Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 d Ausgabe März 2019

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Wasserversorgung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für wirtschaftliche Landesversorgung BWL
Geschäftsstelle IKT

SVGW, Grütlistrasse 44, Postfach 2110, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch

Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 d Ausgabe März 2019

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie (IKT) in der Wasserversorgung

IMPRESSUM

Bezug bei der Geschäftsstelle des SVGW
(support@svgw.ch)

SVGW, Grütlistrasse 44, Postfach 2110, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch

Impressum

Herausgeber

Schweizerischer Verein des Gas- und Wasserfaches (SVGW)
Bundesamt für wirtschaftliche Landesversorgung (BWL)

Autoren der Erstausgabe

Name	Vorname	Organisation	Funktion
Walder	Dario	BWL	Hauptautor/Projektleitung
Schenker	Silvan	BWL	Co-Autor/Stellvertretender Projektleiter
Olschewski	André	SVGW	Auftraggeber SVGW/Fachexperte/ Informationslieferant/Quality Assurance
Domeniconi	Raffaele	SVGW	Fachexperte/Informationslieferant/Quality Assurance
Carusone	Raffael	Energie Thun AG	Fachexperte/Informationslieferant/Quality Assurance
Garcia	Manuel	SIG	Fachexperte/Informationslieferant/Quality Assurance
Kasme	Samir	SIG	Fachexperte/Informationslieferant/Quality Assurance
Kegele	Karl	WWZ AG	Fachexperte/Informationslieferant/Quality Assurance
Maître	Nathalie	ESB	Fachexpertin/Informationslieferantin/Quality Assurance
Matt	Georg	WV Liechtensteiner Unterland e.G.	Fachexperte/Informationslieferant/Quality Assurance
Rickenbacher	Andreas	IWB	Fachexperte/Informationslieferant/Quality Assurance
Romano	Roberto	EW Rothrist AG	Fachexperte/Informationslieferant/Quality Assurance
Stöckli	Markus	Energie Thun AG	Fachexperte/Informationslieferant/Quality Assurance
Weyermann	Thomas	SWG	Fachexperte/Informationslieferant/Quality Assurance
Zberg	Leo	WV Sarnen	Fachexperte/Informationslieferant/Quality Assurance

Chronologie

Datum	Kurzbeschreibung
2016	Durchführung IKT-Verwundbarkeitsanalyse der Wasserversorgung
Oktober 2017	Erste Besprechung betreffend IKT-Minimalstandard zwischen BWL und SVGW
Dezember 2017	Erste Vorbesprechung der Kick-off-Sitzung
Januar 2018	Zweite Vorbesprechung der Kick-off-Sitzung
Januar 2018	Arbeitsaufnahme des Projektteams (Kick-off)
Februar 2018	Besprechung kommentiertes Inhaltsverzeichnis
März 2018	Review Entwurf durch die Fachexperten
April 2018	Zweites Review Entwurf & Abnahme durch Fachexperten
Mai 2018	Übersetzung ins Französische
Mai 2015	Vernehmlassung durch SVGW, Hauptkommission beauftragt
Mai bis August 2018	Vernehmlassung durch SVGW & Erarbeitung Umsetzungsbeispiele
Dezember 2018	Veröffentlichung des IKT-Minimalstandards für die Wasserversorgung

Das Dokument wurde unter Einbezug und Mithilfe des Bundesamtes für wirtschaftliche Landesversorgung, des Schweizerischen Verein des Gas- und Wasserfaches sowie Fachexpertinnen und Fachexperten der Wasserversorgung erarbeitet.

INHALTSVERZEICHNIS

VORWORT

Die zunehmende Durchdringung und Vernetzung der Informations- und Kommunikationstechnologie (IKT) in allen Lebensbereichen eröffnet ökonomische wie gesellschaftliche Potenziale, auf die ein hochentwickeltes und industrialisiertes Land wie die Schweiz nicht verzichten kann. Gleichzeitig entstehen durch die fortschreitende Digitalisierung neue Gefährdungslagen, auf die schnell und konsequent reagiert werden muss. Die besondere Gefahr durch gezielte Cyber-Angriffe auf die IT-Infrastruktur oder Fehlfunktionen und -manipulationen versorgungsrelevanter IKT-Systeme betrifft staatliche Stellen ebenso wie Betreiber kritischer Infrastrukturen und weitere Unternehmen, die mit besonders wertvollen Informationen umgehen.

Der IKT-Minimalstandard setzt dort an, wo sich eine moderne Gesellschaft Ausfälle nicht leisten kann: bei den IKT-Systemen der Wasserversorger. Wasser als lebensnotwendiges Gut muss unsere vollste Aufmerksamkeit erhalten. Nicht nur die Qualität, sondern auch die Verfügbarkeit des kostbaren Nasses sind essentiell, dies gehört schliesslich zum Verfassungsauftrag der WL. Deshalb bin ich froh, dass die WL gemeinsam mit dem Fachverband (SVGW) sowie Vertretern der Wasserversorgung mit dem vorliegenden Branchenstandard einen Beitrag zur Erhöhung der Widerstandsfähigkeit der Wasserversorgung leisten kann.

Der IKT-Minimalstandard wird von der WL gemeinsam mit dem SVGW als Minimalsicherheitsniveau in der IKT empfohlen. Der Rückhalt dieses Standards in der Branche ist für die WL von grösster Wichtigkeit. Daher bevorzugt die wirtschaftliche Landesversorgung die enge Zusammenarbeit mit der Branche und dem Branchenverband und sucht nicht wie in anderen Ländern eine zentralistische Lösung.

Werner Meier,
Delegierter für wirtschaftliche
Landesversorgung

Cyber Security ist nun auch in der Schweiz als wichtige Aufgabe bei der kritischen Infrastruktur «Trinkwasserversorgung» erkannt worden. Beachtet werden sollten nicht nur der sorgsame Umgang mit Passwörtern bei der Büro-IT, sondern auch der Schutz der SCADA-Systeme oder Schnittstellen mit Nachbarsystemen. Cyber Security ist nicht nur ein «Muss» für grosse Werke, die als Querverbundunternehmen besonders exponiert sind. Auch kleine Werke sollen sich schützen, da auch sie oft komplizierte Anlagen bewirtschaften, um die Bevölkerung und Wirtschaft sicher mit Trinkwasser versorgen zu können.

Diese Branchenempfehlung (IKT-Minimalstandard) wurde gemeinsam durch das Bundesamt für wirtschaftliche Landesversorgung und den Schweizerischen Verein des Gas- und Wasserfaches für die Trinkwasser-versorgungen erarbeitet. Diese Zusammenarbeit stellte die branchenübergreifend einheitliche Methodik mit all ihren Synergien sicher.

Die Branchenempfehlung ist skalierbar aufgebaut, d.h. sie unterstützt sowohl grosse Versorger als in pragmatischer Weise auch mittlere und kleinere Versorgungen. Für die hervorragende Zusammenarbeit mit dem BWL und die hohe Qualität des Produktes möchten wir allen Beteiligten ganz herzlich danken. Wir hoffen, dass die Empfehlung von möglichst vielen Versorgungen rasch umgesetzt wird, so dass das Niveau hinsichtlich Cyber Security mit sinnvollem Aufwand massgeblich gesteigert werden kann. Gerne unterstützt der SVGW die Versorgungen bei dieser Aufgabe mit spezifischen Ausbildungsangeboten.

Markus Küng
Präsident Schweizerischer Verein des
Gas- und Wasserfaches

ZUSAMMENFASSUNG

Die fortschreitende Digitalisierung und Professionalisierung in der Wasserversorgung erhöhen gleichermassen die Effizienz für die Aufbereitung und Verteilung von Trinkwasser, wie auch den Grad der Abhängigkeit von IKT-Systemen. Wasserversorger verwenden beispielsweise für die Steuerung der Aufbereitung und Verteilung des Wassers IKT-basierte Prozessleitsysteme (SCADA[1] - Systeme).

SCADA-Systeme sind ein integraler Bestandteil kritischer Infrastrukturen, die den Betrieb von Unternehmen in wichtigen Branchen wie der Wasserversorgung, aber auch der Strom-, Öl- und Gasversorgung, der Logistik usw. erleichtern. Die zunehmende Bedeutung hinsichtlich ausreichender Cyber-Sicherheit solch kritischer IKT-Systeme ist offensichtlich. Eine effiziente Bewältigung der Cyber-Sicherheitsprobleme erfordert ein klares Verständnis der aktuellen Sicherheitsherausforderungen sowie der verfügbaren Gegenmassnahmen.

Vorliegender IKT-Minimalstandard bietet ein Rahmenwerk, damit sich die Wasserversorger auf einem angemessenen Sicherheitsniveau gegen Angriffe sowie Fehlmanipulationen schützen und sich nach einem Vorfall möglichst rasch wieder erholen können. Dabei stufen Unternehmen ihr Risiko selbständig ein und setzen entsprechende Massnahmen um.

Der vorliegende IKT-Minimalstandard stützt sich auf bestehende, bewährte Grundlagen wie das NIST Core Framework sowie die Risiko- und Gefährdungsanalyse der Wasserversorgung des Bundesamtes für wirtschaftliche Landesversorgung[2]. Der IKT-Minimalstandard bezweckt ein einheitliches Vorgehen, das vergleichbare Resultate in der Branche erlaubt und das Sicherheitsniveau der IKT-Systeme in der Wasserversorgung verbessert.

Für Querverbundunternehmen (z. B. Gas, Wasser, Strom, Abwasser, Kommunikation) ist es von grosser Wichtigkeit, dass für die unterschiedlichen Branchen dieselben IKT-Minimalstandards gelten. Der Verband der Schweizer Elektrizitätsunternehmen (VSE) wendet in seinem Standard dieselben Grundlagen an, wie in dem hier vorliegenden IKT-Minimalstandard für die Wasserversorgung.

Der IKT-Minimalstandard ist in sechs Teile unterteilt. Erstens in das hier vorliegende Hauptdokument). Es bietet eine Einleitung, Handlungsanweisungen sowie eine Einführung in die Wasserversorgung und bildet die Grundlage für die Umsetzung. Zweitens stehen vier Anhänge (Defense in Depth, Cyber Security Framework, Empfehlungen, Umsetzungsbeispiele) sowie ein Excelbasiertes Assessment-Tool zur Verfügung, siehe Kapitel 2.

Haftungsausschluss

[1] SCADA: Supervisory Control and Data Acquisition

[2] Risiko- und Verwundbarkeitsanalyse der Wasserversorgung. Bundesamt für wirtschaftliche Landesversorgung, Bern 2016.

1 Einführung

1.1 Hintergrund im Überblick

Das Bundesamt für wirtschaftliche Landesversorgung überprüfte im Rahmen der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken 2016 die Wasserversorgung auf IKT-Verwundbarkeiten. Die daraus resultierende IKT-Verwundbarkeitsanalyse wurde gemeinsam von Bund und Wasserversorgern erarbeitet. Den Kern der Analyse bilden jene Prozesse, durch die die Versorgung der Schweizer Bevölkerung mit Wasser sichergestellt werden kann.

Die Wasserversorgung lässt sich in den meisten Fällen in fünf Basisprozesse unterteilen: Als erstes muss das Wasser aus Quellen, Seen und/oder Grundwasservorkommen gewonnen und gefördert werden. Danach wird es je nach Qualität unterschiedlich intensiv aufbereitet (keine, einfache oder mehrstufige Aufbereitung) und in das Netz/Reservoirs transportiert. Von dort aus gelangt es in das Verteilnetz, das das Wasser bis zum Endkonsumenten verteilt.

Das zentrale IT-System der Wasserversorgung in diesen fünf Kernprozessen ist das sogenannte SCADA-System. Zur Steuerung seiner Pumpen, Reservoire oder Aufbereitungsanlagen betreibt jedes Wasserwerk ein SCADA-System. Wenn dieses ausfiele, würden die Aufbereitungsanlagen ihre Aufgabe nicht mehr wahrnehmen können. Aber auch die Steuerung der Pumpen würde teilweise nicht mehr funktionieren, da nicht alle manuell bedient werden können. Ausserdem kann dessen Ausfall unter Umständen dazu führen, dass Störungsmeldungen und Alarme nicht mehr empfangen werden können.

Neben dem SCADA-System sind auch Kommunikationssysteme wie z. B. E-Mail, mobile Kommunikation, VoIP[3] und teilweise Funkkommunikation wichtig für die Wasserversorger. Ohne Kommunikationssysteme können die Werke mit verteilten Anlagen (z. B. Seewasserwerk) nicht mehr effizient miteinander kommunizieren und Störungen beheben.

Basierend auf der erwähnten IKT-Verwundbarkeitsanalyse der Wasserversorgung bietet der vorliegende Minimalstandard Empfehlungen zur Erhöhung des Sicherheitsniveaus der IKT in der Wasserversorgung[4] Die betroffenen Akteure sind gehalten, ihr Sicherheitsniveau anhand des vorliegenden Dokuments selbst einzuschätzen und ihr Maturitätsniveau (Reifegrad der IKT-Sicherheit) mit dem Sollwert zu vergleichen. Bei Abweichungen bietet der vorliegende Standard (sowie weitere referenzierte und anerkannte Standards) eine Hilfestellung zur Verbesserung betroffener Sicherheitsbereiche.

Das Landesversorgungsgesetz gibt dem Bundesrat die Kompetenz, vorsorgliche Massnahmen zur Förderung der Resilienz (Widerstandsfähigkeit) der für unser Land lebenswichtigen Versorgungsprozesse anzuordnen. Der hier vorliegende IKT-Minimalstandard für die Wasserversorgung ist eine solche Resilienz-Massnahme, die jedoch im Sinn einer Selbstregulierung von der Branche freiwillig umgesetzt wird. Der IKT-Minimalstandard wurde dementsprechend gemeinsam mit dem Schweizerischen Verein des Gas- und Wasserfaches (SVGW) als Branchenempfehlung abgefasst.

[3] VoIP: Voice over IP

[4] Als Grundlagen für den hier vorliegenden IKT-Minimalstandard wurden insbesondere die folgenden vier Dokumente verwendet:
- Der Allgemeine IKT-Minimalstandard der wirtschaftlichen Landesversorgung
- Framework for Improving Critical Infrastructure Cybersecurity
- Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
- Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU)

1.2 Ausgangslage und Zielsetzung

Die Verwundbarkeitsanalyse der Wasserversorgung[5] (2016) zeigte eine zunehmende IKT-Abhängigkeit der Trinkwasserversorgung. Die Digitalisierung schreitet auch bei den Wasserversorgern voran, was einerseits die Effizienz steigert, jedoch andererseits die Komplexität der Versorgung erhöht. Der Ausfall kritischer IKT-Systeme kann grosse Auswirkungen auf die Versorgung mit Trinkwasser, Prozesswasser oder Löschwasser nach sich ziehen.

Vorliegende Branchenempfehlung der Wirtschaftlichen Landesversorgung (WL), bzw. des Bundesamts für wirtschaftliche Landesversorgung (BWL) und des SVGW verfolgt einen Defense in Depth Ansatz [6] und berücksichtigt eine breite Palette von Bedrohungen für die IKT-Sicherheit. Ziel ist es, den IKT-Verantwortlichen der Wasserversorger ein praxisnahes Werkzeug zur Verfügung zu stellen, um die Cyber-Sicherheit in ihren Unternehmen zu beurteilen und zu verbessern. Damit soll die Resilienz der Wasserversorger gegenüber IKT-Bedrohungen verbessert und letztlich die Versorgungssicherheit ins-gesamt erhöht werden.

IKT-Bedrohungen werden umfassend verstanden: von physischer Beschädigung über den Verlust oder die Manipulation von Daten, bis hin zum Schutz vor Cyber-Angriffen in zerstörerischer Absicht. Es werden insbesondere auch jene Bedrohungen berücksichtigt, die im Rahmen der IKT-Verwundbarkeitsanalyse der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken identifiziert wurden.

Diese Branchenempfehlung berücksichtig neben technischen Massnahmen auch die Ausbildung und Schulung der Mitarbeitenden sowie die Governance, um die Resilienz von wichtigen IKT Systeme zu verbessern. Dazu empfehlen wir einen mehrschichtigen Ansatz, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.

Die Cyber-Sicherheitsstrategie einer Organisation sollte die Vermögenswerte schützen, die sie für einen erfolgreichen Betrieb für wichtig erachtet. Leider gibt es keine Abkürzungen, einfache Lösungen oder einen «Königsweg», um Cyber Security-Schwachstellen innerhalb der kritischen Infrastruktur anzugehen. Es erfordert einen mehrschichtigen Ansatz, der als Defense in Depth bekannt ist. Letzteres trägt dazu bei, die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen:

- **Verfügbarkeit**
  Gewährleisten, dass Informationen zum Zeitpunkt des Bedarfs verfügbar sind. Dies setzt voraus, dass die Systeme zur Verarbeitung und Übertragung einsatzfähig und verfügbar sind.
- **Integrität**
  Gewährleisten, dass Informationen jederzeit vollständig, richtig und zuverlässig sind sowie ein unerlaubtes Abändern bzw. Zerstören verhindert wird.
- **Vertraulichkeit**
  Gewährleisten, dass Informationen ausschliesslich berechtigten Personen beziehungsweise Systemen zugänglich sind.

[5] Risiko- und Verwundbarkeitsanalyse des Teilsektors Wasserversorgung. Durchgeführt durch die wirtschaftliche Landesversorgung (https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ncs_strategie/stand_der_umsetzungsarbeiten.html) [Stand 07.09.2018].

[6] Siehe auch Anhang 1.

1.3 Geltungsbereich und Abgrenzung

Vorliegende Branchenempfehlung der WL bzw. des SVGW fokussiert auf jene Unternehmensprozesse, die einen direkten Einfluss auf die sichere Versorgung der Schweizer Bevölkerung mit Trinkwasser haben. Der Umfang dieser Branchenempfehlung ist wie folgt definiert:

Geltungsbereich

- Der IKT-Minimalstandard schliesst alle Informations- und Kommunikationstechnologie ein, die für den Betrieb der Systeme und Netze der Trinkwasserversorgung notwendig sind.
- Die Resilienz der Systeme soll branchenweit verbessert werden. Das angestrebte minimale Schutzniveau soll verhindern, dass die Wasserversorgung durch einen Cyber-Vorfall massgeblich gestört wird.
- Im Fokus stehen insbesondere folgende Systeme: SCADA-Systeme, ERP-Systeme[7], Kommunikationssysteme. Betroffen sind aber auch Laptops und PC-Arbeitsplätze, Mobiltelefone, Instandhaltungssoftware, Schnittstellen zu SCADA-Systemen, Smart Metering, Netzwerke und Systeme in nicht eigenen Gebäuden (Kundenanlagen).
- Die Empfehlung hat Unternehmen der Wasserversorgung im Fokus, die zur Aufrechterhaltung des Betriebs massgeblich auf IKT-Systeme angewiesen sind.

Abgrenzung

- Die Fähigkeit, die eigene Wasserversorgung in Notsituationen (wie z. B. einem Cyber-Angriff) auch ohne IKT-Systeme in einem «manuellen Betrieb» aufrecht zu erhalten, ist nicht Teil dieser Branchenempfehlung. Trotzdem wird an dieser Stelle empfohlen, diese Fähigkeiten, wo möglich, zu erhalten oder zu erstellen, falls es die betriebswirtschaftlichen Umstände zulassen. Der manuelle Betrieb ist essentiell für kritische Infrastrukturen – zumindest das geordnete Abschalten der Infrastruktur sollte zu jeder Zeit noch möglich sein.
- Die Stromversorgung ist nicht Teil dieses IKT-Minimalstandards. Trotzdem wird ein Notkonzept zum Umgang mit Stromversorgungsengpässen oder einem Blackout für jede Wasserversorgung empfohlen. Hinsichtlich Stromversorgung besteht eine grosse Abhängigkeit. Pumpstationen, Aufbereitung des Rohwassers, Transport und Gewinnung können ohne Strom nur beschränkt oder gar nicht mehr ausgeführt werden. Hingegen würden Quellwasserfassungen grösstenteils auch ohne Strom funktionieren (ohne Desinfektion). Da über 40 % des Trinkwassers aus Quellwasservorkommen gewonnen wird, kann lokal ein beträchtlicher Teil des Trinkwassers noch ohne Strom gewonnen werden. Einige Versorgungsgebiete benötigen auch zur Verteilung des Quellwassers keinen Strom. Andere Wasserversorger sind dagegen für die Gewinnung und Verteilung von Quell- und insbesondere Grundwasser mit Notstromaggregaten ausgerüstet. Dies sind Massnahmen, die die Wasserversorgung bis zu einem gewissen Grad auch bei einer Strommangellage oder einem Blackout sicherstellen.
- Die Verordnung über die Sicherstellung der Trinkwasserversorgung in Notlagen (s. Kapitel 5.1) ist nicht Teil dieses Standards, sondern eine allgemeine Resilienz-Massnahme für die Wasserversorgung.
- Massnahmen zur Arbeitssicherheit sind nicht Bestandteil dieser Branchenempfehlung.

[7] Enterprise Ressource Planning-System: Das ERP-System ist eine komplexe Anwendung oder eine Vielzahl miteinander kommunizierender Anwendungssoftware- bzw. IT-Systeme, die zur Unterstützung der Ressourcenplanung des gesamten Unternehmens eingesetzt werden.

1.4 Notwendigkeit für einen IKT-Minimalstandard

Im sich ständig weiterentwickelnden Bereich der IKT verändern sich ebenfalls die Bedrohungen permanent und betreffen sowohl kleine und als auch grosse Wasserversorger. Cyberangriffe sind von der Grösse der Unternehmung unabhängig; sie sind häufig sogar zufällig oder geschehen, weil sich günstige Gelegenheiten bieten. Solche ergeben sich aufgrund der fortschreitenden Digitalisierung immer häufiger. Mehr und mehr Wasserversorger verbinden ihre Steuerungssysteme mit dem Internet, um beispielsweise durch Fernüberwachung Kosten zu sparen oder flexibler zu werden. Dies kann zu neuen Verwundbarkeiten führen, die von Hackern ausgenutzt werden, um z. B. Daten zu stehlen, fremde IKT-Ressourcen zu nutzen oder die Kontrolle über kritische Anlagen zu übernehmen.

Solche Bedrohungen sind sehr real. Bei Angriffen mit Ransomware zum Beispiel, werden Computernetzwerke oder Kontrollsysteme gesperrt und erst gegen die Zahlung eines Lösegelds wieder freigegeben. Wasserversorgungsunternehmen in den USA wurden auf diese Weise bereits erpresst, jedoch nur wenige haben Lösegeld bezahlt. Vielmehr haben sie ihren Betrieb wiederhergestellt, mit Hilfe von «Backups» oder indem sie das System ersetzt haben[8] Trotzdem verursachen solche Angriffe erhebliche Schäden und haben hohe Kosten für die Organisationen zur Folge.

Andere Angriffe wurden direkt auf die Steuerungssysteme ausgeübt. 2016 griffen Hacker ein Wasser-versorgungsunternehmen (Kemuri Water Company – KWC) an und manipulierten dessen Prozessleit-systeme, die für die Wasseraufbereitung und Durchflusskontrolle notwendig sind[9]. Der Internet Service Provider Verizon bemerkte, dass die Kemuri Water Company eine unzureichende Sicherheitsarchitektur hatte und die mit dem Internet verbundenen Systeme Schwachstellen und damit ein hohes Risiko für Angriffe aufgewiesen habe[10]. Da das kompromittierte Prozessleitsystem zur Steuerung der Zugabe von Chemikalien verwendet werden konnte, gelang es den Angreiffern, den Wasserfluss und die Chemikalienmenge zu beeinflussen. In mindestens zwei Fällen gelang es den Angreifern, das System so zu manipulieren, dass die Wasseraufbereitungs- und Produktionskapazitäten behindert wurden. Glücklicherweise war KWC dank der Alarmfunktion in der Lage, die chemischen Veränderungen und Änderungen in der Flussgeschwindigkeit schnell zu erkennen und rückgängig zu machen, wodurch die Auswirkungen auf die Kunden weitgehend minimiert werden konnten.

Um solche und weitere Gefahren möglichst zu beschränken, ist ein hohes Sicherheitsniveau der IKT-Systeme in der Wasserversorgung notwendig. Die Einführung eines einheitlichen standardisierten Vorgehens hinsichtlich Cyber Security erlaubt einer Organisation, ihre IKT möglichst adäquat zu schützen und diesen Schutz kontinuierlich zu verbessern. Vorliegender IKT-Minimalstandard gibt dazu praktisch umsetzbare Handlungsanweisungen.

Die Unternehmen der Wasserversorgung sind angehalten, ihre Risiken selbst zu identifizieren und ihre Risikobereitschaft selbständig zu definieren. Je nach Grösse, Ressourcen und vorhandenem Wissen kann der vorliegende Standard auf den Risikoappetit der Organisation angepasst werden (risikobasierter Ansatz). Der Aufwand für die Umsetzung ergibt sich aus den entsprechenden Überlegungen.

Letztlich sei darauf hingewiesen, dass die Verantwortung des Wasserversorgers zur Sicherstellung eines sicheren Betriebes in jedem Fall ihm selbst obliegt.

[8] WaterNews - Water Sector Prepares for Cyberattacks. June 9, 2016/in Infrastructure, United States, Water Management, Water News/by Brett Walton, in: http://www.circleofblue.org/2016/world/water-sector-prepares-cyberattacks/ [Stand 22.02.2018].

[9] Verizon, Data Breach Digest 2016, in: http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf [Stand 22.02.2018].

[10] Security Week Online: https://www.securityweek.com/attackers-alter-water-treatment-systems-utility-hack-report [Stand 22.02.2018].

2 Anleitung zur Anwendung des IKT-Minimalstandards

Der IKT-Minimalstandard ist in mehrere Teile gegliedert (Abb. 1). Der vorliegende Hauptteil bildet die Grundlage für die Umsetzung des IKT-Minimalstandards und bietet eine Einleitung, Handlungsanweisungen sowie einen Überblick über die Wasserversorgung in der Schweiz. Dazu gibt es vier Anhänge und ein Excel basiertes Assessment-Tool.

Abb. 1 Übersicht über die Dokumente des IKT-Minimalstandards

Hauptdokument (hier vorliegend) (notwendig)
Das hier vorliegende Hauptdokument des IKT-Minimalstandards (Branchenempfehlung BWL/SVGW) bietet eine Einführung in das Thema und gibt Handlungsanweisungen, wie der Standard umzusetzen ist.

Anhang 1 – Defense in Depth (fakultativ)
Bietet eine Einführung in die Grundlagen (Defense in Depth).

Anhang 2 – Cyber Security Framework (fakultativ)
Stellt das im Assessment-Tool verwendete Cyber Security-Framework dar und bietet Informationen über die Einstufung der eigenen Maturität mit Hilfe der Maturitätsskala (Tier 0 bis 4) sowie einen Überblick über die Darstellung der Resultate des Assessment-Tools.

Anhang 3 – Empfehlungen für kleine Wasserversorger (notwendig für kleine Versorger)
Bietet spezifische Empfehlungen für Wasserversorger mit einem Versorgungsgebiet von weniger als 5000 versorgten Einwohnern.

Anhang 4 – Umsetzungsbeispiele (fakultativ)
Stellt anonymisierte Umsetzungsbeispiele zur Verfügung, die bei Fragen während der Umsetzung des IKT-Minimalstandards hinzugezogen werden können.

Assessment-Tool (Excel basiert – notwendig für Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 versorgten Einwohnern)
Das Excel basierte Assessment-Tool bietet eine Unterstützung bei der Umsetzung des IKT-Minimalstandards und erlaubt die Einschätzung der Maturität einer Wasserversorgung hinsichtlich ihrer Cyber Security. Das Assessment-Tool wird für alle Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 Einwohnern empfohlen.

Die Branche ist hinsichtlich Grösse der für die Wasserversorgung verantwortlichen Unternehmen sehr heterogen. Dieser IKT-Minimalstandard hat den Anspruch, die gesamte Branche abzudecken. Die Branche hat sich für ein differenziertes Vorgehen entschieden. Für Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 Einwohnern gilt der IKT-Minimalstandard vollumfänglich. Diese Versorger sind angehalten, ihr Maturitätsniveau entsprechend dem Assessment-Tool zu eruieren und kontinuierlich zu verbessern. Insbesondere für die grössten Wasserversorger der Schweiz sollte ein Maturitätsniveau, das über dem empfohlenen Minimalsicherheitsniveau liegt, erreicht werden.

Für Wasserversorger, die weniger als 5000 Einwohner versorgen ist der Aufwand an Zeit und Fachwissen, der mit der Anwendung des Assessment-Tools anfällt, möglicherweise zu hoch. Für sie wurden spezifische Empfehlungen (siehe Anhang 3) erarbeitet, deren Umsetzung als Minimalvorgabe (und anstelle des Assessment-Tools) empfohlen wird.

2.1 Umsetzung des IKT-Minimalstandards

2.1.1 Differenziertes Vorgehen

Versorgte Einwohner	Umsetzungsempfehlung
≥ 5000	IKT-Minimalstandard vollumfänglich, inklusive Assessment-Tool
< 5000	Empfehlungen (siehe Anhang 3)

Tab. 1 Umsetzung des IKT-Minimalstandards

2.1.2 Vorbereitung

Die Umsetzung des IKT-Minimalstandards kann anhand des folgenden Prozesses (Flow-Charts) angegangen werden (Abb. 2). Falls die IT der Wasserversorgung Teil der IT-Organisation der Gemeinde ist, kann die Umsetzung übergeordnet erfolgen und auch weitere Versorgungsprozesse umfassen. Falls dies nicht der Fall ist oder die Wasserversorgung eigenständig nach diesem Standard gesichert werden soll, wird als nächstes eine Grösseneinstufung durchgeführt. Wasserversorger, die weniger als 5000 Einwohner versorgen, setzen die Empfehlungen im Anhang 3 um. Wasserversorger, die mehr als 5000 Einwohner versorgen, setzen diesen IKT-Minimalstandard vollumfänglich und mit Hilfe des Assessment-Tools um.

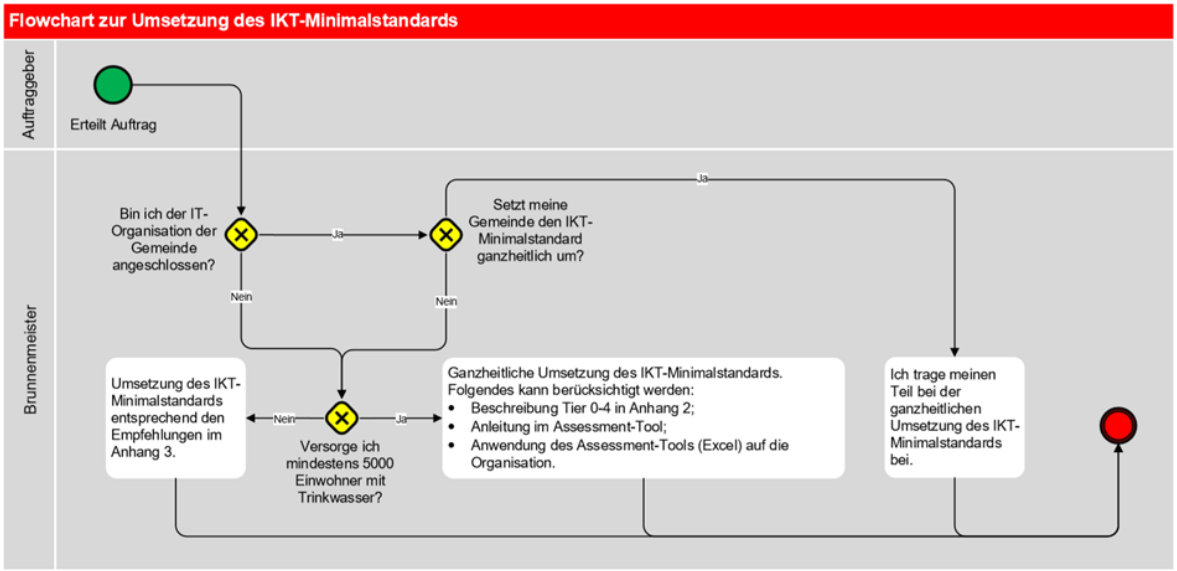

Abb. 2 Prozess zur Umsetzung des IKT-Minimalstandards

2.1.3 Anleitung für Wasserversorger mit einem Versorgungsgebiet von weniger als 5000 Einwohnern

Wasserversorger, zuständig für ein Versorgungsgebiet von weniger als 5000 Einwohnern, sind ebenfalls vom vorliegenden IKT-Minimalstandard betroffen, jedoch nicht vollumfänglich. Im Anhang 3 zu diesem Branchenstandard befindet sich eine Liste mit Empfehlungen, die anstelle des Assessment-Tools umgesetzt werden sollen. Anhand der Hilfestellung in Anhang 3 soll der bisherige Umsetzungsstand der Empfehlungen abgeschätzt werden. Dadurch wird ersichtlich, in welchen Bereichen Handlungsbedarf besteht. In Anhang 4 steht ein Umsetzungsbeispiel eines kleinen Wasserversorgers zur Verfügung.

Der Minimalstandard für kleine Wasserversorger gilt dann als erfüllt, wenn alle Empfehlungen in Anhang 3 umgesetzt sind.

2.1.4 Anleitung für Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 Einwohnern

Für Wasserversorger mit einem Versorgungsgebiet von mehr oder gleich 5000 Einwohnern gilt der IKT-Minimalstandard vollumfänglich. Das hier vorliegende Dokument gilt als Handlungsanleitung sowie Umsetzungshilfe. Der IKT-Minimalstandard gilt dann als umgesetzt, wenn die Wasserversorgung ihre Maturität mit dem beiliegenden Assessment-Tool eingestuft hat und diese entsprechend dem eigenen risikobasierten Ansatz mindestens den Minimalvorgaben im Overall-Rating (siehe Assessment-Tool) entspricht.

Grundsätzlich wird insbesondere für grosse Wasserversorger ein prozessbasierter Ansatz empfohlen. Dies bedeutet, dass Cyber Security kein Zustand ist, sondern als Prozess verstanden und gelebt wird. Sicherheit im Umgang mit IKT kann nie erzielt werden, sondern muss ständig angestrebt und regelmässig überprüft sowie verbessert werden. Die regelmässige (z. B. jährliche) Überprüfung und Verbesserung anhand des IKT-Minimalstandards wird empfohlen. Der SVGW wird dazu spezifische Ausbildungen und Unterstützung anbieten.

Das Assessment-Tool ist ein Hilfsmittel zur Selbsteinschätzung und entspricht im Wesentlichen den Anforderungen des NIST Framework Core[11]. Es umfasst fünf Funktionen (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen) (Abb. 3). Diese sind in 23 Kategorien aufgeteilt, die sich ihrerseits wiederum in gesamthaft 106 Aktivitäten gliedern.

[11] NIST Framework Core: https://www.nist.gov/framework [Stand 26.03.2018].

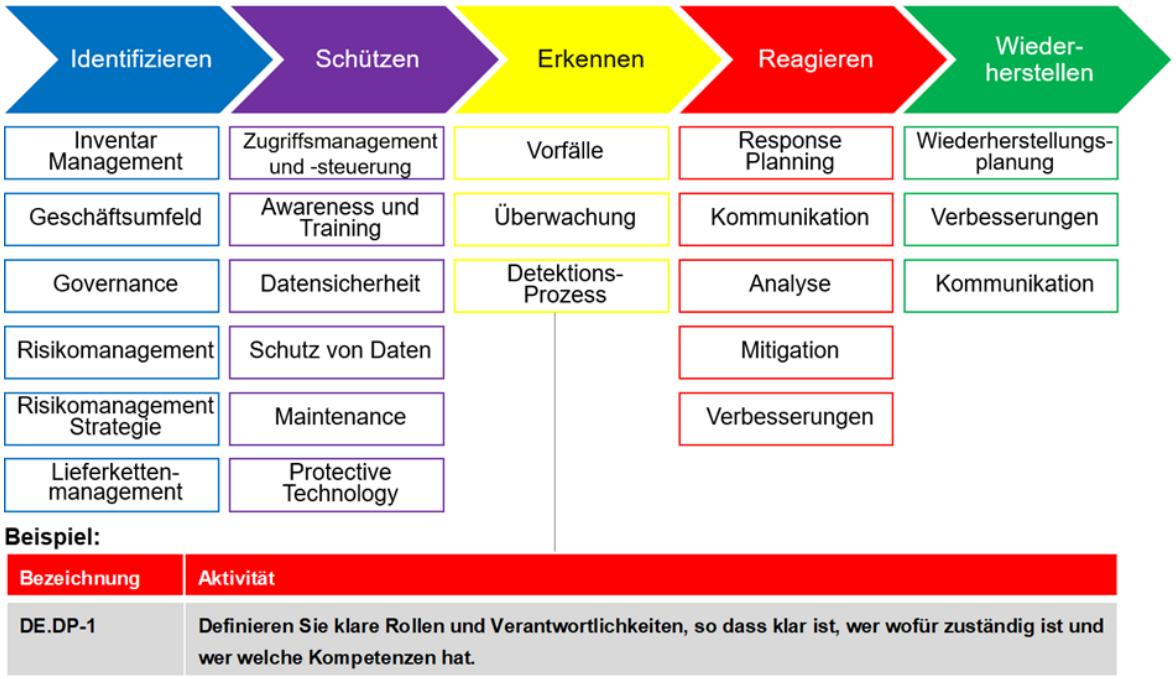

Abb. 3 Funktionen, Kategorien und Beispiel-Aktivität des Cyber Security Frameworks

Anhang 2 stellt das Cyber Security Framework dar und wird als Informations- und Diskussionsgrundlage zur Verfügung gestellt. Im Assessment-Tool sind alle fünf Funktionen, 23 Kategorien und 106 Aktivitäten abgebildet und so dargestellt, dass sie bewertet und kommentiert werden können.

Bevor mit dem Assessment durch das Assessment-Tool begonnen wird, können die Funktionen und Kategorien des Cyber Security Frameworks entsprechend der Risikobereitschaft der Organisation priorisiert werden. Dazu werden entsprechend dem risikobasierten Ansatz der Organisation die fünf Funktionen und 23 Kategorien bewertet. Die Wasserversorger beurteilen, welche Funktionen und Kategorien für die Organisation besonders wichtig sind (hohe Priorität), und welche als weniger relevant eingestuft werden.[12] So können beispielsweise bereits einige Kategorien festgelegt werden, bei denen weniger oder mehr Ressourcen aufgewendet werden sollen. In Kategorien, die entsprechend dem risikobasierten Ansatz der Organisation weniger im Fokus stehen, können die Risiken akzeptiert (mit «nicht zutreffend» bewertet) werden. Im Vergleich zu einem nichtpriorisierten Vorgehen erlaubt dies einen Effizienzgewinn bei der Bewertung der 106 Aktivitäten und ist insbesondere für Wasserversorger von mittlerer Grösse (ca. zwischen 5000 und 15000 Einwohnern) von besonderem Interesse. Den grössten Wasserversorgern der Schweiz (grosse Städte) wird dagegen die Umsetzung aller 106 Aktivitäten des Cyber Security Frameworks empfohlen.
Anschliessend kann das Assessment mit Hilfe des Assessment-Tools durchgearbeitet und die Antworten direkt in das Tool eingetragen werden. Bei Fragen zu den Aktivitäten können die referenzierten Standards (siehe Assessment-Tool) oder der Theorieteil im Anhang 2 zum IKT-Minimalstandard konsultiert werden. Besonders hilfreich könnten auch die Umsetzungsbeispiele mit Musterantworten zu den 106 Aktivitäten im Anhang 4 sein.

[12] Der risikobasierte Ansatz basiert kann beispielsweise auf dem Risikomanagement der Organisation basieren. Siehe dazu auch die Umsetzungsbeispiele in Anhang 4.

2.2 Struktur der Branche

Mehr als 2500 Wasserversorger beliefern die Einwohner der Schweiz mit Trinkwasser. Bei der Mehrheit handelt es sich um Klein- und Kleinstbetriebe. Der Grund für die hohe Anzahl eigenständiger Wasserversorgungen liegt darin, dass in der Schweiz die Trinkwasserversorgung in den Kompetenzbereich der Kantone fällt. Diese delegieren den Versorgungsauftrag weiter an die Gemeinden und räumen ihnen diesbezüglich erhebliche Entscheidungsfreiheiten ein. So betreiben üblicherweise die politischen Gemeinden die Wasserversorgung, teilweise auch Aktiengesellschaften. Mehrheitlich handelt es sich dabei um öffentlich-rechtliche Körperschaften. Vielerorts schliessen sich mehrere Gemeinden zusammen und lösen gemeinsam die Aufgabe der Wasserversorgung. Daneben gibt es zahlreiche Betriebe, die als Querverbundunternehmen organisiert sind und somit mehrere Versorgungsaufgaben gleichzeitig wahrnehmen (z. B. Gas- und Wasserversorgungen oder Gas-, Wasser- und Elektrizitätsversorgungen). Es gibt jedoch für die Schweizer Wasserversorgung kein Einheitsmodell.

2.3 Versorgungsleistung

Wasser wird in der Schweiz für vielfältige Zwecke genutzt; nicht nur die Haushalte, auch das Gewerbe, die Industrie und Landwirtschaft brauchen das kostbare Nass. Täglich verbrauchen Frau und Herr Schweizer etwa 142 Liter Trinkwasser zum Trinken, Kochen, Waschen und Reinigen. Der Verbrauch in den Haushalten macht etwa einen Viertel des Gesamtverbrauchs aus. Weitere 20 % entfallen auf die Landwirtschaft. Allerdings fliesst rund die Hälfte des zur Landwirtschaft gerechneten Wassers ungenutzt durch die Brunnen ab. Gut die Hälfte des Wassers verbrauchen Gewerbe und Industrie (Abb. 4).

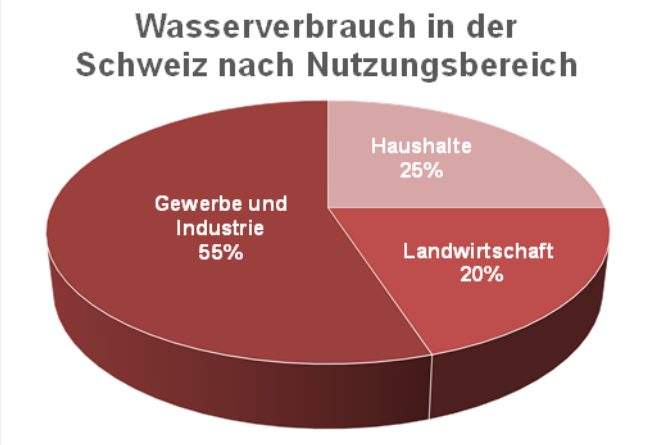

Abb. 4 Wasserverbrauch in der Schweiz

In der Schweiz entfallen drei Viertel des landwirtschaftlichen Wasserverbrauchs auf die Herstellung von Milch-, Rind- und Schweineprodukten. Im Gegensatz zu den tierischen Erzeugnissen wird ein überwiegender Teil der pflanzlichen Produkte importiert. Ein wesentlicher Anteil des Wassers, das in Gewerbe, Landwirtschaft und Industrie genutzt wird, stammt nicht aus den öffentlichen Wasserversorgungen, sondern aus konzessionierten Eigenförderungen, die hinsichtlich ihrer Menge die öffentliche Gewinnung übertrifft. Neben der wirtschaftlich wichtigen Verwendung des Trinkwassers für die Produktion wird es ausserdem als Löschwasser benötigt.

2.4 Übersicht der kritischen Systeme

Die Abhängigkeit der Wasserversorgung von IKT-Systemen ist hoch. Insbesondere die Aufbereitung von Rohwasser sowie der Kommunikationsprozess und die Überwachung des gesamten Versorgungsgebietes können ohne IKT-Systeme – wie beispielsweise dem SCADA-System oder den Kommunikationsmitteln – nur beschränkt aufrechterhalten werden. Folgende Tabelle stellt die wichtigsten Systeme für die Kernprozesse der Wasserversorgung dar

Liste wichtiger IKT-Systeme im Teilsektor Wasserversorgung	
Kernprozess Wasserversorgung	Wichtigste IKT-Systeme
Wassergewinnung	SCADA-System*
Aufbereitung	SCADA-System*
Transport	SCADA-System*
Speicherung	SCADA-System*
Verteilung	SCADA-System*
Kommunikationsprozess	Mobile- und Festnetz-Telefonie, VoIP, E-Mail
Steuerungsprozess	SCADA-System*

Tab. 2 Liste wichtiger IKT-Systeme zur Versorgung der Schweiz mit Wasser

* Unter einem SCADA-System werden die Steuerungssysteme der Wasserversorgung verstanden. Beispielsweise das Steuerungssystem eines Seewasserwerkes, inklusive Steuerungskomponenten (SPS) der Anlagen selbst sowie dem dazugehörenden Leitsystem.

3 Schlussfolgerungen

Trinkwasser bildet eine Lebensgrundlage für unsere Gesellschaft und ein wichtiges Produktionsmittel in diversen Zweigen der Wirtschaft. Charakteristisch für die Schweizer Wasserversorgung sind die unterschiedlichen Organisationsformen und die grosse Anzahl an involvierten Akteuren. Derzeit stellen in der Schweiz gesamthaft 2500 Wasserversorger die Trinkwasserversorgung sicher. Dabei beziehen Wasserversorger das Wasser oftmals aus verschiedenen Fassungen mit unterschiedlichen Wasservorkommen und zum Teil mit variierender Qualität. In der Schweiz wird das Trinkwasser zu 80 % aus Grund- und Quellwasser und 20 % aus Oberflächengewässern gewonnen. Insbesondere die Aufbereitung des Oberflächenwassers ist ein komplexer Prozess, in dem oft mehrere Filtrations- und Desinfektionsschritte präzise gesteuert werden müssen. Bei einem Ausfall der IKT-Systeme zur Steuerung dieser Prozesse kann die Aufbereitung des Wassers nicht mehr gesichert durchgeführt werden, da eine manuelle Steuerung dieses Prozesses, aufgrund der hohen Komplexität, nur sehr beschränkt möglich ist.

Ein grossflächiger Ausfall der Wasserversorgung durch Cyber-Angriffe hätte verheerende Konsequenzen für die betroffenen Bevölkerungsteile und die Wirtschaft. Einem Ausfall der für die Wasserversorgung wichtigen IKT-Systeme, der einzelnen Anlagen oder gar der Stromversorgung kann jedoch auf verschiedene Weise entgegengewirkt werden. Eine zentrale Rolle spielt dabei die Anwendung und periodische Überprüfung der Prozesse und Anlagen auf Basis dieses IKT-Minimalstandards. Er bietet als Branchenempfehlung eine praxisnahe Hilfestellung für jede Wasserversorgung, um ihr Sicherheitsniveau auf ein einheitliches Minimum anzuheben. Für Wasserversorger mit einem Versorgungsgebiet von grösser als 5000 Einwohnern steht ein Assessment-Tool zur Verfügung. Insbesondere bei sehr grossen Wasserversorgern mit einem Versorgungsgebiet von über 50 000 versorgten Einwohnern ist ein Sicherheitsniveau anzustreben, das klar über den Minimalvorgaben liegen sollte. Für Wasserversorger, die weniger als 5000 Einwohner versorgen, sind im Anhang 3 spezifische Empfehlungen angefügt, die eine einfachere Umsetzung des Standards erlauben.

Der in diesem IKT-Minimalstandard verfolgte Defense in Depth legt einen hohen Wert auf den risikobasierten Ansatz. Er bietet bewusst keine Standardlösungen, sondern fordert die Akteure der Wasserversorgung auf, anhand des risikobasierten Ansatzes die eigene Situation betreffend Cyber Security zu analysieren und zu bewerten. Der IKT-Minimalstandard ermöglicht jedem Unternehmen oder jeder Organisation, die Risikobereitschaft selbst zu definieren und Massnahmen zur Verbesserung von Risiken zu entwickeln und zu priorisieren. Die Verantwortung für Cyber Security bleibt in jedem Fall bei der Wasserversorgung (und allenfalls den politischen Verantwortlichen).

Mit einem Excel basierten Assessment-Tool bietet dieser IKT-Minimalstandard ein Werkzeug, mit dem die Akteure der Wasserversorgung ihr Sicherheitsniveau einfach, aber systematisch auf ein einheitlich hohes Minimum anheben können. Die IKT-Sicherheit ist kein Zustand, sondern soll als iterativer Prozess umgesetzt und gelebt werden. Dieser IKT-Minimalstandard basiert auf einer bewährten Methodik, um diesen Prozess anzuregen und effizient umzusetzen. Auch andere Versorgungsbranchen wie die Stromversorgung verwenden dieselben Grundlagen und Ansätze, was nicht zuletzt bei Querverbundunternehmen grosse Synergien ermöglicht.

Damit das Fachwissen zur Umsetzung dieser Branchenempfehlung möglichst breit gestreut und umgesetzt werden kann, wird der SVGW den IKT-Minimalstandard in der Branche bekannt machen. Anhand spezifischer Ausbildungen und Beratung unterstützt der SVGW seine Mitglieder bei der Einführung und Umsetzung des IKT Minimalstandards.

4 Appendix

4.1 Grundlagen-Dokument und Standards (Stand Mai 2018)

Dieses Dokument berücksichtigt Konzepte, Empfehlungen und Massnahmen von verschiedenen Standards und anderen normativen Dokumenten. Siehe untenstehende Tabelle:

Titel	Jahr	Herausgeber und Beschreibung
Massnahmen zum Schutz von industriellen Kontrollsystemen (SCADA)	2013	Hrsg.: **Melde- und Analysestelle Informationssicherung MELANI** Diese Anleitung beschreibt basierend auf US-amerikanischen Unterlagen vom *Department of Homeland Security, Industrial Control Systems - Cyber Emergency Response Team (SCADA-CERT)* sowie dem *National Institute of Standards and Technology (NIST)* knapp und pragmatisch auf acht Seiten die wichtigsten elf Massnahmen, die SCADA-Betreiber gewährleisten müssen.
Risiko- und Verwundbarkeitsanalyse des Teilsektors Wasserversorgung	2016	Hrsg.: **Bundesamt für wirtschaftliche Landesversorgung (BWL)** Die Risiko- und Verwundbarkeitsanalyse ist basierend auf der Nationalen Cyber-Strategie (NCS) und der Strategie zum Schutz kritischer Infrastrukturen (SKI) entwickelt worden. Ziel ist die Analyse der Verwundbarkeit gegenüber von Ausfällen oder Störungen der IKT im kritischen Teilsektor «Wasserversorgung».
Leitfaden Schutz kritischer Infrastrukturen (Leitfaden SKI)	2015	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Der Leitfaden stellt ein Instrument zur Überprüfung und gegebenenfalls Verbesserung der Resilienz der kritischen Infrastrukturen dar. Insbesondere ist er in Hinblick auf die Anwendung in kritischen Teilsektoren durch Betreiber, Branchenverbände und Fachbehörden konzipiert. Im Wesentlichen beschreibt der Leitfaden ein mögliches Risikomanagement-Vorgehen: Analyse (Ressourcen-Identifikation, Verwundbarkeiten, Risiken), Bewertung, Massnahmen sowie deren Sicherstellung (Umsetzung, Überprüfung, Verbesserung). Das Vorgehen kann durchaus bzw. sollte sogar in bestehende Managementprozesse integriert oder darauf aufbauend ausgeführt werden.
Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI)	2012 und 2018	Hrsg.: **Bundesamt für Bevölkerungsschutz (BABS)** Die Strategie umschreibt den Geltungsbereich, bezeichnet die kritischen Infrastrukturen (u. a. Wasserversorgung) und hält die übergeordneten Grundsätze beim Schutz kritischer Infrastrukturen fest. Die nationale SKI-Strategie richtet sich an alle Stellen, die im Umfeld des Schutzes kritischer Infrastrukturen Verantwortlichkeiten aufweisen, insbesondere an die jeweils zuständigen Behörden, die politischen Entscheidungsträger und die Betreiber von kritischen Infrastrukturen.
Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)	2012	Hrsg.: **Informatiksteuerungsorgan des Bundes (ISB)** Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, hat der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken in Auftrag gegeben. Diese Strategie soll aufzeigen, wie diese Risiken heute aussehen, wie die Schweiz dagegen gerüstet ist, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind. Die Strategie identifiziert vorhandene Strukturen, definiert Zielsetzungen sowie sieben Handlungsfelder mit entsprechenden Massnahmen (z. B. Risiko- und Verwundbarkeitsanalysen eines Teilsektors wie Wasserversorgung – siehe weiter oben).

Titel	Jahr	Herausgeber und Beschreibung
Bundesgesetz über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG)	Stand 2016	Hrsg.: **Die Bundesversammlung der Schweizerischen Eidgenossenschaft** Dieses Gesetz regelt Massnahmen zur Sicherstellung der Versorgung des Landes mit lebenswichtigen Gütern und Dienstleistungen in schweren Mangellagen, denen die Wirtschaft nicht selbst zu begegnen vermag. Der Bund kann im Rahmen der bewilligten Mittel Massnahmen von privatrechtlichen und öffentlich-rechtlichen Unternehmen zur Sicherstellung der wirtschaftlichen Landesversorgung fördern, sofern die Massnahmen im Rahmen der Vorbereitung auf eine schwere Mangellage zu einer wesentlichen Stärkung lebenswichtiger Versorgungssysteme und Infrastrukturen beitragen. Eine dieser Massnahmen bildet der vorliegende IKT-Minimalstandard für die Wasserversorgung.
KRITIS-Sektorstudie «Ernährung und Wasser»	Stand 2015	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik** Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine der zentralen Stellen Deutschlands unter den zuständigen Behörden zum Schutz von kritischen Infrastrukturen. Mit unterschiedlichen Aktivitäten wie der Organisation von Branchengesprächen, der Bereitstellung von Standards und Leitfäden zu wichtigen IT-Sicherheitsthemen und nationalen Projekten sowie der Koordination des UP KRITIS verfolgt das BSI die Umsetzung der Nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) und der nationalen Cyber-Sicherheitsstrategie. In seinen Arbeiten ist das BSI auf genaue Kenntnisse zu den Funktionen kritischer Dienstleistungen und der damit verbundenen Bedeutung wichtiger Anlagen und Einrichtungen (KRITIS) angewiesen.
VTN - Verordnung über die Sicherstellung der Trinkwasserversorgung in Notlagen	Stand 2017	Hrsg.: **Der Schweizerische Bundesrat** Diese Verordnung soll die Trinkwasserversorgung in Notlagen sicherstellen. Die vorgesehenen Massnahmen sollen gewährleisten, dass: a. die normale Versorgung mit Trinkwasser so lange wie möglich aufrechterhalten bleibt, b. auftretende Störungen rasch behoben werden können, c. das zum Überleben notwendige Trinkwasser jederzeit vorhanden ist.
DVGW W 1060 (M) – Technischer Hinweis, Merkblatt	2017	Hrsg.: **Deutscher Verein des Gas- und Wasserfaches** Der DVGW hat mehrere Regularien und Leitfäden für die IT-Sicherheit in der Wasserversorgung erarbeitet. Das Merkblatt «W1060» bietet einen Überblick über vorliegende Regularien sowie «Tools» zu deren Umsetzung.
Process Control System Security Guidance for the Water Sector	2017	Hrsg.: **American Water Works Association (AWWA)** Ziel des AWWA-Leitfadens ist es, den Eigentümern/Betreibern von Wasserversorgungsunternehmen eine konsistente und wiederholbare Handlungsempfehlung zur Verringerung der Anfälligkeit für Cyber-Angriffe zu geben.
SCADA Security Good Practices for the Drinking Water Sector – TNO Report	2008	Hrsg.: **TNO Defence, Security and Safety** Die SCADA Security Good Practices für den niederländischen Trinkwassersektor sollen den Standard der Widerstandsfähigkeit des gesamten Trinkwassersektors gegen die unbefugte Cyber-Manipulation der Überwachungs- und Datenerfassungssysteme (SCADA) und anderer Systeme und Software der Informations- und Kommunikationstechnologie (IKT) erhöhen.
Produits de sécurité qualifiés - ANSSI (France)	2017	Hrsg.: **ANSSI (Agence nationale de la sécurité des systèmes d'information)** Die Qualifikation eines Sicherheitsprodukts ist in Artikel 9 der Verordnung Nr. 2005-1516 vom 8. Dezember 2005 über den elektronischen Austausch zwischen Nutzern und Verwaltungsbehörden sowie zwischen Verwaltungsbehörden vorgesehen.

Titel	Jahr	Herausgeber und Beschreibung
Guide d'hygiène informatique - ANSSI (France)	2017	Hrsg.: **ANSSI (Agence nationale de la sécurité des systèmes d'information)** Leitfaden zur Computerhygiene: 42 wesentliche Massnahmen zur Gewährleistung der Sicherheit Ihres Informationssystems und der Mittel zu deren Umsetzung, mit praktischen Hilfsmitteln.
Les règles de sécurité - ANSSI (France)	2017	Hrsg.: **ANSSI (Agence nationale de la sécurité des systèmes d'information)** Die Sicherheitsregeln sind sowohl organisatorisch als auch technisch. Die meisten davon müssen bereits von allen Betreibern eingesetzt werden, um ihre lebenswichtigen Informationssysteme effektiv zu sichern. Diese Sicherheitsregeln gelten insbesondere für SIIVs, die von Subunternehmern betrieben werden.
10 Steps to Cyber Security – NCSC (UK)	2016	Hrsg.: **NCSC (National Cybersecurity Centre, UK)** Anleitung, wie sich Organisationen im Cyberspace schützen können. • eine Einführung in die Cybersicherheit für Führungskräfte und leitende Angestellte, • ein Whitepaper, das erklärt, wie ein gewöhnlicher Cyberangriff aussieht und wie Angreifer ihn ausführen, • die zehn technischen Beratungsblätter, die Sie in Betracht ziehen sollten, einzurichten.
ISO 27001:2013 Information technology - Security techniques - Information security management systems - Requirements ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls	2013	Hrsg.: **International Standard Organization (ISO)** Detailliert die Anforderungen an ein Information Security Management System (ISMS). Die ISO 27k-Serie umfasst eine Reihe von *Information Security Standards*, wovon folgende hier von Interesse sind: • 27000:2016 Übersicht und Vokabular (2016 indiziert Jahr der Herausgabe) • 27001:2013 Anforderungen: Grundlagen mit Kontrollen und Kontrollzielen im Anhang • 27002:2013 Leitfaden für Kontrollen • 27003:2010 Anleitung zur Implementation • 27005:2011 Risiko-Management Die ISO 27000 Security Standards sind mittlerweile die am meisten verbreiteten und dürften sich in den kommenden Jahren als die massgebenden erweisen. Schon heute liegt durchaus richtig, wer ISO Security Standards befolgt. Im Gegensatz zu anderen Standards, wie IT Grundschutz, ANSI/ISA oder NIST, sind sie weniger detailliert, dementsprechend flexibel anwendbar und können über eine längere Zeitspanne kontinuierlich verbessert und erweitert werden.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieser Leitfaden gibt eine umfassende Einführung in SCADA, Topologien und Architekturen, identifiziert Bedrohungen und Verwundbarkeiten und gibt Empfehlungen zu Gegenmassnahmen und Risikominderung. Zudem werden SCADA-spezifische Kontrollen basierend auf dem NIST 800-53 Framework präsentiert.
ISA 62443 Industrial communication networks – Network and system security	2009 ff	Hrsg.: **International Society of Automation (ISA)** Serie von insgesamt 13 *Industrial Automation and Control System* (IACS) Security Standards und technischen Berichten. Diese Normen sind allgemein anwendbar im Bereich industrieller Automation und nicht stromversorgungs-spezifisch. Sie basieren auf den ISO 27000 Standards und erweitern diese mit Unterschieden und Spezifika industrieller Automation. Speziell zu erwähnen ist die Behandlung von Netzwerk- und Zonenarchitektur, die sich in anderen Standards kaum oder nicht so detailliert findet.

Titel	Jahr	Herausgeber und Beschreibung
Recommended Practice: Improving Industrial Control System Cyber Security with Defense in Depth Strategies	2016	Hrsg.: **Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)** Eine erweiterte und erneuerte Ausgabe einer früheren Veröffentlichung aus dem Jahre 2006. Umfassende Einführung in die Defense in Depth-Sicherheitsstrategie für industrielle Kontrollsysteme.
BSI IT-Grundschutz-Kataloge, 15. Ergänzung 2016 BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz (V1.2 2014) BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz	2016	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1 bis 100-4 eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Informations-Sicherheits-Management-Systems (ISMS). Die IT-Grundschutz-Kataloge beschreiben die Umsetzung der damit einhergehenden Massnahmen und Ziele. Das damit aufgebaute ISMS erfüllt die Anforderungen von ISO 27001 und verfügt über ein Äquivalent zu den Handlungsempfehlungen von ISO 27002. Sicherheit kann nach den vom BSI entwickelten Vorgehensweisen des IT-Grundschutzes, aber auch nach Standards der ISO 27000-Familie eingeführt und kontrolliert werden. Beide Möglichkeiten sind von ihrem Ansatz her kompatibel. Mit beiden wird ein ISMS aufgebaut und betrieben, mit den Risiken im Bereich der Informationssicherheit ermittelt und durch geeignete Massnahmen auf ein akzeptables Mass reduziert werden. Ein wesentlicher Bestandteil eines ISMS nach ISO 27001 ist die Risikoanalyse und -bewertung, wohingegen eine Risikoanalyse beim BSI-Grundschutz nur in besonderen Fällen erforderlich ist. In den BSI-Grundschutzkatalogen wird die detaillierte Vorgehensweise zur Minimierung von Risiken beschrieben. Demnach lassen die ISO-Standards mehr Interpretation offen und sind flexibler, geben aber auch entsprechend weniger detailliert Anleitung und Unterstützung. Für den IT-Grundschutz-Ansatz gilt demnach das Gegenteil und bietet, wie der Name aussagt, einen «Grundschutz». Der Aufwand für eine ISO-basierte Zertifizierung ist geringer.
BSI ICS Security – Kompendium	2013	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Das Kompendium stellt ein Grundlagenwerk dar und soll einen einfachen Zugang zur SCADA IT Security ermöglichen. Erläutert werden die notwendigen SCADA-Grundlagen, Abläufe, relevante Standards und ein konkreter Zusammenhang zum IT-Grundschutz, wobei auch Unterschiede und Lücken etablierter Standards und insbesondere des IT-Grundschutzes im Bereich SCADA-Security aufgezeigt werden.
BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS)	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Der Standard beschreibt ISMS-relevante Methoden, Aufgaben und Aktivitäten, die ein erfolgreiches ISMS ausmachen und welche Aufgaben auf die Führungsebene zukommen. Bei der Umsetzung der Empfehlungen hilft die Methodik des IT-Grundschutzes, die eine Schritt-für-Schritt-Anleitung für die Entwicklung eines ISMS in der Praxis gibt und konkrete Massnahmen für alle Aspekte der Informationssicherheit nennt. Der Standard 100-1 richtet sich an Verantwortliche für den IT-Betrieb, Sicherheitsbeauftragte, -experten und -berater, die mit dem Management für Informationssicherheit betraut sind.
BSI-Standard 100-2 IT-Grundschutz Vorgehensweise	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Die IT-Grundschutz-Vorgehensweise beschreibt Schritt für Schritt, wie ein Managementsystem für Informationssicherheit in der Praxis und mit Hilfe der Grundschutzkataloge aufgebaut und betrieben werden kann. Es wird sehr ausführlich

Titel	Jahr	Herausgeber und Beschreibung
		darauf eingegangen, wie ein Sicherheitskonzept in der Praxis erstellt wird, wie angemessene Sicherheitsmassnahmen ausgewählt werden und was bei der Umsetzung zu beachten ist.
BSI-Standard 100-3 Risikoanalyse	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Durchführung von Risikoanalysen, die ein bestehendes IT-Grundschutz-Sicherheitskonzept ergänzen. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen als Hilfsmittel verwendet. Ein wesentlicher Unterschied zu den meisten anderen Risikoanalysemethoden ist das gänzliche Weglassen von Eintrittswahrscheinlichkeiten von Schadensereignissen.
BSI-Standard 100-4 Notfallorganisation	2008	Hrsg.: **Bundesamt für Sicherheit in der Informationstechnik (BSI)** Dieses Dokument beschreibt eine Methodik zur Etablierung eines Notfallmanagements, die auf die in Standard 100-2 beschriebenen Vorgehensweisen aufsetzt und ergänzt. Beschrieben werden sämtliche Prozesse innerhalb einer Notfallorganisation von Business Impact Analyse über Krisenmanagement bis hin zu Rückführung und kontinuierlichen Prozesstätigkeiten ausserhalb von Krisensituationen.
ISA 95 / ISO 62264 Enterprise Control System Integration	2010 ff	Hrsg.: **International Society of Automation (ISA)** Eine Normenreihe von insgesamt fünf Standards zur Integration von Unternehmens-IT und Kontroll-Leitsystemen.
Framework for Improving Critical Infrastructure Cyber Security	2014	Hrsg.: **National Institute of Standards and Technology (NIST)** Dieses Framework stammt aus der Forderung der US Presidential Executive Order «Improving Critical Infrastructure Cyber Security» aus dem Jahre 2013. Es ist eine Zusammenstellung verschiedener Guidelines, um den aktuellen Status in einem Unternehmen zu ermitteln und eine Roadmap zu verbesserten Cyber Security-Praktiken mit Verweisen zu anderen Frameworks und Standards wie ISO27001, ISA 62443, NIST 800-53 und Cobit zu definieren.
Communication network dependencies for ICS/SCADA Systems	2016	Hrsg.: **European Union Agency for Network and Information Security (ENISA)** Dieser Bericht konzentriert sich auf die Aspekte der Kommunikationsnetze und der Interkommunikation zwischen ICS/SCADA und der Erkennung von Schwachstellen, Risiken, Bedrohungen und Sicherheitsauswirkungen, die durch cyberphysikalische Systeme verursacht werden können. Der Bericht enthält auch eine Reihe von Empfehlungen zur Minderung der identifizierten Risiken. Das wichtigste Ergebnis der vorgängigen Studie ist eine Liste von bewährten Praktiken und Richtlinien, um die Angriffsfläche von ICS/SCADA-Systemen so weit wie möglich zu begrenzen. Hauptziel des Dokumentes ist es, einen Einblick in die Kommunikationsnetzwerkabhängigkeiten der ICS/SCADA-Systeme zu geben sowie kritische Sicherheitsressourcen und realistische Angriffsszenarien und Bedrohungen gegen diese Kommunikationsnetze zu identifizieren.
Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU). Das erweiterte 10-Punkte-Programm schafft mehr Schutz.	2005	Hrsg.: **InfoSurance** Der Verein InfoSurance hat sich seit Jahren mit den Risiken beim Einsatz von IT in KMU auseinandergesetzt. Um die Unternehmen bei der Einführung eines entsprechenden Schutzes zu unterstützen, hat InfoSurance 2005 die Broschüre 10-Punkte-Programm für einen wirkungsvollen IT-Grundschutz publiziert.

Tab. 3 Nationale und internationale Standards zur IKT-Sicherheit

4.2 Glossar

Abkürzung	Beschreibung
BABS	Bundesamt für Bevölkerungsschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWL	Bundesamt für wirtschaftliche Landesversorgung
DMZ	Demilitarized Zone, Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten (wird oft benutzt um eine logische Trennung zwischen zwei Netzwerkzonen zu generieren)
DNS	Domain Name System
eDec	Elektronische Datendeklaration. System der eidgenössischen Zollverwaltung für Importzollanmeldungen
EDV	Elektronische Datenverarbeitung
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Ressource Planning - System
Facility Control	Gebäudetechnik, Steuerung und Überwachung von Anlagen
Field	Feldebene
FINMA	Eidgenössische Finanzmarktaufsicht
HIDS	Host Intrusion Detection System
HMI	Human Maschine Interface, Stelle oder Handlung, mit der ein Mensch mit einer Maschine in Kontakt tritt
IaaS	Infrastructure as a Service
ICS	Siehe SCADA
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnologie (dt. elektronische Datenverarbeitung EDV)
IP	Internet Protocol
IPS	Intrusion Prevention System
ISA	International Society of Automation
ISO	Internationale Organisation für Normung
ISB	Informatiksteuerungsorgan des Bundes
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnologie
Kommunikationsnetzwerk	Netzwerk zur internen Daten- und Sprachkommunikation
Leittechnik	Netz-, Stations- und Kraftwerksleittechnik
MELANI	Melde- und Analysestelle Informationssicherung (Informatiksteuerungsorgan des Bundes)
NIST	National Institute of Standards and Technology
MOU / MOA	Memorandum of Understanding / Agreement
MPLS	Multiprotocol Label Switching, im Datenkommunikationsverkehr verwendete Technologie
MPLS-TP	Multiprotocol Label Switching Transport Profile
NAC	Network Access Control
OT	Operational Technology (insbesondere SCADA-Systeme)
PaaS	Platform as a Service
PC	Personal Computer
PDH	Plesiochronous Digital Hierarchy, eine im Sprach- und Datenkommunikationsverkehr verwendete Technologie

Private Range	Private IP-Adressen (abgekürzt Private IP) sind IP-Adressen, die von der IANA nicht im Internet vergeben sind. Sie wurden für die private Nutzung aus dem öffentlichen Adressraum ausgespart, damit sie ohne administrativen Mehraufwand (Registrierung der IP-Adressen) in lokalen Netzwerken genutzt werden können.
PRTG Network Monitor	PRTG Network Monitor ist eine umfassende Netzwerk-Monitoring-Lösung zur Überwachung von Up-/Downtime, Traffic und Nutzung.
SaaS	Software as a Service
SCADA	Supervisory Control and Data Acquisition, Überwachen und Steuern technischer Prozesse. Zum SCADA-System gehören die Sensoren, Leitungen, Computer und Leitstelle des (Produktions-) Systems. Gemeint sind insbesondere Kommissioniersysteme, Produktionssteuerungssysteme der Verarbeiter sowie Kassensysteme der Detailhändler. Wird synonym zum Begriff ICS verwendet. Beinhaltet auch die SPS-Steuerungen.
SPS	Speicherprogammierbare Steuerung, siehe SCADA.
SDH	Synchronous Digital Hierarchy, eine im Sprach- und Datenkommunikationsverkehr verwendete Technologie
SIEM	Security Incident and Event Management
SLA	Service Level Agreement, Dienstleistungsvereinbarung
SQL	SQL ist eine Datenbanksprache zur Definition von Datenstrukturen in relationalen Datenbanken sowie zum Bearbeiten (Einfügen, Verändern, Löschen) und Abfragen von darauf basierenden Datenbeständen.
Thin-Client	Ein Thin Client, lean client oder slim client (englisch dünner, schlanker bzw. magerer Client) ist ein Client, d. h. ein Computer oder Programm, das auf die Hilfe eines Servers angewiesen ist, um seine Aufgaben zu erfüllen.
VoIP	Voice over IP
VPN	Virtual Private Network
VTN	Verordnung über die Sicherstellung der Trinkwasserversorgung in Notlagen
WAN	Wide Area Network

Tab. 4 Abkürzungsverzeichnis

4.3 Abbildungsverzeichnis

4.4 Tabellenverzeichnis