Security-Self-Assessment in kritischen Infrastrukturen

Jörg Schneider[1] · David Fuhr[1] · Edgar Korte[2] · Christof Thim[3]

[1]HiSolutions AG
{schneider | fuhr@hisolutions.com}

[2]Pretherm GmbH
edgar.korte@pretherm.de

[3]Universität Potsdam
Christof.Thim@wi.uni-potsdam.de

Zusammenfassung

Die Bedrohungslage bezüglich Cybervorfällen hat sich für kritische Infrastrukturen in den letzten Jahren weiter verschärft. Die Regulierung versucht dem mit Vorgaben für große Betreiber wie dem IT-Sicherheitsgesetz gerecht zu werden. Kleine und mittlere Betreiber kritischer Infrastrukturen stehen damit vor der doppelten Herausforderung, mangels gesetzlicher Anforderungen einerseits ihre eigene Lösung finden und zweitens dies mit ihrem begrenzten Budget an Finanzen und Personal stemmen zu müssen. Im BMBF-geförderten Forschungsprojekt Aqua-IT-Lab wurde eine Methodik entwickelt, die kleinen und mittleren Betreibern von Wasserver- und -entsorgungsanlagen erlaubt, die IT-Sicherheit ihrer Automatisierungstechnik mit begrenztem Aufwand und ohne tiefes Security-Fachwissen selbst abzuschätzen, um so risikobasiert ressourcenschonend die wichtigsten Umsetzungsschritte planen zu können. Die Methodik lässt sich zudem auf andere Sektoren wie Energie übertragen.

1 Security in kritischen Infrastrukturen

1.1 Bedrohungen

Kritische Infrastrukturen (KRITIS) besitzen ein besonderes Cyber-Risikoprofil. Zum einen eröffnen die zunehmende Automatisierung und Vernetzung eine Vielzahl neuer Angriffsvektoren. Zum anderen professionalisieren sich die Angreifer und damit einhergehend deren Tools zusehends. Spätestens seit den Angriffen auf Energieanlagen in der Ukraine 2015 [UKR16] ist klar, dass Täter auch in Europa zunehmend ressourcenstark sowie mit tiefgehendem Fachwissen ausgestattet agieren und häufig nachrichtendienstlich gesteuert sein dürften.

1.2 Anforderungen

Dazu passend gelten im KRITIS-Umfeld zumindest für größere Betreiber besondere Anforderungen wie gesetzliche Regelungen. Hier sind vor allem zu nennen das IT-Sicherheitsgesetz [ITSG15] samt KRITIS-Verordnung [KRIT17] zur Bestimmung der von diesem betroffenen Anlagen. Hinzu kommen sektorspezifische Anforderungen wie der IT-Sicherheitskatalog

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 193-203.

[ITSK15] für Energienetzbetreiber. Für den Wassersektor in Deutschland gelten weitere Regularien (s.u.).

1.3 Herausforderungen für kleinere Betreiber

Die Bedrohungslage stellt insbesondere kleinere Betreiber vor Herausforderungen. Wir verstehen unter kleineren Betreibern solche, die nicht unter das IT-Sicherheitsgesetz fallen, also in der Regel weniger als 500.000 Menschen mit kritischen Dienstleistungen (z.B. Wasser oder Energie) versorgen bzw. für deren ebenso kritische Entsorgung zuständig sind. Bei diesen ist häufig die IT-Kompetenz auf wenige, manchmal gar einen Mitarbeiter konzentriert. Spezielle IT-/ICS-Security-Kenntnisse sind selten und meist nicht umfassend vorhanden. Gleichzeitig ist kein Budget für den Einkauf größerer Kontingente externer Beratungsdienstleistungen vorhanden. Dies wird sich voraussichtlich auch in absehbarer Zukunft nicht ändern.

1.4 Besonderheiten im Wassersektor

Unter den kritischen Infrastrukturen stechen Wasserver- und -entsorgungsbetriebe in mehrfacher Hinsicht heraus:

1. Aufgrund der Eigentümerstrukturen und der sich vergleichsweise langsam entwickelnden Grundprozesse kommt teilweise noch deutlich ältere Automatisierungstechnik zum Einsatz als in anderen KRITIS-Sektoren. 30 Jahre alte Automatisierungs- und Nachrichtentechnik ist keine Seltenheit.
2. Die IT-Vernetzung hat noch nicht alles durchdrungen, ist aber stetig auf dem Vormarsch, zumindest zur Überwachung. Dies bekommt zukünftig weiteren Auftrieb durch Themen wie Smart Metering.
3. Aufgrund der räumlichen Verteilung in der Fläche in Kombination mit steigendem Kostendruck findet zunehmend Nutzung fremder Infrastruktur statt, etwa von angemieteten MPLS-Netzen anstelle der traditionell vorhandenen eigenen Leitungen.
4. Bezogen auf die weiten Wege, die im (IT-)Notfall zu bewältigen sind, um Störungen zu beheben oder die Steuerung manuell durchzuführen, ist relativ wenig Personal vorhanden, mit weiter sinkender Tendenz.
5. Es existieren für die unterschiedlichen Prozesse verschiedene „analoge“ Sicherheitsmechanismen wie manuelle Messungen der Wasserqualität, welche jedoch in der Regel nicht in Echtzeit arbeiten.

1.5 Konsequenzen für das Vorgehensmodell

Im Wassersektor kommen vier Effekte zusammen, die die Nutzung einer Vorgehensweise analog zum IT-Grundschutz nach BSI-Standard 100-2 in Frage stellen:

1. Höherer Schutzbedarf
   Da es sich beim Wassersektor um eine kritische Infrastruktur handelt, liegt zumindest für die Technik zur Steuerung der Prozesse fast immer hoher, häufig sogar sehr hoher Schutzbedarf vor. Die Basisabsicherung des IT-Grundschutzes genügt dadurch grundsätzlich nicht.
2. IT-untypische Einsatzszenarien
   Da der IT-Grundschutz für die öffentliche Verwaltung entwickelt und von da aus nach

und nach für klassische private Unternehmen geöffnet wurde, betrachtet er vor allem Einsatzszenarien der Office-IT, von Rechenzentren, Bürogebäuden und Arbeitsplätzen. Die entscheidenden IT-Prozesse der Wasserver- und entsorgung hingegen werden in Warten, Klärwerken, Pumpstationen und anderen Außenstellen betrieben, worauf die Maßnahmenbündel nicht ausgelegt sind.

3. Fehlende Bausteine für Automatisierungstechnik
   Dazu kommt, dass für die wichtigsten Komponenten der Automatisierungstechnik – SPSen, Prozessleitsysteme, Feldbus- und Fernwirktechnik sowie Programmiergeräte – keine Bausteine vorhanden sind. Zwar hat das BSI Ende 2016 einen Baustein IND.1 „ICS-Betrieb“ für komponentenübergreifende, konzeptionelle und architektonische Sicherheitsanforderungen für ICS-Anlagen als Community Draft veröffentlicht und weitere sind in Arbeit (SPS, HMI, Fernwirksystem, Leitwarte). Diese stehen jedoch Stand heute noch nicht zur Verfügung, sodass auf weiten Strecken manuelle Analyse notwendig ist.
4. Ressourcenmangel für die Risikoanalyse
   Die genannten Probleme werden dadurch verschärft, dass kleine Betreiber von Wasserinfrastrukturen in der Regel weder über ausreichend eigene Kompetenzen noch Ressourcen verfügen, um die nicht zuletzt auch für die Wirtschaftlichkeit notwendige Risikoanalyse vorzunehmen.

2 Schutzkonzepte im Wassersektor

Kritische Infrastrukturen werden spätestens seit den Terroranschlägen und Naturkatastrophen nach 2000 als besonderes Schutzgut erkannt. Die Trinkwasserversorgung stand dabei vom Anfang an mit im Blickpunkt der Überlegungen. Der DVGW e.V. als der für die Beschreibung des „Stands der Technik“ verantwortliche Regelsetzer der Wasserwirtschaft hat 2008 mit seiner Technischen Mitteilung [W1001] eine Vorgehensweise entwickelt, wie sich Wasserversorger in Normalzeiten auf Krisenlagen vorbereiten können. Ausgangspunkt ist eine Gefährdungsanalyse, in der die Gefährdung der verschiedenen Prozesse des Versorgers entlang der Gewinnungs-, Aufbereitungs-, Förderungs-, Speicherungs-, Transport- und Verteilungskette des Versorgers untersucht wird. Dabei werden die Auswirkungen unterschiedlicher Gefährdungen (z.B. unterteilt in Naturkatastrophen, menschliches oder technisches Versagen und schwere Kriminalität und Terrorismus) auf die einzelnen Prozesse untersucht und bewertet. Die Analyse kulminiert in einer Risikoabschätzung, in der Eintrittswahrscheinlichkeit und Schadensausmaß der verschiedenen Gefährdungen in eine 3x3-Matrix zusammengefasst werden:

Tab. 1: Risikomatrix

Eintrittswahrscheinlichkeit	Gering	Mittel	Hoch
Hoch	Mittleres Risiko	Hohes Risiko	Hohes Risiko
Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
Gering	Niedriges Risiko	Niedriges Risiko	Hohes Risiko

Schadensausmaß

Die Gesamtsicht erlaubt dann eine vergleichende Risikoabschätzung, die wiederum Grundlage für eine nach Prioritäten geordnete Maßnahmenplanung zur Risikobeherrschung ist. Die Bewertung der Schadenswahrscheinlichkeit erfolgt dabei semi-quantitativ, quantitativ oder auf qualitativer Basis. Insbesondere bei Gefährdungen, die sich aus absichtlichen Handlungen wie kriminellen oder terroristischen Aktionen ergeben, geraten Wahrscheinlichkeitsbetrachtungen jedoch an ihre Grenzen, die häufig zu einer normierten Einordnung der Wahrscheinlichkeit als „mittel“ oder „niedrig“ führen. IT-Risikoanalysen etwa nach der IT-Grundschutzvorgehensweise des BSI verzichten aus diesem Grund seit langem auf solche Wahrscheinlichkeitsbewertungen und untersuchen stattdessen, ob eine bestimmte Gefährdung grundsätzlich zutreffend ist. Wenn diese Möglichkeit bejaht wird, sind in jedem Fall geeignete Maßnahmen für ein normales Schutzniveau zu ergreifen, bei höherem Schutzbedarf ist eine detaillierte spezifische Risikoanalyse vorzunehmen. Grundsätzlich stellt sich daher die Frage, ob zwei unterschiedliche Ansätze der Risikobewertung parallel durchgeführt werden oder ob das zuvor beschriebene Konzept mit den in der IT entwickelten Analysemethoden verzahnt werden soll.

Im Forschungsprojekt Aqua-IT-Lab wurde letzterer Weg beschritten. Das entwickelte Self-Assessment-Tool sieht eine Analyse vor, die sich in die oben beschriebene Risikomatrix integrieren lässt. Nur so kann ein einheitliches Schutzkonzept erarbeitet werden, in dem auch eine optimale Zuteilung der für Sicherheit vorhandenen Ressourcen möglich ist. Die IT-Risikoanalyse ist demnach eine Teilbetrachtung des gesamten Risikomanagements des Betreibers.

3 Self-Assessment

Im Forschungsprojekt Aqua-IT-Lab wurde ein Self-Assessment-Tool entwickelt, mittels dessen kleine und mittlere Betreiber im Wassersektor aufwandsarm und selbsterklärend ein Risikoprofil erstellen können. Darüber hinaus werden durch das Tool automatisch priorisierte Handlungsempfehlungen generiert, die eine erste Grobplanung der Maßnahmenumsetzung ermöglichen.

Ein Self-Assessment, also eine möglichst weit automatisierte Selbsteinschätzung des Stands der ICS-Security beim Betreiber durch die IT-Verantwortlichen selbst, stellt ein naheliegendes Mittel dar, um den initialen Aufwand für eine Risikoanalyse niedrig zu halten. Gleichzeitig verspricht eine fundierte Methodik, die Prioritäten von Anfang an richtig setzen zu können. So kann einerseits vermieden werden, dass der Betreiber nichts unternimmt, da die Verantwortlichen nicht wissen, wo sie anfangen sollen, als auch andererseits, dass kein Aktionismus entsteht, der viel Aufwand in Kleinigkeiten investiert, welche der Gesamtsicherheit wenig nützen oder die knappen Ressourcen unwirtschaftlich binden.

Im den folgenden Unterkapiteln werden die Herausforderungen beschrieben, welche ein solches Tool meistern muss:

3.1 Mangel an Security-Wissen

Um von den Verantwortlichen beim Betreiber sinnvoll eigenständig ausgefüllt werden zu können, darf das Tool zwar sehr gutes Branchenwissen des Wasserfachs sowie gute Fachkenntnisse der Automatisierung voraussetzen, jedoch kein tiefgehendes Security-Spezialwissen. Daher müssen die Fragen so gestellt werden, dass sie einen typischen Nutzer des Tools wie den IT- oder Betriebsverantwortlichen mit großer Wahrscheinlichkeit zu sinnvollen Eingaben und da-

mit Auswertung leiten. Dies konnte in der Entwurfsphase des Tools durch iterative Feedbackrunden mit den Praxispartnern Wasser- und Abwasserzweckverband Calau sowie Stadtwerke Brandenburg (Havel) erreicht werden.

3.2 Zeitliche Ressourcen

Security ist für die Betreiber nur eins von vielen Themen, welche sie mit begrenzten Ressourcen abdecken müssen. Um eine Akzeptanz in der Branche zu erreichen, darf der initiale Aufwand nicht zu hoch sein bei gleichzeitiger Aufrechterhaltung des Anspruchs fundierter Ergebnisse. Im Projekt wurde empirisch eine maximale Fragenanzahl von ca. 50 ermittelt, was einer erstmaligen Ausfüllzeit von 1 ½ bis 2 Stunden entspricht. Eine besondere Schwierigkeit stellen Fragen da, die von einem Nutzer allein nicht beantwortet werden können und erst Rücksprache benötigen. Da jeglicher Verzug hier die Fortführung der Nutzung des Tools gefährdet, mussten solche Fragen vermieden und die entsprechenden Informationen über andere, indirekte Fragen ermittelt werden. Die Repräsentativität der Fragen und eine angemessene Wichtung der Themen und Anforderungen wurden durch eine allgemeine Bedrohungs- und spezifische Risikoanalyse des Wassersektors anhand von einschlägigen Quellen (Standards und Richtlinien), Interviews und Fallstudien ermittelt (s.u.).

3.3 Inhomogenität im Feld

Die Auswertung von Fallstudien hat bestätigt, dass die Heterogenität bezüglich Security – zu begreifen als Vektor über die Themen – sehr groß ist. Da das Tool in der Nutzung nicht begleitet werden kann, muss die Auswertung derart strukturiert sein, dass sie sowohl Betreibern, die noch ganz am Anfang stehen, als auch Betreibern, die schon ein CSMS[1] etabliert haben, nützliche Anhaltspunkte gibt – ohne erstere zu frustrieren oder zweitere zu demotivieren. Erreicht werden konnte dies durch eine strukturierte Fragenführung nach Themenblöcken, die einzeln gefiltert und ausgeblendet werden können. So ist es möglich, zunächst ein Bild des eigenen Risikoprofils bezüglich bestimmter Themen wie Notfallplanung oder Kommunikation zu erhalten. Sukzessive können bei Beschäftigungen mit weiteren Themen diese in die Auswertung mit eingeschlossen werde. Zudem erfolgt eine mehrstufige „pädagogische“ Auswertung in dem Sinn, dass bei niedrigem Reifegrad nicht eine lange Liste von Versäumnissen ausgegeben wird, sondern angepasst an das jeweilige Level das realistisch innerhalb eines gewissen Zeitraums (z.B. ein Jahr) erreichbare Pensum. Anfangs wird lediglich eine Liste von wenigen sogenannten „KO-Anforderungen“ – Management-Attention, Verantwortlicher für Security, Ressourcen/Budget – abgefordert, solange eine von diesen noch nicht erfüllt ist.

3.4 Dynamik in der Regulierung

Aktuell besteht im Bereich KRITIS in Deutschland die besondere Situation, dass sich die Regulierung in den verschiedenen Sektoren unterschiedlich schnell voran bewegt. Während im Energiebereich die Anforderungen bereits klar definiert sind, wird der Branchenstandard Wasser seit langem erwartet. Das Tool muss daher derart anpassbar sein, dass neue Entwicklungen in den gesetzlichen Vorgaben einfach integriert werden können, ohne die grundsätzliche Auswertungslogik in Frage zu stellen oder frühere Auswertungen unbrauchbar zu machen. Dies

[1] Cyber Security Management System, auch IACS-SMS – Industrial and Automation Control Systems Security Management System.

kann ebenfalls durch die oben beschriebenen KO-Kriterien abgebildet werden, welche sich mit neuen regulatorischen Anforderungen leicht ergänzen lassen.

3.5 Sprache

Ein wichtiges Beispiel für sprachliche Inkompatibilität ist das der Zonen bzw. Zonierung. In der IT(-Security) ein Fachbegriff, wird im Wassersektor hierunter meist ein räumliches oder prozessororientiertes Segmentierungsmodell verstanden. Zur Vermeidung von Missverständnissen war es daher notwendig, an allen entsprechenden Stellen konsequent von „IT-Zonen“ zu sprechen und dies, wo immer notwendig, durch konkrete Umsetzungshinweise wie Bezug auf Firewalls und ähnliche Techniken zu unterfüttern.

3.6 Skalen

Als besonderes Problem entpuppte sich die Skalierung bzw. Normalisierung des Self-Assessments. Da unter den kleineren Wasserbetreibern eine große Spannbreite der Strategie und Umsetzung von Security herrscht, muss die Auswertungsmethodik selbstskalierend definiert werden, um in jedem Bereich sinnvolle und trennscharfe Aussagen treffen zu können.

4 Aqua-IT-Lab Self-Assessment-Tool

Als Lösung für die genannten Herausforderungen wurde im BMBF-geförderten Forschungsprojekt Aqua-IT-Lab zunächst eine Self-Assessment-Methodik entwickelt und darauf aufbauend ein Self-Assessment-Tool für kleinere Betreiber im Wasser-Umfeld. Auf Basis der ISO 2700x-Reihe, des IT-Grundschutzes, der IEC 62443 sowie weiterer branchenspezifischer Sicherheitsstandards ermöglicht der Schnelltest eine Bewertung des Reifegrades der IT-Sicherheit in 11 Dimensionen. Mit insgesamt 50 Fragen werden die größten Lücken in der IT-Sicherheit identifiziert und automatisiert Vorschläge zu deren Behandlung gegeben. Die Priorisierung der Handlungsempfehlung sorgt dafür, dass sie in handhabbaren Projekten mit flexiblem Ressourcenaufwand umgesetzt werden können.

Die Themenbereiche umfassen dabei nicht nur klassische Themen der Sicherheit der Office-IT, sondern greifen auch die Besonderheiten der Operational Technology auf. Der Umgang mit der Sicherheit der Steuerungstechnik im gesamten Komponentenlebenszyklus ist das Kernstück zum Erhalt der Versorgungssicherheit. Zur Verfeinerung der Schnelltestergebnisse wurde daher die Business Impact Analyse (BIA) der IT auf den Wasserversorgungsprozess angepasst, um Komponenten zu identifizieren, welche eines priorisierten Schutzes bedürfen. Der Schnelltest orientiert sich somit an den zu erwartenden Security-Branchenstandards des Wassersektors, [W1060] (B3S – branchenspezifischer Sicherheitsstandard).

5 Maßnahmenkataloge

5.1 Statische Maßnahmenkataloge

Eine der Besonderheiten der IT-Grundschutzmethodik ist es, dass in den Bausteinen für bestimmte Zielobjekte neben den Standardgefährdungen für diese Assets feste Maßnahmen aufgeführt sind. Diese Maßnahmen sind umzusetzen, um eine Basisabsicherung zu erreichen. Es bleibt lediglich zu überprüfen, welche Maßnahmen bereits umgesetzt sind („Basis-Sicherheit-

scheck“, BSC) und welche ggf. überflüssig sind bzw. an konkrete lokale Gegebenheiten angepasst werden müssen. Der große Vorteil dieses Vorgehens ist, dass bei „normalem“ Schutzbedarf die aufwändige Risikoanalyse eingespart werden kann. Letztere ist lediglich in einem der folgenden drei Fälle durchzuführen:

1. höherer Schutzbedarf (hoch oder sehr hoch),
2. ungewöhnliche Einsatzszenarien oder
3. kein passender Baustein in den Grundschutzkatalogen vorhanden

5.2 Dynamische Maßnahmenkataloge

Im Verbundprojekt Aqua-IT-Lab haben wir versucht, aus dem beschriebenen Grundproblem der Betreiber – Ressourcenknappheit – eine Chance zu machen. Idealerweise führt ein Mangel dazu, dass Kräfte effizient eingesetzt werden.

5.2.1 Verzicht auf betreiberspezifische Risikoanalyse

Es musste also erreicht werden, dass kleine Betreiber auf die Risikoanalyse im ersten Schritt verzichten können. Dies konnte auf zwei Wegen erfolgen: Erstens musste ähnlich wie im Grundschutz die Bedrohungsanalyse allgemein a priori vorgenommen werden – denn die Voraussetzungen wie Akteure, zeitliche Entwicklung der Bedrohungslage, grobe Typen von Prozessen, Anlagen und Technik – sind bei kleinen Betreibern ähnlich. Zweitens waren für die typischen Prozesse und Installationen allgemeine Maßnahmen nach Stand der Technik für den passenden Schutzbedarf – hoch bis sehr hoch – zu entwickeln. Beides konnte geleistet werden durch die Analyse diverser einschlägiger Bedrohungs- und Maßnahmenkataloge, Standards und Richtlinien sowie durch die Erprobung des im Projekt entwickelten Self-Assessments.

5.2.2 Automatische Erzeugung von Maßnahmen

Um in der Ressourcenschonung noch einen Schritt weiter zu gehen, haben wir uns entschlossen, auch den Schritt der Umsetzungsüberprüfung der Maßnahmen (BSC, siehe oben) zu integrieren und halbautomatisch ausführen zu lassen. Zu dem Zweck wurde das Self-Assessment um die automatische Generierung von Handlungsempfehlungen, also High-Level-Maßnahmen, erweitert. Dem zugrunde liegt ein umfangreicher Maßnahmenkatalog, der jedoch nie in Gänze ausgegeben wird, um einen Abschreckungseffekt und Demotivation zu vermeiden, sondern immer gemäß der aktuell geltenden Selbsteinschätzung über 11 Themenfelder die ressourcenoptimal jeweils schutzmaximierenden/risikominimierenden nächsten Maßnahmen berechnet.

6 Maßnahmen für den Wassersektor

Nach [W1001] sind die vom Self-Assessment-Tool vorgeschlagenen und nach Entscheidung des Managements umgesetzten Maßnahmen zu validieren und zu überwachen. Soweit entsprechende Maßnahmen nicht im Regelwerk enthalten sind, soll eine gesonderte Validierung durchgeführt werden. Der Erfüllung dieser Anforderung dient die Auswertungsfunktion des Self-Assessment-Tools. Die erforderlichen Überwachungsmaßnahmen werden über geforderte Audits geregelt.

In vergleichbarer Weise ist eine einheitliche IT-Maßnahmenplanung in das Krisenfall-Management des Versorgers zu integrieren. In der hier relevanten [W1002] des DVGW kommt bei-

spielsweise der Einberufung, Zusammensetzung und Arbeitsweise eines Krisenstabes eine besondere Bedeutung zu. Das im Forschungsprojekt entwickelte Tool berücksichtigt diese Anforderung im Thema „Notfallplanung".

Der Schutz der relevanten Gebäude ist ein Teil der Maßnahmenplanung, der sich traditionell auch in den Zonenkonzepten von IT-Sicherheitsanalysen wiederfindet. Auch das Self-Assessment-Tool enthält eine solche Anforderung. Im Regelwerk des DVGW wird dieser Schutz in der [W1050] („Objektschutz von Wasserversorgungsanlagen") geregelt. Dort wird Bezug genommen auf die Einteilung von Objekten in Widerstandsklassen nach DIN EN 1627. Leitstellen sind demnach nach den Anforderungen der höchsten Widerstandklasse 4 zu schützen. Es ist Aufgabe des Versorgers, die Anforderungen des IT-Zonenkonzeptes mit denen des Objektschutzes nach [W1050] in Übereinstimmung zu bringen.

Neben den speziellen Regelungen des Tools wird an einer Stelle insgesamt die Einhaltung regulatorischer Vorgaben gefordert. Dabei spielt die [W1000] „Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern" eine Rolle. Dort wird zum Beispiel gefordert, dass in einer Aufbauorganisation Zuständigkeiten, Verantwortlichkeiten und Befugnisse „in transparenter und überschneidungsfreier" Art schriftlich festzulegen seien. Das beinhaltet auch die mit allen Unternehmensbereichen eng vernetzte IT-Organisation. Die Ablauforganisation sollte so geregelt sein, dass „Schnittstellen, die durch innerbetrieblich abgegrenzte Aufgabenfelder, bei Kooperationen mehrerer Trinkwasserversorger oder durch Einschaltung von Dienstleistern entstehen" widerspruchsfrei zu regeln sind. Auch hier bestehen für die IT besonders vielfältige Anforderungen.

Trinkwasserversorger benötigen eine „Technische Führungskraft", die „über die erforderlichen Befugnisse verfügt, um in sicherheitsrelevanten und insbesondere hygienischen Angelegenheiten verantwortlich handeln zu können." Damit liegen auch die Entscheidungen über die IT-Sicherheit in Ihren Händen, was bei Qualifikations- und Schulungsmaßnahmen zu berücksichtigen ist.

Zum Abschluss soll noch auf die Trinkwasserverordnung [TrinkwV] hingewiesen werden, die Bürger vor Gefahren schützen soll, die sich aus der Verunreinigung von Trinkwasser ergeben. In der Verordnung werden an einer Vielzahl von Stellen Prozesse beschrieben, die sich der Datenübermittlung, Kommunikation und der Steuerung technischer Prozesse bedienen und damit alle IT-relevant sind. Es ist Aufgabe der IT-Verantwortlichen, diese Prozesse bei ihrer Schutzkonzeptplanung besonders zu berücksichtigen.

In naher Zukunft sind Erweiterungen des Regelwerkes um den Bereich IT-Sicherheit zu erwarten. Sie werden in das noch bis Ende 2017 laufende Forschungsprojekt integriert.

7 Auswertung in der Praxis

Das entwickelte Self-Assessment-Tool wurde in mehreren Iterationen durch die Praxispartner getestet. Infolge des Feedbacks, dass die Sprache der IT-Security für Verantwortliche im Wasserbereich teilweise schwer zugänglich ist, wurden mehrfach Termini und Bezüge angepasst, bis sie mit beiden Diskursen kompatibel waren.

Auswertung - Reifegrad

Thema	Praxis - Minimum	Praxis - Reifegrad	Doku - Minimum	Doku - Reifegrad
01 - Organisation	0%	43%	0%	43%
02 - Dokumentation und Zonen	33%	52%	0%	29%
03 - Datenübertragung	33%	44%	0%	33%
04 - Berechtigungsmanagement	0%	33%	0%	25%
05 - Outsourcing & Fernadministr.	0%	47%	0%	40%
06 - Schadsoftware & Schwachstellen	0%	33%	33%	42%
07 - Wechseldatenträger & mobil	33%	50%	33%	42%
08 - Komponentenlebenszyklus	0%	38%	0%	29%
09 - IT-Störungsmanagement	33%	33%	67%	67%
10 - Notfallplanung	0%	33%	33%	50%
11 - Audit	33%	33%	33%	44%
Gesamtergebnis	0%	41%	0%	38%

Abb. 1: Auswertung statistisch

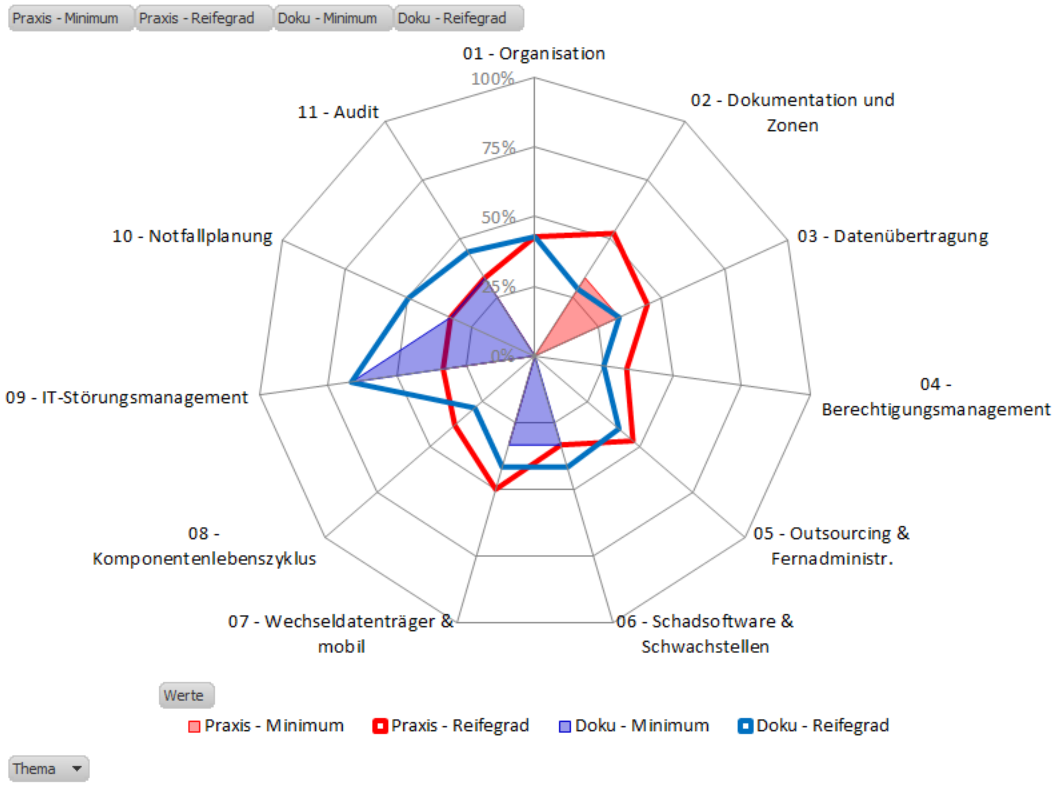

Abb. 2: Auswertung grafisch

7.1 Handlungsempfehlungen

Um das Self-Assessment für die Betreiber lohnenswert zu machen, wurde angeregt, die ebenfalls im Forschungsprojekt für den Wassersektor entwickelten Handlungsempfehlungen spezifisch je Betreiber auszuwerten. Dies umfasst

1. die automatische Auswahl der jeweils notwendigen Handlungsempfehlungen,
2. die spezifische angemessene, d.h. risikobasierte Priorisierung sowie
3. die Beschränkung der priorisierten Auswahl durch Deckelung des im nächsten Iterationsschritt realistisch leistbaren Aufwands.

06 - Schadsoftware & Schwachstellen	27. Virenschutzkonzept	Es existiert ein Virenschutzkonzept, welches alle Systeme, die grundsätzlich durch Schadsoftware bedroht sind, betrachtet und schützt. Systeme müssen entweder - nicht mit Schadsoftware in Berührung kommen können (auch nicht über Wechseldatenträger), - durch Virenschutzmaßnahmen gesichert sein oder - jede Kommunikation zu ihnen auf Schadsoftware überprüft werden. Es wird geprüft, ob der Scanner freigegeben und aktiviert ist. Ausnahmen sind begründet, dokumentiert und es sind alternative Schutzmaßnahmen festgelegt.	Systeme, die nicht per IP vernetzt sind und an die keine Wechseldatenträger angeschlossen werden, benötigen keinen Virenschutz, ebensowenig Rechner auf Unix-Basis oder proprietäre Embedded-Geräte. Alle Windows-Maschinen, die entweder Netzwerkverkehr erhalten oder mit mobilen Datenträgern oder mobilen Geräten (z. B. Programmiergerät) in Kontakt kommen, sollten mit vom jeweiligen Hersteller freigegebenen aktuellen Virenscannern ausgestattet sein oder über alternative Schutzmaßnahmen verfügen (z. B. Whitelisting). Ausnahmen sind zu dokumentieren und zu begründen. Es wird empfohlen, den eingehenden Netzwerkverkehr aus unsicheren Netzen wie dem Internet zu prüfen, z. B. durch Firewallfunktionalität an der Zonengrenze.	33%
	28. Schwachstellenmanagement	Es existiert ein grundsätzlicher Prozess, wie Schwachstellen erkannt (z.B. über bestimmte Informationsquellen) und bewertet werden. Hierfür ist die Verantwortlichkeit festgelegt.	Zu allen eingesetzten Softwareprodukten sollten die Security-Alerts der Hersteller abonniert sein. Der IT-Sicherheitsbeauftragte prüft diese auf Relevanz für die Infrastruktur, passt ggf. die Risikoanalyse an und veranlasst wenn notwendig Maßnahmen.	0%
	29. Umgang mit Schwachstellen	Alle erkannten und als relevant bewerteten Schwachstellen werden so behandelt, dass sie - nicht ausnutzbar sind (Minimierung der Angriffsfläche oder Abtrennung von Systemen), - geschlossen werden (z. B. durch Patching) oder - zumindest eine Ausnutzung schnell und verlässlich erkannt und unterbunden wird.	In einem Schwachstellenbehandlungsplan werden alle erkannten Schwachstellen geführt und bewertet sowie mit Maßnahmen versehen, wenn notwendig. Die Umsetzung dieser Maßnahmen mit Verantwortlichkeit und Priorität wird vom IT-Sicherheitsbeauftragten regelmäßig nachverfolgt. Jede relevante Schwachstelle muss mit einer der folgenden Maßnahmen behandelt sein: - Minimierung der Angriffsfläche oder Abtrennung von Systemen - Schließung der Schwachstelle (z. B. durch Patching) - Einrichtung eines Monitoring zur Erkennung der (versuchten) Ausnutzung der Schwachstelle	33%

Abb. 3: Automatisierte Generierte Handlungsempfehlungen (Auszug)

Für den Betreiber bleiben im Wesentlichen folgende Aufgaben:

1. Verifizierung und Entscheidung der Priorisierung mit der Leitungsebene
2. Planung der Umsetzung und Ressourcen über die Zeit
3. Konkretisierung der Handlungsempfehlungen für die eigenen Rahmenbedingungen
4. Umsetzung der geplanten Maßnahmen

Insbesondere bei letzterem Punkt kann das Vorgehensmodell natürlich nicht helfen. Bei den Punkten 2 und 3 sollte in der Regel die Hilfe eines Beraters hinzugezogen werden, um auch die Umsetzung effizient zu planen und anzugehen.

8 Ausblick

Folgende Punkte bieten sich an für mögliche Weiterentwicklungen des Tools:

8.1 Online-Fähigkeit

Um die Reichweite und damit die Verbreitung des Tools zu erhöhen, bietet sich eine Online-Version an. Im Lauf des Projekts hat sich jedoch die Datenpreisgabe im Internet als starkes Hemmnis erwiesen. Daher ist hierfür zunächst ein Anonymisierungs- bzw. Pseudonymisierungsverfahren zu entwickeln, welches den sicheren Betrieb und die Akzeptanz des Tools als Online-Dienst vertretbar macht.

8.2 Meta-Auswertung: Benchmarking, Trends

Liegen die Daten einmal in anonymisierter, aggregierter Form vor, können Metaauswertungen wie Benchmarks erstellt und den Betreibern zurückgespielt werden. Dies ermöglicht es zum

einen, allgemeine Erkenntnisse zu generieren, zum anderen die Priorisierung und Maßnahmenplanung auf nationaler Ebene zielgenauer zu justieren.

8.3 Förderung von anonymisiertem Wissensaustausch

Im dritten Schritt kann das System Betreibern und weiteren Stakeholdern helfen, zu bestimmten Themen und Herausforderungen in einen für alle Seiten nutzbringenden Austausch zu kommen. Dafür sind weitreichende Governanceüberlegungen zu treffen, abzustimmen und geeignet zu kommunizieren.

Alle genannten Ansätze und die dafür notwendigen (datenschutz-)rechtlichen und technischen Rahmenbedingungen werden etwa u.a. im laufenden Forschungsprojekt ITS.OVERVIEW[2] (gefördert vom BMBF) weiter untersucht.

Literatur

[ITSG15] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – IT-SiG) vom 17. Juli 2015, geändert durch Artikel 5 Absatz 8 des Gesetzes vom 18. Juli 2016, https://www.jurion.de/gesetze/itsg/

[ITSK15] IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_08-2015.pdf?__blob=publicationFile

[KRIT17] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritis-Verordnung – BSI-KritisV) vom 22. April 2016, geändert durch Artikel 1 der Verordnung vom 21. Juni 2017, https://www.gesetze-im-internet.de/bsi-kritisv

[TrinkwV] Trinkwasserverordnung 2001, https://www.gesetze-im-internet.de/bundesrecht/trinkwv_2001/gesamt.pdf

[UKR16] Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case, E-ISAC/NERC 2016, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

[W1000] DVGW Arbeitsblatt W1000: Anforderungen an die Qualifikation und die Organisation von Trinkwasserversorgern, 2016-01

[W1001] DVGW Arbeitsblatt W1001: Sicherheit in der Trinkwasserversorgung – Risikomanagement im Normalbetrieb

[W1002] DVGW Arbeitsblatt W1002: Sicherheit in der Trinkwasserversorgung – Risikomanagement im Notbetrieb

[W1050] DVGW Arbeitsblatt W1050: Objektschutz von Wasserversorgungsanlagen

[W1060] DVGW Regelwerk Security, noch nicht erschienen

[2] Partner: Universität Bonn, HiSolutions AG, Comma Soft AG, KIT, ASW Bundesverband.