
TK.00	Unternehmensdaten, allgemeine Angaben zu Rechtsform und Organisation, Anlagenkennwerte
TK.01	Richtlinien und Rollen im Kontext der IKT-Sicherheit
TK.02	Perimeterschutz, physische Anlagensicherheit und Zutrittsmanagement
TK.03	OT-Zugriffsmanagement
TK.04	OT-Systemarchitektur
TK.05	Trennung der OT von anderen Netzwerken, IT und IT-Management
TK.06	Updates, laufende Betreuung und IKT-Wartung
TK.07	Parallel zur OT betriebene, nicht direkt in diese eingebundene Sensornetze, Internet of Things

anderem zur Repräsentation von Steuerelementen, Kommunikationsanlagen und der Netzwerktrennung der IT von der OT eingesetzt. Bei den *organisatorischen Komponenten* wurden Standardbausteine definiert, mit deren Hilfe die Verwaltung von Zutritts- oder Zugriffsberechtigungen oder der geregelte Umgang mit Systemkomponenten dargestellt werden kann.

In Abb. 3 ist die typische Anlagenstruktur eines siedlungswasserwirtschaftlichen Betriebs anhand dieser Standardbausteine dargestellt. Neben den verschiedenen Möglichkeiten der Vernetzung von Anlagen und Gewerken sind, für organisatorische Belange und institutionellen Umgang, die auftretenden Mensch-Maschine-Schnittstellen wesentlich. Diese sind in Abb. 3 durch Elemente mit kontinuierlichem Farbverlauf dargestellt. Im Rahmen der Erhebung werden organisatorische Komponenten dort ergänzt, wo diese Mensch-Maschine-Schnittstellen auftreten. Als Grundlage für die Nachbildung und Abstraktion der IKT-Systeme dienen Informationen aus der Datenerhebung, Skizzen des IT-Systems und der OT sowie der damit gesteuerten Anlagen, wobei die IT lediglich als potenzielle Schwachstelle für die OT berücksichtigt wird.

2.1.4 *Identifikation kritischer Gefährdungen und Wirkungsanalyse*

Mithilfe der nachgebildeten Anlagen und IKT-Systeme ist es möglich, die identifizierten Schwachstellen einzelnen IKT-Komponenten zuzuordnen und so für die OT relevante Schwachstellen zu bestimmen. Ausgehend von Schwachstellen einzelner Komponenten wurden Wirkungskaskaden kritischer Gefährdungen, von der Schwachstelle bis hin zu den Anlagenteilen der Wasserversorgung oder der Abwasserentsorgung, wie beispielsweise Pumpen oder Kompressoren, bestimmt. Durch die integrierte Betrachtung der Wirkungskaskaden aller kritischen Gefährdungen für ein IKT-System ist es möglich, die Konsequenzen mangelnder Sicherheitsvorkehrungen bzw. Schwachstellen für den Anlagenbetrieb zu bestimmen.

2.1.5 *Risikobewertung oder Risikoanalyse*

Aufgrund des Mangels an belastbaren Daten und der Eintrittswahrscheinlichkeiten von IKT-Vorfällen konnte im Rahmen der Studie keine umfassende, quantitative Risikoanalyse durchgeführt werden. An Stelle einer quantitativen Risikoanalyse wurden Wirkungskaskaden für maßgebliche Szenarien analysiert und die daraus resultierenden Risiken für die Versorgung der Kunden von WVU und die Betriebssicherheit der ARA bewertet. Die Risikobewertung erfolgte qualitativ unter Einbeziehung zahlreicher Randbedingungen. Die für den Betrieb erforderlichen OT-Kenntnisse, sowie das erforderliche Wissen um die Prozesse des WVU bzw. der ARA wurden mitberücksichtigt. Darüber hinaus wurde bedacht, wie weitreichend die Konsequenzen einzelner IKT-Vorfälle für Standorte und Prozesse der Anlagen wären, wie lange es dauern würde, bis ein Vorfall detektiert wird, wie schnell eine adäquate Reaktion möglich wäre und wie rasch zum Regelbetrieb zurückgekehrt werden könnte.

3 Ergebnisse und Diskussion

Aufgrund des sicherheitsrelevanten Charakters der gewonnenen Erkenntnisse und um die Anonymität der Studienteilnehmer zu wahren und keine spezifischen Schwachstellen preiszugeben, werden im Folgenden vorwiegend Punkte angeführt, die bei der Mehrheit der Unternehmen beobachtet wurden.

3.1 Bedeutung der IKT-Sicherheit

Grundsätzlich hat sich gezeigt, dass sich Entscheidungsträger und Anlagenverantwortliche der zunehmenden Bedeutung der IKT-Sicherheit und der sich ständig weiterentwickelnden, potenziellen Gefährdungen, denen ihre Anlagen ausgesetzt sind, bewusst sind. Dieses Bewusstsein wurde bei fast allen Studienteilnehmern festgestellt. Als Gründe für entsprechende Überlegungen wurden meist die sich ändernde rechtliche Situation oder auch die Erwartung einer solchen Änderung genannt. In Anbetracht der zunehmenden Digitalisierung der Branche werden IKT-Vorfälle und -Attacken bei gleichen oder ähnlichen Infrastrukturen mit großer Achtsamkeit und zum Teil auch aus persönlichem Interesse verfolgt. Das Bewusstsein für die Vulnerabilität, die sich durch unzureichende IKT-Sicherheit ergeben kann, ist jedoch nicht automatisch eine Garantie für die Entwicklung einer entsprechenden Sicherheitsstrategie. Die konsequente Umsetzung und kontinuierliche Verbesserung entsprechender technischer und organisatorischer Maßnahmen wird künftig von zentraler Bedeutung sein.

Während das Bewusstsein für die technischen Aspekte der IKT-Sicherheit und die Grenzen der Kompetenz im eigenen Unternehmen vorhanden ist, wurde ein ähnlich ausgeprägtes Interesse bei Aspekten, die dem institutionellen Umgang mit der IKT-Sicherheit und deren organisatorischer Umsetzung zuzuordnen sind, nicht immer festgestellt. Dies ist von erheblicher Bedeutung. Es lässt sich zeigen, dass diesen Aspekten bei der Sicherstellung der IKT-Sicherheit eine maßgebliche Bedeutung zukommt. Vor allem auf operativer Ebene wurde eine signifikante Anzahl von technischen und organisatorischen Schwachstellen identifiziert, die unmittelbar auf den inkonsequenten institutionellen Umgang mit der IKT-Sicherheit zurückzuführen waren.

Um die Bedeutung strikter Richtlinien und besonderer Schutzmaßnahmen im operativen Umgang mit der IKT zu verdeutlichen, erwies es sich bei den Interviews als besonders zweckmäßig, dem Betriebspersonal vor Augen zu führen, dass sich die Netzwerke im Rahmen eines steuernden Fernzugriffs

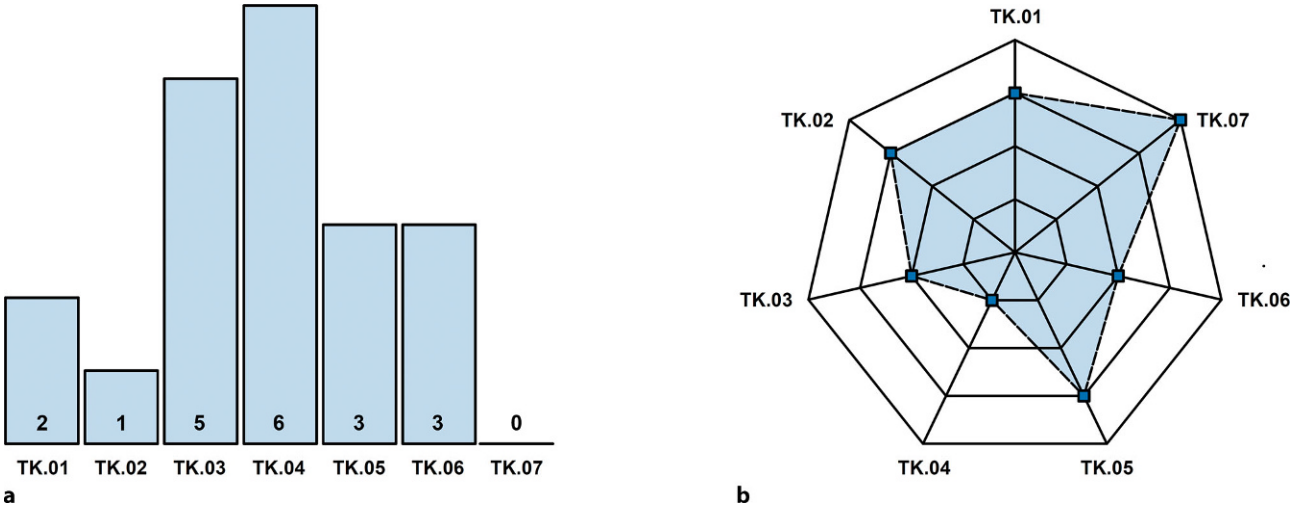

Abb. 2 Exemplarische Darstellung der Schwachstellen (**a**) und der endgültigen Sicherheitsniveaus (**b**) eines fiktiven Unternehmens für die Themenkomplexe TK.01 bis TK.07

von zum Teil sehr gut gesicherten, zentralen Anlagenteilen, mitunter bis in das private Wohnzimmer erstrecken. Die Reaktionen auf dieses Szenario verdeutlichten den zentralen Aspekt des operativen Anlagenbetriebs: das permanente Spannungsfeld zwischen möglichst einfacher Handhabung der OT und der Ausgestaltung technischer Systeme mit einem höchstmöglichen Niveau an IKT-Sicherheit. Problematisch ist in diesem Bereich das zum Teil wenig ausgeprägte, institutionelle Bewusstsein für organisatorische Strukturen und der Umgang mit der Thematik als Teil der Unternehmenskultur. So wurde zum Teil ein *falsches Sicherheitsgefühl* bei Anlagenverantwortlichen und Betriebspersonal sowie eine gewisse, aus der täglichen Routine resultierende Nachlässigkeit oder auch *Betriebsblindheit* festgestellt.

Das falsche Sicherheitsgefühl beruht im Bereich der WVU in vielen Fällen auf der redundanten Gestaltung von Wasserversorgungsanlagen und der Annahme, dass Attacken auf die OT unwahrscheinlicher und ungleich schwieriger seinen als andere Wege, den Anlagenbetrieb zu stören. Zusätzlich sind Anlagen und OT von WVU und ARA so gestaltet, dass Subsysteme bei einem Ausfall der zentralen Steuerung, sofern die Stromversorgung erhalten bleibt, im Inselbetrieb weiterlaufen oder durch manuelle Steuerung betrieben werden können, bis zum Regelbetrieb zurückgekehrt werden kann. Auch die durchgeführten Wirkungsanalysen haben gezeigt, dass für gezielte Cyberangriffe auf ein WVU neben umfangreichen IKT- und vor allem OT-Kenntnissen meist ein detailliertes Wissen über Betrieb und Aufbau der individuellen Wasserversorgungsanlagen erforderlich ist, um diese mit einer Cyberattacke langfristig und großflächig zu stören. Dieser Aspekt wird mit dem Begriff *Defense-in-Depth* zusammenfasst und ist grundsätzlich ein Zeichen einer guten Sicherheitsarchitektur. Problematisch ist in diesem Zusammenhang jedoch zum einen, dass durch das vermeintliche Wissen um die resilienten Anlagen Gefährdungen durch ungezielte, systematische Attacken und unbewusste bzw. unbeabsichtigte Eingriffe oder Bedienfehler oft nicht berücksichtigt werden. Zum anderen birgt das falsche Sicherheitsgefühl unter Umständen das Risiko einer institutionellen Betriebsblindheit, die zu technischen und organisatorischen Schwachstellen bei den IKT-Systemen führt.

In vielen Fällen existieren Wechselwirkungen zwischen institutionellen, organisatorischen und technischen Aspekten der IKT-Sicherheit. So ließ sich ein erheblicher Teil der identifizierten technischen Schwachstellen auf Unachtsamkeit, Fehlkonfigurationen oder den Einsatz veralteter oder anfälliger Komponenten zurückführen. Daneben wurde im Bereich der WVU eine Reihe technischer Schwachstellen auf eine nicht eindeutige oder unklare Beauftragung von Mitarbeitern oder Dienstleistern, häufig in Kombination mit einer unzureichenden Dokumentation, zurückgeführt. Sicherheitsmaßnahmen werden teilweise aus Komfortgründen, beispielsweise beim Einsatz von Technologien für Fernzugriffen auf die OT, unbewusst oder auch bewusst umgangen. Das Spannungsfeld Komfort und Sicherheit wurde besonders in diesen Fällen evident.

Im Bereich der ARA wurde auf bislang wenig bekannt gewordene Angriffe hingewiesen, wobei sich das vorhandene Bewusstsein für Gefährdungen, vor allem im Bereich ungezielter Angriffe, zum Teil als ausbaufähig erwies. Obwohl bei Ausfall zentraler IKT-Systeme eine manuelle Anlagensteuerung zumindest möglich ist, sind ein geordneter Betrieb und die Einhaltung der üblichen Ablaufgrenzwerte in diesem Betriebsmodus nicht auf Dauer zu gewährleisten. Ähnlich dem Befund im Bereich der WVU ist ein guter Teil realer Gefährdungen dem zugestandenen Komfort im Rahmen des üblichen Betriebs geschuldet. In diesem Kontext sind auch bei den ARA OT-Eingriffe, teils als Fernzugriffe und mit hinterlegtem und bereits vorausgefülltem Kennwort zu nennen. Prinzipiell sind technische Lösungen für Fernzugriffe, die grundsätzliche Sicherheitsvorkehrungen, auch bei gegenüber Netzwerkzugriffen von außen ansonsten restriktiven Systemen, wirksam umgehen können, besonders hervorzuheben. Diese Technologien und deren Einsatz sind vor allem in jenen Fällen kritisch zu bewerten, wo die IT- und OT-Netzwerke durch unzureichende Zonierung nicht hinreichend gut voneinander getrennt sind.

Der organisatorische Aufwand für die Sicherung der IKT-Systeme der ARA ist dem technischen mindestens

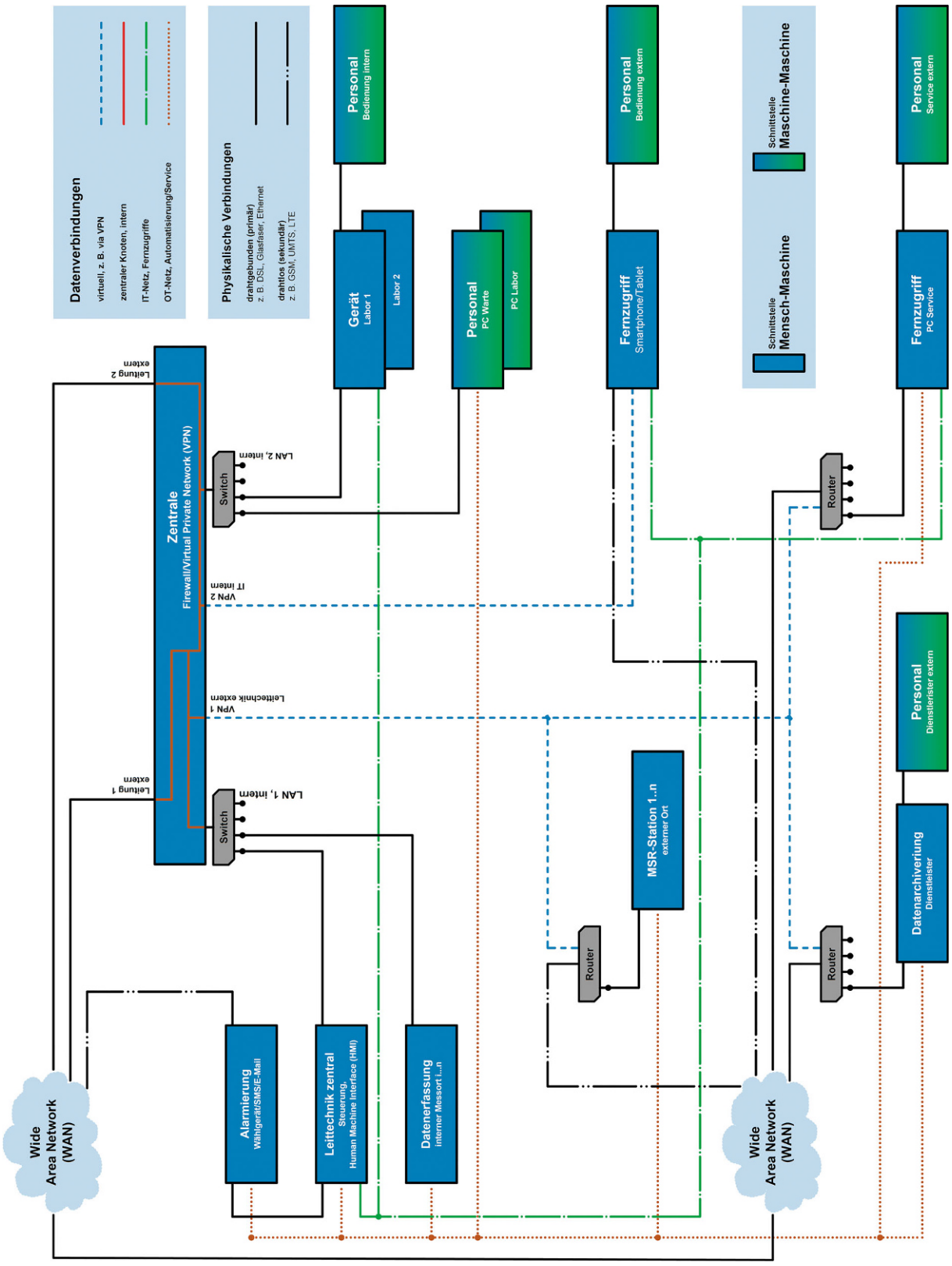

Abb. 3 Typische Anlage der Siedlungswasserwirtschaft, repräsentiert mittels festgelegter Standardbausteine

ebenbürtig. Aus Betreibersicht wird diesbezüglich Fragen nach Kosten und fachlicher Zuständigkeit die größte Relevanz zugemessen. Das Halten eines einmalig erreichten, guten Sicherheitsniveaus und der Ausstattung am Stand der Technik über den gesamten Lebenszyklus der Anlagen hinweg ist im Regelfall nur durch langfristige, fachliche Betreuung realisierbar.

3.2 Umgang mit der IKT-Sicherheit

Bei den untersuchten WVU wird eine große Bandbreite verschiedener IKT-Systeme und zugehöriger Betriebskonzepte eingesetzt. Bei der OT befinden sich in der Wasserversorgung neben selbst entwickelten Systemen auch Systeme diverser regionaler, nationaler und internationaler Anbieter im Einsatz. Die Art der Wassergewinnung, die Wasserqualität sowie die Topgrafie und Größe des Versorgungsgebiets beeinflussen den Aufbau der oft weitläufigen Wasserversorgungssysteme mit einer Vielzahl an Anlagenstandorten und damit die eingesetzte OT und Kommunikationstechnologie maßgeblich. Die OT der untersuchten ARA ist meist direkt auf der Kläranlage konzentriert. Anlagen im Kanalnetz, wie Pumpwerke oder aktivierbare Speicher- und Stauräume, sind über Datenübertragungsstrecken eingebunden und unter dem Gesichtspunkt etablierter IKT-Sicherheit besonders relevant. Bei der IT verwenden WVU und ARA gleichermaßen Komponenten und Systeme unterschiedlicher Hersteller.

Art und Größe des Unternehmens und damit in der Regel Budget, Personalstand und -qualifikation, spielen zentrale Rollen beim Umgang mit den IKT-Systemen. Wesentliche Unterschiede bestanden bei Ausschreibung, Anschaffung und Betrieb dieser Systeme. Bei Mehrspartenunternehmen und größeren Unternehmen im Allgemeinen ist meist eigenes, geschultes Personal oder entsprechende Abteilungen während des gesamten Lebenszyklus, von der Anschaffung bis zur Ausscheidung, für die IKT-Systeme verantwortlich. Bei kleineren und mittleren Unternehmen werden diese Aufgaben häufig in Zusammenarbeit von eigenem Personal, Anlagenherstellern oder externen Dienstleistern gehandhabt. Daneben werden in Fällen, wo kein geeignetes Personal verfügbar ist, Systeme eingesetzt, bei denen die OT teilweise oder komplett von Herstellern oder Dienstleistern betrieben und beispielsweise über mit Webbrowsern erreichbare Bedienoberflächen gesteuert wird.

Die historisch vielfach vorhandene und auch nach tiefgreifenden Systemadaptierungen noch als solche wahrgenommene *Kapselung* der OT, also deren vollständige, physische Trennung von allen anderen Netzwerken, wurde bei keinem Unternehmen festgestellt. Entsprechend hohe Bedeutung ist der Implementierung, Konfiguration und Betreuung der eingesetzten logischen Netzwerktrennung im Sinne einer Segmentierung beizumessen. WVU und ARA sichern sich die dafür erforderliche Fachkenntnis durch Qualifikation und kontinuierliche Fortbildung des eigenen Personals oder über Rahmenverträge mit OT-Herstellern und IKT-Dienstleistern.

Die Integrität von Sicherheitsarchitektur und Netzwerktrennung wird in den meisten Fällen zwar laufend evaluiert und es werden sicherheitsrelevante Updates durchgeführt, regelmäßige Audits durch Dritte finden bislang aber in den wenigsten Fällen statt. Audits und Prüfungen sind vor allem in jenen Fällen von hoher Bedeutung, in denen die Anlagenbetreuung von OT und IT durch eine einzelne Person bestritten wird. In Kombination mit unzureichender Dokumentation birgt die Konzentration des IKT-Betriebs auf eine Person eine signifikante Gefährdung der Kontinuität der IKT-Sicherheit, beispielsweise bei einem plötzlichen Ausscheiden der Person aus dem Unternehmen. Aus diesem Grund erachteten sämtliche betroffene Unternehmen unter den Studienteilnehmern den Aufbau personeller und fachlicher Redundanzen sowie einer entsprechenden, nachvollziehbaren Dokumentation als wesentlich und hatten damit meist bereits begonnen.

Bei der Nutzung der IKT-Systeme durch das Betriebspersonal über zentrale Leitwarten, Terminals in Außenanlagen und mobile Geräte gab es weitgehende Parallelen zwischen WVU und ARA. So sind z. B. Fernzugriffe auf die OT über mobile Geräte heute für Betriebspersonal und im Speziellen für Bereitschaftsdienste der gesamten Siedlungswasserwirtschaft Stand der Technik.

Trotz des weithin hohen Sicherheitsstandards gab es bei den meisten Unternehmen Verbesserungspotenzial im operativen Umgang mit IT und OT. Neben technischen Schwachstellen, die nicht selten ein Spezifikum einzelner Anlagen oder Unternehmen waren, wurde vielfach eine Reihe von organisatorischen Aspekten identifiziert, die besonderer Beachtung bedürfen.

Die durchgeführten Analysen zeigen deutlich, dass es zur Sicherstellung der IKT-Sicherheit eines kontinuierlichen Verbesserungsprozesses bedarf, der diese strategisch und operativ sicherstellt und eine laufende Evaluierung mit regelmäßigen Audits vorsieht. Die Umsetzung von organisatorischen und technischen Maßnahmen, die zu einem bestimmten Zeitpunkt dem jeweils aktuellen Stand der Technik entsprechen, können die IKT-Sicherheit von Anlagen und Komponenten nur temporär und nicht über deren gesamte Lebensdauer sicherstellen. Beispielhaft sei hier das Bekanntwerden eines erfolgreichen Angriffs gegen eine etablierte Verschlüsselungstechnologie genannt. Ab dem Zeitpunkt des Bekanntwerdens müssen Systeme, deren Sicherheitsarchitektur auf dem nunmehr schwachen Algorithmus aufbaut, als nicht mehr hinreichend sicher und angreifbar angesehen werden. Ein dementsprechendes Verständnis muss in den Unternehmen als wesentlicher Teil der institutionellen IKT-Sicherheit etabliert und dem gesamten Personal dementsprechend kommuniziert werden. Nur so kann Betriebsblindheit und routine- oder komfortbedingten Schwachstellen konsequent vorgebeugt werden.

Eine signifikante, komfortbedingte Schwachstelle stellt das unzureichende Management von Zugriffsberechtigungen auf die OT, meist in Kombination mit der Verwendung von mobilen privaten oder dienstlichen Geräten, dar. Berechtigungen für OT-Zugriffe sollten restriktiv nach betrieblichen Erfordernissen vergeben und entzogen werden. Mehrere, hierarchisch gegliederte und separat gesicherte Zugriffsebenen mit unterschiedlichen Bedienrechten sind vorzusehen. Typischerweise kann es erforderlich sein, dass ein größerer Personenkreis Einblick in den Betrieb der OT haben muss, aber lediglich ein Teil davon auch die Berechtigung benötigt, steuernd einzugreifen.

Ähnlich wie bei der Handhabung von Anlagenzutritten sind auch bei OT-Zugriffen ein möglichst hoher Authentifizierungsstandard, eine laufende (automatisierte) Dokumentation der Zugriffe und eine Alarmierung bei Anomalien erforderlich. Eine laufende Evaluierung der Zugriffsprotokolle sollte durchgeführt werden. Berechtigungen

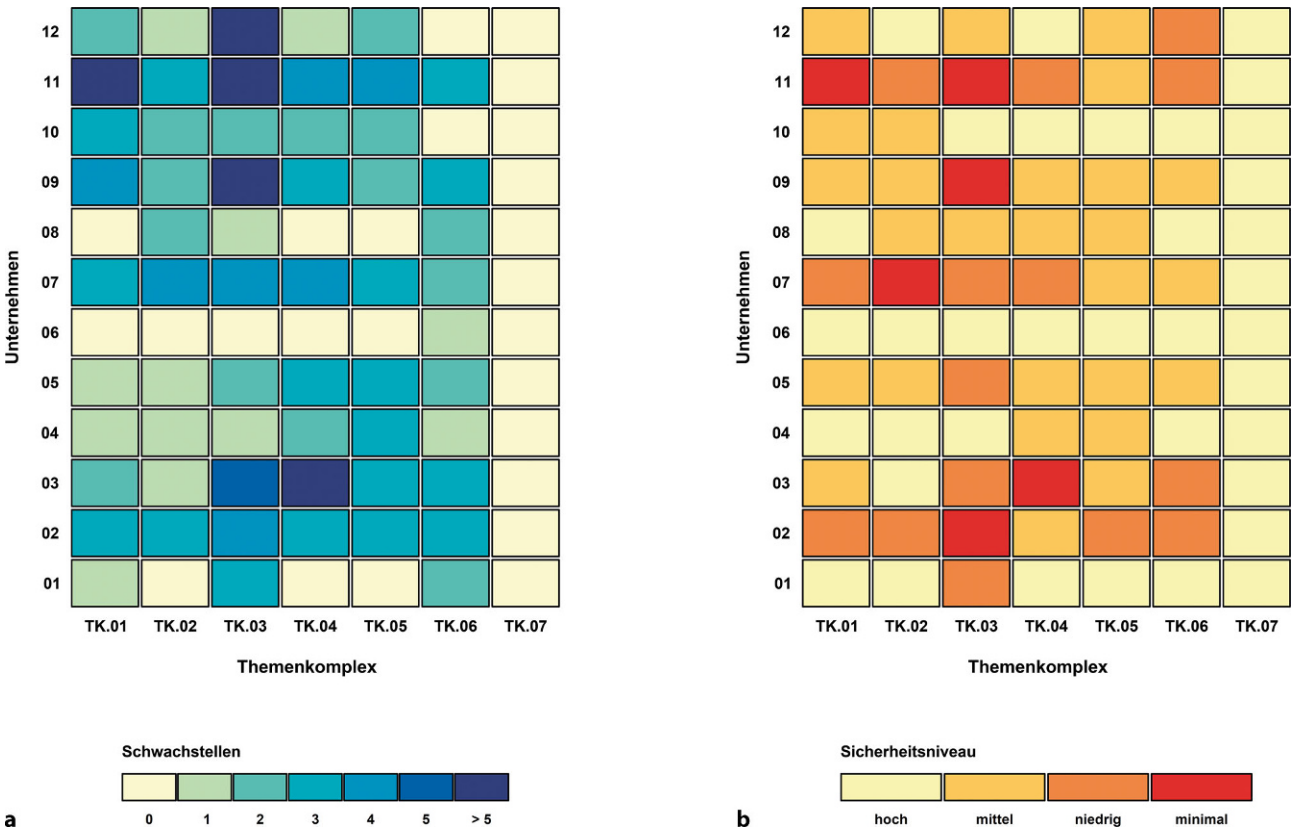

Abb. 4 Schwachstellen (**a**) und Sicherheitsniveaus (**b**) der untersuchten Unternehmen

an Dritte sollten nur eingeschränkt und temporär vergeben werden und immer, zumindest durch Zeitablauf, automatisch erlöschen. Auch bei adäquat gesicherten Verbindungen und hohem Authentifizierungsstandard können Fernzugriffe bei der Verwendung bestimmter Software die Konfiguration von Firewalls umgehen. Dies wird im Besonderen bei mehrfach geteilten oder permanent in Anmeldemasken hinterlegten Zugangsdaten als kritisch erachtet. Erschwerend kommt hinzu, dass diese Zugriffe teilweise von ungesicherten Privatgeräten erfolgten.

Besonders bei unzureichendem Schutz für den Zugriff auf die OT kommt der physischen Anlagensicherheit bzw. dem Perimeter- und Objektschutz eine zentrale Rolle bei der Verhinderung unberechtigter Eingriffe in die OT zu. Kernpunkte der physischen Anlagensicherheit sind dabei klare, aufgabenspezifische Hierarchien bei Zutrittsberechtigungen. Diese Berechtigungen sollten regelmäßig auditiert, gegebenenfalls adaptiert und an Dritte nur temporär vergeben werden. Beim Zutrittsmanagement ist auf die Implementierung einer automatischen Dokumentation aller Aktivitäten und Alarmierung im Fall von Anomalien zu achten.

Im Allgemeinen hat sich gezeigt, dass bei allen Unternehmen künftig ein verstärkter Fokus auf das Erlöschen von Berechtigungen – sowohl für Zugriffe als auch für Zutritte – für Dritte und beim Ausscheiden von Personen aus den Unternehmen gelegt werden muss.

4 Zusammenfassung und Schlussfolgerungen

Die Ergebnisse der durchgeführten Studie legen nahe, dass sich die IKT-Sicherheit in der österreichischen Siedlungswasserwirtschaft in einem Spannungsfeld zwischen einfacher Handhabbarkeit und wirtschaftlichen Zwängen einerseits, sowie höchstmöglicher Sicherheit und deren kontinuierlicher Verbesserung andererseits, befindet. Den Vorteilen einer zunehmenden Vernetzung von IT und OT steht der Umstand gegenüber, dass sich dadurch zusätzliche und neue, potenzielle Schwachstellen ergeben.

In Abb. 4 findet sich eine Visualisierung der zusammengefassten, anonymisierten Ergebnisse der Schwachstellenanalyse für die untersuchte Gruppe von WVU und ARA. Die Verteilung der Schwachstellen auf die einzelnen Themenkomplexe (Abb. 4a) zeigt, dass bei allen Unternehmen Schwachstellen festgestellt wurden. Im Mittel wurden zwei bis drei Schwachstellen pro Themenkomplex identifiziert, lediglich in Einzelfällen belief sich deren Anzahl auf mehr als fünf. Bei den Sicherheitsniveaus (Abb. 4b), für deren Ableitung neben Anzahl und Schwere der Schwachstellen eines Themenkomplexes unter anderem individuelle Anlagenstrukturen, technische, finanzielle und personelle Möglichkeiten eines Betriebs berücksichtigt wurden, sind hohe und mittlere Sicherheitsniveaus dominant. Nur in wenigen Fällen wurden niedrige oder sogar minimale Sicherheitsniveaus abgeleitet, wobei die Ursache dafür meist in einer Kombination aus institutioneller Nachlässigkeit, inkonsequentem operativen Umgang und signifikanten technischen Schwachstellen lag. Abb. 4 unterstreicht, dass es – obwohl der Großteil der Unternehmen

zum Zeitpunkt der Analysen für die Mehrheit der Themenkomplexe einen durchwegs guten Standard der IKT-Sicherheit aufwies – in fast allen Punkten Verbesserungsbedarf gab.

Um den Anlagenbetreibern den Umfang dieses Verbesserungsbedarfs und die möglichen Konsequenzen unzureichender IKT-Sicherheit zu kommunizieren, erwies sich eine Diskussion der identifizierten Schwachstellen im Kontext realer Gefährdungen und deren potenzieller Wirkung auf ihre individuellen Anlagen als besonders zweckdienlich.

Dabei hat sich gezeigt, dass sich die Verantwortlichen in der Siedlungswasserwirtschaft der kontinuierlichen Änderung der Bedrohungslage und der sich weiterentwickelnden Gefährdungen für ihre IKT-Systeme grundsätzlich bewusst sind und versuchen entsprechend zu agieren. Die Systemsicherheit von IT und OT wird in die strategische Planung einbezogen und es werden gezielt Finanzmittel dafür vorgesehen. Fachliche Kompetenzen und Aufgabenbereiche werden klar definiert und bei Bedarf externe Dienstleister oder Anlagenhersteller involviert. Einige der analysierten Unternehmen entwickeln zurzeit eine Kultur der institutionellen IKT-Sicherheit, indem sie interne Richtlinien und Checklisten für Personen erarbeiten, die mit dem Anlagenbetrieb betraut sind. Im Idealfall werden zusätzlich Schulungen für das gesamte Personal angeboten, um dieses für IKT-Gefährdungen zu sensibilisieren und laufend über entsprechende Risiken zu informieren. Mittels Ausbildung und Information soll das teilweise vorhandene, falsche Sicherheitsgefühl, also die weitverbreitete Annahme, dass sämtliche Anlagen der Siedlungswasserwirtschaft resilient genug seien und ohnehin keine langfristigen oder weitläufigen Störungen auftreten werden, abgebaut werden.

Verbesserungsbedarf gibt es in der Branche bei der konsequenten Umsetzung von Dokumentation, Evaluierung und regelmäßigen Audits der IKT-Sicherheitsarchitektur sowie bei Berechtigungen für Anlagenzutritte und IKT-Zugriffe. So werden aus Gründen der vermeintlich einfacheren Handhabung beispielsweise Schlüssel und Zugangscodes geteilt oder bei Fernzugriffen auf die OT Privatgeräte mit unzureichend oder falsch konfigurierter Software verwendet. Eine konsequente Umsetzung dieser Maßnahmen würde die Zahl der Schwachstellen in Abb. 4 merklich reduzieren und die Sicherheitsniveaus entsprechend erhöhen.

Übergeordnetes Ziel muss sein, IKT-Sicherheit als kontinuierlichen Verbesserungsprozess unter geeigneter fachlicher Betreuung über die gesamte Lebensdauer der Anlagen der IT und OT aufrechtzuerhalten. Um dies auch künftig gewährleisten zu können, ist ein Teil der Studienteilnehmer gerade dabei, veraltete OT-Systeme und deren Komponenten, für die keine Ersatzteile oder Sicherheitsupdates mehr verfügbar sind, auszutauschen. Da gerade in diesem Zusammenhang Kosten und nachhaltige Planung eine große Rolle spielen, äußerten alle teilnehmenden WVU und ARA Interesse an einem IKT-Branchenleitfaden für die Siedlungswasserwirtschaft, der neben klar formulierten Mindeststandards auch Hilfe bei Ausschreibung und Vergabe sowie Anleitungen zur Etablierung und Sicherstellung eines sicheren, laufenden Betriebs enthält.

Für eine branchenweite Umsetzung von handhabbaren IKT-Standards, die sinnvoll auf die hochgradig individuellen Anlagen der österreichischen Siedlungswasserwirtschaft angewendet werden können, wird eine gemeinsame Betrachtung von WVU und ARA sowie eine Zusammenarbeit mit Forschungseinrichtungen, Behörden und Branchenverbänden als notwendig erachtet, um sich laufend ändernden Bedrohungslagen effektiv und effizient stellen zu können.

Danksagung Der besondere Dank der AutorInnen gilt den Wasserversorgungs- und Abwasserreinigungsunternehmen, die umfassenden Einblick in ihre Anlagen, Organisation und internen Abläufe gewährt haben. Darüber hinaus danken die Autoren dem Bundesministerium für Nachhaltigkeit und Tourismus (BMNT) für die finanzielle Unterstützung, die diesen umfassenden Einblick möglich gemacht hat.

Funding Open access funding provided by Graz University of Technology.

Literatur

Alcaraz, C. & Zeadally, S. (2015): Critical infrastructure protection: Requirements and challenges for the 21st century. International Journal of Critical Infrastructure Protection, **8**, 53–66.

AWWA, American Water Works Association (2017): Process Control System Security Guidance for the Water Sector.

Assmann, M., Dürr, K., Haberfellner-Veit, E., Laber, J., Lindtner, S., & Tschiesche, U. (2016): Branchenbild der österreichischen Abwasserwirtschaft 2016, Österreichischer Wasser- und Abfallwirtschaftsverband (ÖWAV), Wien.

BSI, Bundesamt für Sicherheit in der Informationstechnik (2008): BSI-Standard 100-4, Notfallmanagement.

BSI, Bundesamt für Sicherheit in der Informationstechnik (2017a): BSI-Standard 200-1, Managementsysteme für Informationssicherheit (ISMS).

BSI, Bundesamt für Sicherheit in der Informationstechnik (2017b): BSI-Standard 200–2, IT-Grundschutz-Methodik.

BSI, Bundesamt für Sicherheit in der Informationstechnik (2017c): BSI-Standard 200–3, Risikoanalyse auf der Basis von IT-Grundschutz.

Bundeskanzleramt der Republik Österreich (2015): Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP) – Masterplan 2014.

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz-und Informationssystemsicherheitsgesetz – NISG), BGBl. I Nr. 111/2018 (2018) [online] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536.

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017): Protecting Drinking Water Utilities From Cyberthreats. Journal – American Water Works Association, **109**, 50–58.

Cyber Sicherheit Steuerungsgruppe (2018): Bericht Cyber Sicherheit 2018, Wien.

DWA, Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (2017): Merkblatt DWA-M 1060 – IT-Sicherheit – Branchenstandard Wasser/Abwasser.

EPA, Environmental Protection Agency (2016): Water Sector Cybersecurity Brief For States.

Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates (2016): Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

Fluchs, S. (2017a): Erstellung eines IT-Grundschutz-Profils für ein Referenzunternehmen (kleines/mittelständisches Unternehmen, KMU) mit automatisierter Prozesssteuerung (Indus-

trial Control System, ICS) Oder: ICS-Security für kleine Unternehmen machbar machen (Research Group IT-Security, RWTH Aachen, Hrsg.), [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/Fluchs_MA_Profil.pdf?__blob=publicationFile&v=2 (Zugegriffen 7. November 2018).

Fluchs, S. (2017b): IT-Grundschutz-Pilotprofil bzw. IT-Grundschutz-Profil für die Wasserwirtschaft (Bundesamt für Sicherheit in der Informationstechnik, Hrsg.)

Gartner (2018a): IT Glossary: IT (information technology), [online] https://www.gartner.com/it-glossary/it-information-technology/ (Zugegriffen 7. November 2018).

Gartner (2018b): IT Glossary: Operational Technology (OT), [online] https://www.gartner.com/it-glossary/operational-technology-ot/ (Zugegriffen 7. November 2018).

Graham, J. H., Hieb, J. L., & Foreman, J. C. (2012): Mapping Water Sector Cyber-Security Vulnerabilities. CERITAS Tech Report 2012–15.

Lachance, L. (2018): IT vs. OT für das Industrielle Internet – Zwei Seiten einer Medaille?, [online] https://www.globalsign.com/de-de/blog/it-vs-ot-im-industriellen-internet/ (Zugegriffen 7. November 2018).

Luiijf, E., Ali, M., & Zielstra, A. (2011): Assessing and improving SCADA security in the Dutch drinking water sector. International Journal of Critical Infrastructure Protection, **4**(3–4), 124–134.

Manalo, C., Noble, T., Miller, K., & Ferro, C. (2015): Control Systems Cybersecurity: Lessons Learned From Virginia Assessments. Journal – American Water Works Association, **107**(12). [online] http://doi.wiley.com/10.5942/jawwa.2015.107.0174 (Zugegriffen 25. April 2018).

Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., & Reddi, R. (2011): A control system testbed to validate critical infrastructure protection concepts. International Journal of Critical Infrastructure Protection, **4**(2), 88–103.

Nazir, S., Patel, S., & Patel, D. (2017): Assessing and augmenting SCADA cyber security: A survey of techniques. Computers & Security, **70**, 436–454.

Noble, T., Manalo, C., Miller, K., & Ferro, C. (2017): Cybersecurity Assessments of 30 Drinking Water Utilities.

ÖVGW, Österreichische Vereinigung für das Gas- und Wasserfach (2018): Die österreichische Trinkwasserwirtschaft – Branchendaten und Fakten, Österreichische Vereinigung für das Gas- und Wasserfach, Wien.

Panguluri, S., Phillips, W., & Cusimano, J. (2011): Protecting water and wastewater infrastructure from cyber attacks. Frontiers of Earth Science. [online] http://link.springer.com/10.1007/s11707-011-0199-5 (Zugegriffen 25. April 2018).

Papa, S., Casper, W., & Moore, T. (2013): Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis. International Journal of Critical Infrastructure Protection, **6**(2), 96–106.

Pointl, M., Winkelbauer, A., Krampe, J., & Fuchs-Hanusch, D. (2018): Sicherheit von Informations- und Kommunikationssystemen in der österreichischen Siedlungswasserwirtschaft, Graz.

Rao, V. M. & Francis, R. A. (2015): Critical review of cybersecurity protection procedures and practice in water distribution systems. Proceedings of the 2015 Industrial and Systems Engineering Research Conference.

Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017): Characterizing Cyber-Physical Attacks on Water Distribution Systems. Journal of Water Resources Planning and Management, **143**(5), 04017009.

WaterISAC Security Information Center (2015): 10 Basic Cybersecurity Measures.