Branchenstandard Wasser/Abwasser als Teil von KOMMUNAL 4.0

Mit Einführung des branchenbezogenen IT-Sicherheitsstandards (B3S) Wasser/Abwasser, der im August 2017 vom Bundesamt für Sicherheit und Informationstechnik (BSI) anerkannt wurde, erfüllen Wasserver- und Abwasserentsorger als erster Sektor der kritischen Infrastrukturen die gesetzlichen Anforderungen gemäß § 8a (2) BSI-Gesetz. DWA und DVGW stellen Anwendern den Sicherheitsstandard inhaltsgleich als Teil ihrer Regelwerke (DWA-M 1060 bzw. DVGW-Hinweis 1060) inkl. eines webbasierten Sicherheitsleitfadens zur Verfügung.

Auch wenn die BSI-Kritis-Verordnung (BSI-KritisV) im Kontext des BSI-Gesetzes für die Wasserwirtschaft die Grenze zur Beachtung des IT-Sicherheitsgesetzes bei 500.000 Einwohnern bzw. 22 Mio. m³ Trinkwasser pro Tag festgesetzt hat, lässt sich der nun vorliegende Branchenstandard Wasser/Abwasser genauso gut in kleineren und mittleren Organisationen anwenden. Dies ist auch sinnvoll und wird im Regelwerk explizit empfohlen, denn Hacker oder Datendiebe werden sich kaum an die Grenzen des IT-Sicherheitsgesetzes halten und auch in kleinere Wasser-/Abwassernetze eindringen wollen.

Von wesentlicher Bedeutung bei der Erarbeitung des Branchenstandards war die Beachtung der besonderen Organisationsstrukturen, die in der deutschen Wasserwirtschaft vorherrschen. Die Betriebe setzen sich aus vielen kleinen, einigen mittleren und wenigen großen Organisationen zusammen. Sie verfügen über eine sehr heterogene IT-Landschaft, die durch viele Ergänzungen und Erneuerungen über Jahrzehnte gewachsen ist. Selbst innerhalb einzelner Organisationen sind, historisch bedingt, unterschiedlichste IT-Systeme und Softwareversionen im Einsatz. Hinzu kommt eine sehr breite Spanne

an IT-Know-how. Große Organisationen verfügen naturgemäß über gut ausgebildete IT-Experten, während mittlere und kleine Organisationen vorwiegend auf externes Know-how angewiesen sind. Da das Thema IT-Sicherheit erst seit wenigen Jahren auch für die Wasserwirtschaft von zunehmender Bedeutung ist, verfügen weder ältere Prozessleitsysteme noch die gesamte Organisations-IT über ausreichende Sicherheitskonzepte bzw. zugehörige Systemkomponenten. Diese Rahmenbedingungen müssen nun bei der Erstellung und Umsetzung von Sicherheitskonzepten und Systemlösungen im Sinne des Branchenstandards Wasser/Abwasser beachtet werden.
Als wesentliche Ziele des Branchenstandards Wasser/Abwasser benennt Terhart [1] folgende Aspekte:

- Berücksichtigung aller Anlagen(typen) zur Wasserver- und Abwasserentsorgung nach BSI-KRITIS-Verordnung
- Eignung auch für nicht-kritische Infrastrukturen
- unabhängig von der Ausprägung der IT-Systeme und der Anlagengröße
- Beschreibung bis auf Maßnahmenebene
- Verständlich für die Betreiber (eindeutige Ableitung der zu beachtenden Grundsätze und der zu ergreifenden Maßnahmen)
- Integration in bestehende Regelwerke (DVGW, DWA)
- einfach an den jeweiligen Stand der Technik und die Erkenntnisse des BSI anzupassen

Die Basis für den Branchenstandard bilden der BSI-Grundschutz sowie das BSI-ICS-Security-Kompendium. Zudem ist er kompatibel zu den Vorgaben der DIN ISO/IEC 27001. Die wesentliche Vorgehensweise bei der Umsetzung soll mit einer Web-Applikation unterstützt werden. Diese besteht aus den Bearbeitungsschritten Objektauswahl, Anwendungsfallauswahl, Gefährdungsbestimmung, Risikobewertung (nur bei zusätzlichen Risiken erforderlich), Maßnahmenermittlung, Maßnahmenumsetzung und -sofern erforderlich – Auditierung.

B3S-Struktur Bestandteil von KOMMUNAL 4.0

Die von den Fachgremien der DWA und des DVGW erarbeitete Vorgehensstruktur soll insbesondere den kleinen und mittleren Ver- und Entsorgern einen einfachen Einstieg in die IT-Sicherheit bei gleichzeitiger Einhaltung der BSI-Vorgaben ermöglichen und die notwendige Rechtssicherheit schaffen. Anwendungsfälle für die B3S-Struktur sind der Benutzerzugang, die SPS-/PLS-Programmierung und -wartung, das Netzwerkmanagement, der Programmzugang, die Architektur und die Organisation selbst. Für die Applikationen des Fördervorhabens KOMMUNAL 4.0

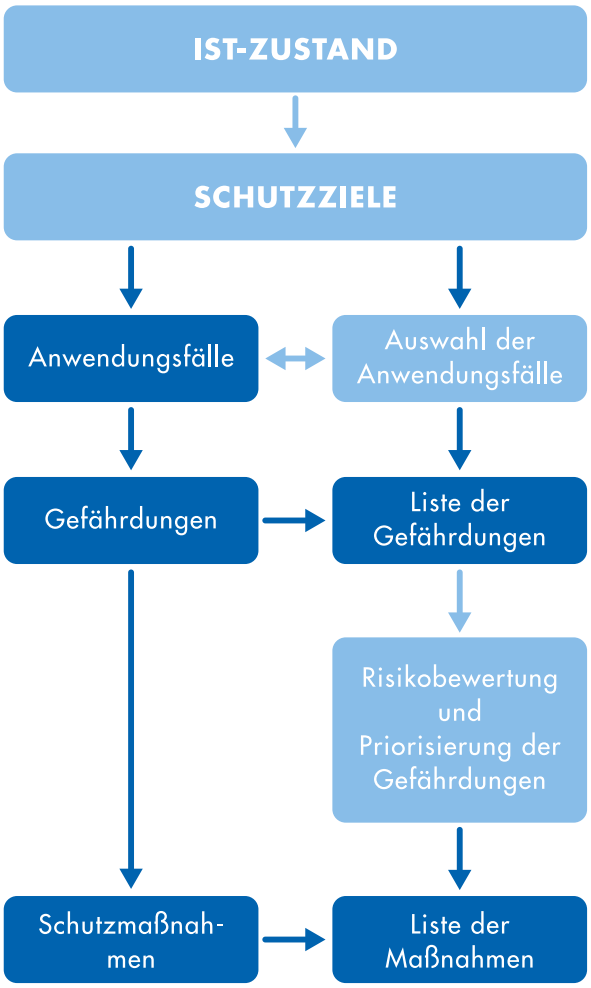

Bild 1: B3S-Struktur und Merkmale [3]

[2] werden die Vorgaben und Anwendungsfälle des Branchenstandards im Sinne des „Security by Design"-Prinzips bereits in der Entwicklungsphase berücksichtigt. Darüber hinaus spielen insbesondere die Anforderungen, die z. B. an den Betrieb einer Applikation in der Cloud gestellt werden (z. B. ISO 27001/27017, BSI-Anforderungskatalog Cloud Computing (C5)), eine besondere Rolle in der Sicherheitskonzeption der Applikationen. Das heißt, Lösungen und Produkte, die aus dem KOMMUNAL 4.0 Projekt hervorgehen, erfüllen von Beginn an alle Anforderungen des Branchenstandards Wasser/Abwasser. Bei der Integration von Systemen/Lösungen/Produkten Dritter in die Plattformumgebung KOMMUNAL 4.0 wird auf eine entsprechende Erfüllung der Branchenstandards geachtet bzw. ist von den jeweiligen Anbietern/Herstellern einzuhalten (Bild 1).
Für die einzelnen Schritte auf dem Weg zu einer rechtskonformen IT-Sicherheitsstruktur stellt ein IT-gestütztes ISMS (Informations-Sicherheits-Management-Sys-

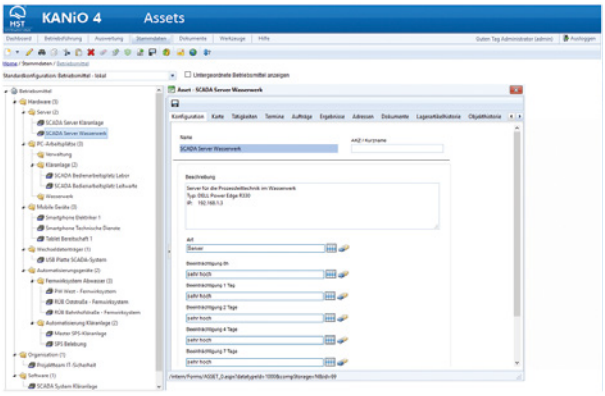

Bild 2: Erfassung und Organisation von Assets in KANiO-ISMS [4]

tem) einen wichtigen Baustein dar. In die KOMMUNAL-4.0-Plattform wird von einem der Projektpartner ein entsprechendes Tool (KANiO-ISMS) integriert. Es kann auch als separate Applikation oder als Bestandteil des Betriebsführungssystems KANiO mit oder ohne Anbindung an die KOMMUNAL-4.0-Plattform verwendet werden. Mit der Toolnutzung werden unkoordinierte Einzelmaßnahmen vermieden, die keinen ausreichend sicheren IT-Betrieb gewährleisten. Zudem stellt das Tool sicher, die eigenen Bemühungen um einen sicheren IT-Betrieb gegenüber Kunden oder dem Gesetzgeber nachzuweisen. Frühere Maßnahmen lassen sich so auch besser mit dem aktuellen Sicherheitsstandard abgleichen.

Das ISMS-Tool ermöglicht ein strukturiertes Vorgehen mit definierten Prozessen und notwendiger Dokumentation (Bild 2). Es erfüllt auch gleichzeitig die Dokumentationsanforderungen der ISO 27001 als wesentlicher Baustein einer Zertifizierung sowie des B3S. Die wesentlichen Funktionsbausteine sind:

- Dokumentenverwaltung zur Dokumentation der IT-Sicherheit
- Stammdatenbereich zur strukturierten Dokumentation aller IT-sicherheitsrelevanten Assets
- Funktionen zur Umsetzung der Risikoanalyse
  - Erfassung von Bedrohungen und Eintrittswahrscheinlichkeiten
  - Erfassung von Beeinträchtigungen
- Automatische Berechnung des Sicherheitsrisikos
- IT-Sicherheitsreport zur Darstellung des aktuellen Sicherheitsstatus
- Auftragsmanagement zur Umsetzung des PDCA-Zyklus
  - Wiederkehrende Sicherheitsprüfungen
  - Checklisten zur Ausführung und Dokumentation der Maßnahmen
  - Integrierter Maßnahmenkatalog nach ISO 27001

Anforderungen an die Erstellung eines Informationssicherheitskonzeptes

Bevor ein ISMS-Tool zum Einsatz kommt, sollte ein Betreiber kommunaler Infrastrukturen ein umfassendes Informationssicherheitskonzept erstellen. Dieses Konzept

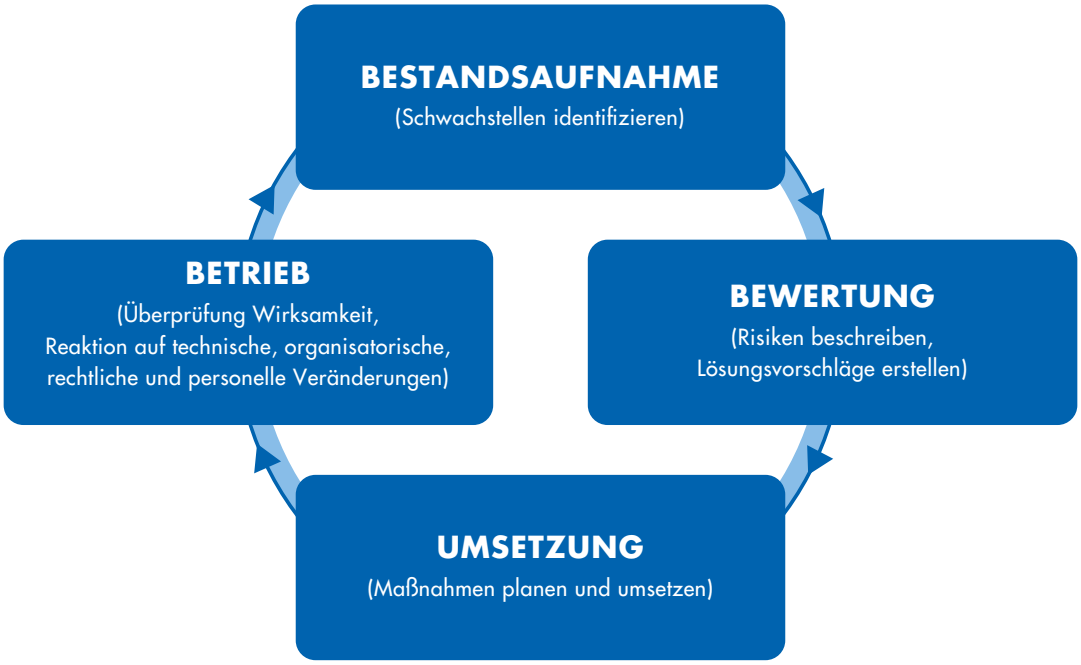

Bild 3: Stufen eines Informationssicherheitskonzeptes [4]

berücksichtigt die Gesamtheit aller vorhandenen Prozesse, deren unterstützende Werte (IT-Systeme, Mitarbeiter, Dienstleister etc.) sowie deren Dokumentation. Zur Umsetzung eines Informationssicherheitskonzepts ist es zunächst notwendig, eine entsprechende Organisationsstruktur aufzubauen, um das dafür notwendige ISMS zu initiieren und steuern zu können. Die Organisationstruktur umfasst grundsätzlich die behördliche Leitung als juristisch verantwortliche Stelle und den Informationssicherheitsbeauftragten als fachlich Verantwortlichen.
Empfehlenswert ist die Einbindung weiterer Fachverantwortlicher, wie der IT-, Personal- und Facility-Leitung, sowie evtl. weiterer (externer) Fachverantwortlicher im Rahmen eines Informations-Sicherheits-Management-Teams (ISMT). Übernehmen nicht-behördliche Organisationen kommunale Aufgaben (Eigenbetriebe, Stadtwerke o. ä.), so sind dabei immer die rechtliche Stellung des Versorgungsbetriebes und die Schnittstellen zu den Prozessen und Dienstleistungen der Kommune zu beachten. Diese sind, wie bei externen Dritten, vertraglich zu regeln und auch innerhalb der Dokumentation klar abzugrenzen. Entsprechend muss der Geltungsbereich definiert und dokumentiert werden (Bild 3).
Mittels einer Asset- und Prozessdokumentation, wie sie mit KANiO-ISMS möglich wird, können zunächst alle Kern- und Unterstützungsprozesse ermittelt und dokumentiert werden. Ziel der Feststellung und Dokumentation ist das Erkennen der Auswirkungen bei Ausfällen von Assets, wie z. B. IT-Systemen, und welche weiteren Teil-/Prozesse von den Ausfällen noch betroffen sein können sowie welche Maßnahmen daraufhin zu ergreifen sind. Dies ist notwendige Grundlage für die Umsetzung eines Business-Continuity- oder IT-Notfallmanagements, die in der ISO 27002 gefordert werden und wichtiger Bestandteil eines Informationssicherheitskonzepts sind.
Nach der Feststellung aller Assets wird im Rahmen einer Schutzbedarfs- und anschließender Risikoanalyse ermittelt, wie kritisch ein Prozess sowie die jeweiligen Assets dafür sind, und welche Risiken bestehen. Erst wenn dies definiert ist, macht eine Umsetzung von Sicherheitsmaßnahmen Sinn, da eine zuvor bereits umgesetzte Maßnahme vielleicht nicht ausreichend ist, weil man den Schutzbedarf oder das Risiko zuvor unterschätzt hat. Im Rahmen der Umsetzungsmaßnahmen müssen alle Prozesse geregelt und dokumentiert werden. Ziel und Zweck ist es, dass Verantwortlichkeiten zu jeder Zeit geregelt, kommuniziert und dokumentiert sind, so dass möglichst keine Unklarheiten offen bleiben. Durch die Umsetzung soll Handlungssicherheit für alle Beteiligten entstehen. Um dies zu erreichen, müssen neben der Erstellung von Leit- und Richtlinien, Verfahrensanweisungen und Prozessbeschreibungen diese auch den Mitarbeitern bekannt gegeben werden. Der Mensch hat gerade für die Informationssicherheit einen enorm hohen Kritikalitätsfaktor. Deshalb ist es sehr wichtig, alle Mitarbeiter bei der Einführung und Umsetzung eines ISMS „mitzunehmen“ und entsprechende Sensibilisierungs- und Schulungsmaßnahmen regelmäßig durchzuführen. Die Einrichtung eines ISMS-Tools zur Prozessführung und -dokumentation ist notwendig, aber als Maßnahme alleine nicht ausreichend.
Zu guter Letzt sind nach der Umsetzung und Dokumentation des Informationssicherheitskonzepts regelmäßige Prüfungen/Audits durchzuführen, um einen kontinuierlichen Verbesserungsprozess zu gewährleisten. Insgesamt betrachtet führt die Umsetzung eines ISMS zu sicheren betrieblichen Prozessen und auf Dauer zu effizienterem Arbeiten.

Literatur:

[1] Dr. Ludger Terhart „B3S Wasser/Abwasser – Wer später anfängt, ist früher fertig“, 10 Jahre UP KRITIS, Quelle: http://www.kritis.bund.de/SharedDocs/Downloads/Kritis/DE/170619_Dr_Ludger_Terhart.pdf?__blob=publicationFile

[2] www.kommunal4null.de

[3] Nico Suchold „ Fluch oder Segen: IT-Sicherheit bei der Digitalisierung kritischer Infrastrukturen“, Vortrag Kolloquium des VDI Arbeitskreises Mess- und Automatisierungstechnik, 15.06.2017

[4] www.hst.de/it-sicherheit

AUTOREN

HEIKO FAUTH
Faktor Sicherheit
72348 Rosenfeld
info@faktor-sicherheit.de

DIPL. WIRT.-INFORM. NICO SUCHOLD
ifak - Institut f. Automation und Kommunikation e.V.
Magdeburg
39106 Magdeburg
Tel.: +49 (0) 391 9901474
nico.suchold@ifak.eu

GÜNTER MÜLLER-CZYGAN
HST Systemtechnik GmbH & Co. KG
59872 Meschede
Tel.: +49 (0) 291-9929-44
guenter.mueller-czygan@hst.de