Praktische IT-Sicherheit in der Wasserwirtschaft

Branchenstandard Wasser/Abwasser als Teil von KOMMUNAL 4.0

Im August 2017 wurde der branchenbezogene IT-Sicherheitsstandard (B3S) Wasser/Abwasser vom Bundesamt für Sicherheit und Informationstechnik (BSI) anerkannt. Damit erfüllt die Wasserwirtschaft als erster Sektor der kritischen Infrastrukturen die gesetzlichen Anforderungen gemäß § 8a (2) BSI-Gesetz. DWA und DVGW stellen den Sicherheitsstandard inhaltsgleich, als Teil ihrer Regelwerke (DWA-M 1060 bzw. DVGW-Hinweis 1060), incl. eines webbasierten Sicherheitsleitfadens, den Anwendern zur Verfügung.

Standard ist für große und kleine Organisationen geeignet

Die BSI-Kritisverordnung (BSI-KritisV) hat im Kontext des BSI-Gesetzes für die Wasserwirtschaft die Grenze zur Beachtung des IT-Sicherheitsgesetzes bei 500 000 Einwohnern bzw. 22 Mio. m^3 Trinkwasser pro Tag festgesetzt. Die Anwendung des vorliegenden Branchenstandards Wasser/Abwasser wird im Regelwerk explizit auch für kleinere und mittlere Organisationen empfohlen, denn Hacker oder Datendiebe halten sich kaum an die Grenzen des IT-Sicherheitsgesetzes. In Deutschland setzen sich die Wasser-/Abwasserbetriebe aus vielen kleinen, einigen mittleren und wenigen großen Organisationen zusammen. Sie verfügen über eine sehr heterogene IT-Landschaft, welche durch viele Ergänzungen und Erneuerungen in Jahrzehnten 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 besonderen Rahmenbedingungen wurden bei der Erstellung des Standards berücksichtigt und müssen nun bei der Erstellung und Umsetzung von Sicherheitskonzepten und Systemlösungen im Sinne des Branchenstandards Wasser/Abwasser beachtet werden.

Nach Terhart [1] beinhaltet der Branchenstandard Wasser/Abwasser folgende wesentliche Ziele:

- 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

Neben der Kompatibilität zu den Vorgaben der DIN ISO/IEC 27001 bildet der BSI-Grundschutz sowie das BSI-ICS-Security-Kompendium die Basis für den Branchenstandard.

Eine eigene Web-Applikation unterstützt den Anwender bei der Umsetzung der Maßnahmen gemäß Branchenstandard. Wesentliche Bearbeitungsschritte sind die Objektauswahl, die Anwendungsfallauswahl, eine Gefährdungsbestimmung, eine Risikobewertung (nur bei zusätzlichen Risiken erforderlich), eine Maßnahmenermittlung, die Maßnahmenumsetzung und – sofern erforderlich – eine Auditierung.

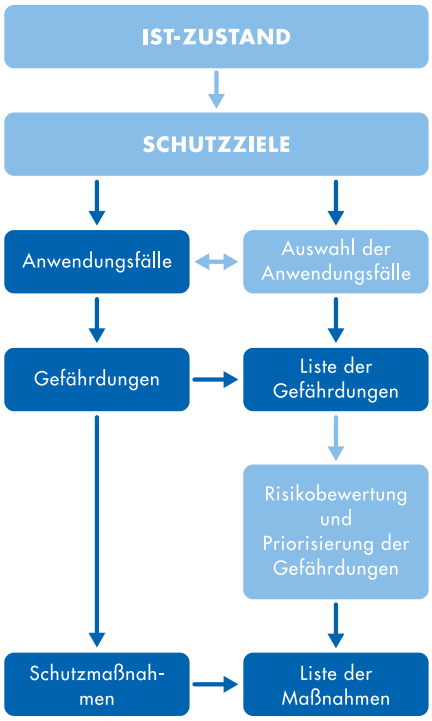
B3S und ISO 27001 Bestandteil von KOMMUNAL 4.0

Zu Beginn werden die Schutzziele gemäß Ist-Zustand definiert und eine Auswahl an in Frage kommenden Anwendungsfällen getroffen. Diese Anwendungsfälle werden im Sicherheitsleitfaden des B3S in die Kategorien Benutzerzugang, SPS-/PLS-Programmierung und -wartung, Netzwerkmanagement, Programmzugang, Architektur und Organisation eingeteilt. Die Vorgehensstruktur der DWA und des DVGW soll insbesondere den kleinen und mittleren Ver- und Entsorgern einen einfachen Einstieg in die IT-Sicherheit ermöglichen. Die Einhaltung der BSI-Vorgaben schafft zudem die notwendige Rechtssicherheit.

Bereits in der Entwicklungsphase werden die Vorgaben und Anwendungsfälle des Branchenstandards im Sinne des „Security by Design" Prinzips für die Applikationen des Fördervorhabens KOMMUNAL 4.0 [2] berücksichtigt. Die dabei umgesetzten Maßnahmen werden sowohl am B3S also auch an der ISO 27001 bzw. ISO 27002 gespiegelt. 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 sicherzustellen.

Anforderungen an die Erstellung eines Informationssicherheitskonzeptes

Ein Kernbestandteil sowohl der B3S als auch im Informationssicherheitsmanagement (ISMS) nach ISO 27001 ist das Erstellen eines umfassenden Informationssicherheitskonzepts. Dieses Konzept 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.

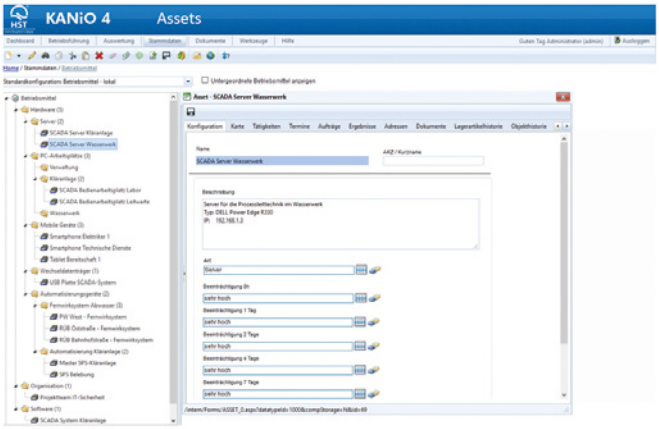


B3S-Struktur und Merkmale [3]

Die Einbindung weiterer Fachverantwortlicher, wie der IT-, Personal- und Facility-Leitung sowie evtl. weiterer (externer) Fachverantwortlicher, im Rahmen eines Informations-Sicherheits-Management-Teams (ISMT) ist empfehlenswert. 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 und wie bei externen Dritten vertraglich zu regeln bzw. innerhalb der Dokumentation klar abzugrenzen. Der Geltungsbereich muss dabei entsprechend definiert und dokumentiert werden.

An Hand einer Asset- und Prozessdokumentation können im ersten Schritt alle Kern- und Unterstützungsprozesse ermittelt und dokumentiert werden. Ziel der Feststellung und Dokumentation ist das Erkennen von Auswirkungen bei Ausfällen der Assets, wie zum Beispiel IT-Systemen, und welche weiteren Teil-/Prozesse von den Ausfällen noch betroffen sein können bzw. welche Maßnahmen daraufhin zu ergreifen sind. Dies ist notwendige Grundlage für die Umsetzung eines Business-Continuity- oder IT-Notfallmanagements, die ebenfalls in der ISO 27002 gefordert werden und wichtiger Bestandteil eines Informationssicherheitskonzepts sind.

Im Rahmen einer Schutzbedarfs- und anschließender Risikoanalyse wird nach der Feststellung aller Assets ermittelt, wie kritisch ein Prozess sowie die jeweiligen Assets dafür sind, und welche Risiken bestehen. Eine Umsetzung von Sicherheitsmaßnahmen macht erst Sinn, wenn die Risiken definiert sind, da eine zuvor bereits umgesetzte Maßnahme vielleicht nicht ausreichend ist, weil man den Schutzbedarf oder das Risiko zuvor un-



Maßnahmenplanung in KANiO-ISMS [6]

terschätzt hat. Im Rahmen der Umsetzungsmaßnahmen müssen alle Prozesse geregelt und dokumentiert werden, um sicherzustellen, dass Verantwortlichkeiten zu jeder Zeit geregelt, kommuniziert und dokumentiert sind. Es sollen möglichst keine Unklarheiten offen bleiben und Handlungssicherheit für alle Beteiligten bestehen. Neben der Erstellung von Leit- und Richtlinien müssen Verfahrensanweisungen und Prozessbeschreibungen den Mitarbeitern bekannt gegeben werden. Da der Mensch gerade für die Informationssicherheit einen enorm hohen Kritikalitätsfaktor darstellt, sind alle Mitarbeiter bei der Einführung und Umsetzung eines ISMS „mitzunehmen" und regelmäßig entsprechende Sensibilisierungs- und Schulungsmaßnahmen 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.

Der „Standard"-Weg – von B3S zur ISO 27001 und wieder zurück

Die Einführung eines ISMS nach ISO 27001 wird im Branchenstandard zwar empfohlen, ist jedoch nicht verpflichtend. Der IT-Sicherheitsleitfaden, der neben dem Merkblatt ein Hauptbestandteil des B3S ist, basiert vollständig auf dem BSI-Grundschutz. Dabei wurde jedoch eine branchenspezifische Vorauswahl von relevanten Gefährdungen sowie der entsprechenden Maßnahmen aus den Bereichen Trinkwasserversorgung und Abwasserentsorgung vorgenommen und somit die Anwendung des BSI-Grundschutz wesentlich vereinfacht. Diese Vereinfachung stellt jedoch keine Einschränkung dar, da der Leitfaden als „Best Practices" für den Sektor Wasser/Abwasser angesehen werden soll und Betreiber jederzeit die Möglichkeit haben, für den spezifischen Anwendungsbereich zum Beispiel ergänzende Maßnahmen aus dem BSI-Grundschutz anzuwenden oder besser geeignete Maßnahmen umzusetzen.

Die in der ISO-Norm 27001 beschrieben allgemeinen Anforderungen werden gemäß BSI-Grundschutz im Rahmen der Gefährdungs- und der Maßnahmenkataloge ganz konkret ausgeprägt und stellen somit eine Implementierung der Norm dar. Hierbei setzt der IT-Sicherheitsleitfaden vollständig auf den BSI-Grundschutz und setzt ausnahmslos auf die Zuordnungsketten (Bausteine à Gefährdungen à Maßnahmen) die in den Kreuzreferenztabellen [4] des BSI-Grundschutzes enthalten sind. Neben den Kreuzreferenztabellen wird ebenso die „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz" [5] und die Verlinkung zu aktuellen Fassungen der Grundschutzkataloge auf den Internetseiten des BSI unterstützt. Somit wird eine bidirektionale Verbindung zu den ISO-Normen ermöglicht und sichergestellt, dass der IT-Sicherheitsleitfaden konsistent und aktuell mit dem BSI-Grundschutz sowie zur ISO-Norm bleibt.

ISMS-Tool als Bindeglied zwischen verschiedenen Sicherheitsstandards

Ein IT-gestütztes ISMS (Informations-Sicherheits-Management-System) stellt für die einzelnen Schritte auf dem Weg zu einer rechtskonformen IT-Sicherheitsstruktur einen wichtigen Baustein dar. Von einem der Projektpartner wird ein entsprechendes Tool (KANiO-ISMS) in die KOMMUNAL 4.0 Plattform integriert, welches auch als separate Applikation bzw. als Bestandteil des Betriebsführungssystems KANiO separat verwendet werden kann. 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. Es erfüllt auch gleichzeitig die Dokumentationsanforderungen der ISO 27001 als wesentlicher Baustein einer Zertifizierung sowie den B3S. Die wesentlichen Funktionsbausteine sind:

- Dokumentenverwaltung zur Dokumentation der IT-Sicherheit
- Stammdatenbereich zur strukturierten Dokumentation aller IT-Sicherheits-relevanten 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

Literatur/Quellennachweis

[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] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Check/kreuzreferenz_tabellen_zip.zip

[5] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf

[6] Bildquelle: HST Systemtechnik GmbH & Co. KG

Autoren:

Heiko Fauth
Faktor Sicherheit
Häselhöfe 7
D-72348 Rosenfeld
www.faktor-sicherheit.de

Nico Suchold
ifak - Institut f. Automation und Kommunikation e. V. Magdeburg
Werner-Heisenberg-Straße 1
D-39106 Magdeburg
www.ifak.eu

Günter Müller-Czygan
HST Systemtechnik GmbH & Co. KG
Heinrichsthaler Straße 8
D-59872 Meschede
www.hst.de