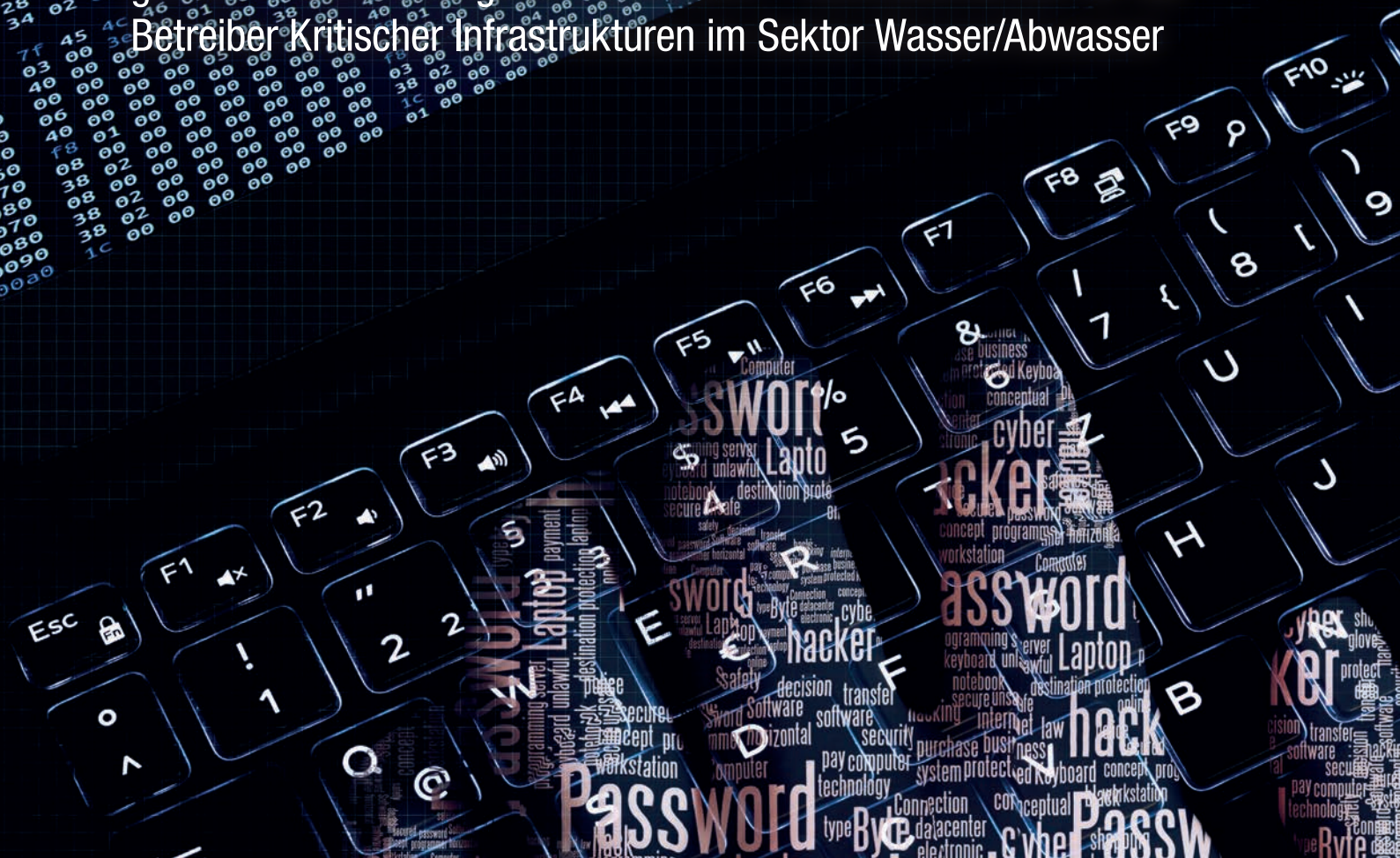


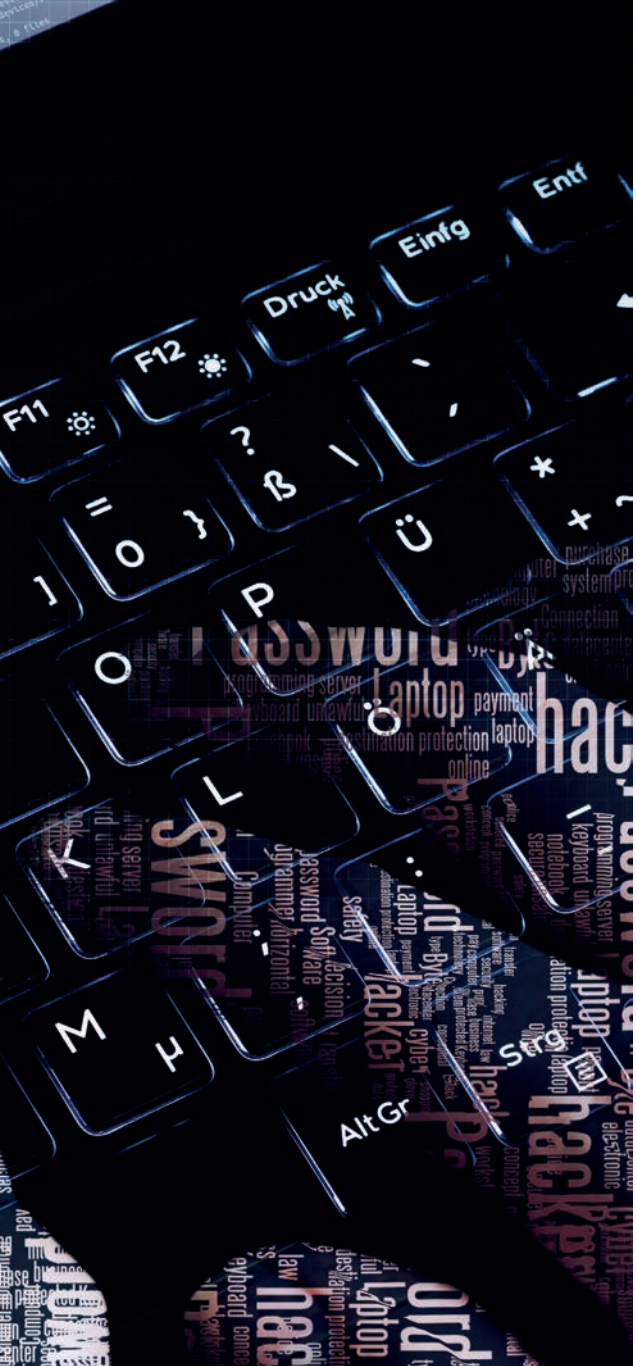
Branchenspezifischer Sicherheitsstandard Wasser/Abwasser

gemäß IT-Sicherheitsgesetz anerkannt – Rechtssicherheit für die Betreiber Kritischer Infrastrukturen im Sektor Wasser/Abwasser



Das durch das IT-Sicherheitsgesetz erweiterte BSI-Gesetz (BSIG) definiert die Anforderungen an die IT-Sicherheit für die Betreiber Kritischer Infrastrukturen, zu denen auch der Sektor Wasser mit den Branchen Trinkwasserver- und Abwasserentsorgung zählt. Das Gesetz bietet den betroffenen Branchen die Möglichkeit, einen „Branchenspezifischen Sicherheitsstandard“ (kurz: B3S) zu entwickeln, durch den der laut Gesetz geforderte „Stand der Technik“ in Bezug auf die Kritischen Infrastrukturen der Branche definiert wird. Mit den Merkblättern DVGW W 1060 und DWA M 1060 „IT-Sicherheit – Branchenstandard Wasser/Abwasser“ in Verbindung mit dem dazugehörigen IT-Sicherheitsleitfaden ist es den Branchen Wasser/Abwasser gelungen, den ersten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannten B3S zu erarbeiten. Bei der Erstellung spielten vor allem das Wissen der Experten beider Branchen, die Nutzung bestehender Standards, Flexibilität in Bezug auf individuelle Gegebenheiten, eine strukturierte Umsetzung und eine regelwerkskonforme Ausgestaltung eine entscheidende Rolle.

von: Uwe Marquardt (GELSENWASSER AG) & Dr. Ludger Terhart (Emschergenossenschaft/Lippeverband)



- Regelwerkskonformität (DVGW und DWA)
- Erfüllung der Anforderungen der BSI-Orientierungshilfe für einen B3S
- Flexible Anpassbarkeit an technische Entwicklungen
- Nutzung bestehender Standards
- Nachvollziehbarkeit (Verständlichkeit) und Anwendbarkeit durch alle Betreiber in der Branche, insbesondere auch kleinere Unternehmen
- Konformität zu bestehenden Normen (insbesondere DIN ISO/IEC 27001 ff.) für den Einsatz etwa in Verbundunternehmen
- Strikte Beschränkung auf die Gegebenheiten der Branche und deren Infrastrukturen
- Berücksichtigung individueller Gegebenheiten in Bezug auf spezifische Anlagenkomponenten und eingesetzte IT-Systeme
- Angemessenheit der zur Umsetzung erforderlichen Prozesse
- Konkrete Benennung der durchzuführenden Maßnahmen

Die auf Basis dieser Anforderungen von DVGW und DWA entwickelte und nachfolgend beschriebene Vorgehensweise und Struktur des B3S WA kann als Blaupause für andere Branchenspezifische Sicherheitsstandards verstanden werden, da sie grundsätzlich keine branchenspezifischen Vorannahmen trifft.

Wie bereits in [1] dargestellt, basiert der B3S WA auf zwei Säulen: der regelwerkskonformen Verankerung in Form eines DVGW- bzw. DWA-Merkblattes und dem zugehörigen, flexibel anpassbaren IT-Sicherheitsleitfaden. Ergänzt werden diese beiden Säulen durch die Regularien zur Nachweisführung der Einhaltung des Standes der Technik. Das Merkblatt selbst enthält die grundlegenden Vorgaben und ist bewusst auf eine längerfristige Gültigkeit ausgerichtet. Verfahren und Strukturen, die sich kurzfristig dem Stand der Technik anpassen müssen, wie z. B. die möglichen Gefährdungen und die zu ihrer Abwehr oder Milderung notwendigen Maßnahmen, sind im Rahmen des IT-Sicherheitsleitfadens abgebildet.

Das Merkblatt fügt sich ein in das technische Risikomanagement gemäß DIN EN 15975-2 „Sicherheit in der Trinkwasserversorgung – Leitlinien für das Risiko- und Krisenmanagement – Teil 2: Risikomanagement“ (ehemals DVGW-Hinweis W 1001). Dementsprechend werden neben den Grundlagen und Zielen des Schutzes der Informationstechnik, der Beschreibung der

Im Gegensatz zu vielen anderen Branchen verfügt der Sektor Wasser mit den Bereichen Trinkwasserversorgung (DVGW) und Abwasserentsorgung (DWA) über zwei regelsetzende Verbände, die auf eine lange Tradition in Bezug auf die Erarbeitung von branchenspezifischen Regelwerken zurückschauen können. Vor diesem Hintergrund lag es nahe, eben diese Verbände mit der Erstellung eines Branchenspezifischen Sicherheitsstandards nach BSI-Gesetz für die Bereiche Wasser/Abwasser zu betrauen.

DVGW und DWA haben zu diesem Zweck gemeinsame Arbeitsgruppen gebildet, die sich mit den verschiedenen Aspekten eines solchen B3S für Wasser und Abwasser (kurz: B3S WA) auseinandergesetzt haben. Wesentliche Anforderungen, die bei dessen Erstellung zu berücksichtigen waren, sind:

Struktur des B3S WA und organisatorischer Anforderungen inklusive Informationssicherheits- und/oder betriebliches Kontinuitätsmanagement die klassischen Elemente zur Risikoabschätzung und -verminderung beschrieben und entsprechende Anforderungen formuliert. Nicht enthalten sind Anforderungen zum Objektschutz; diesbezüglich wird auf das DVGW-Merkblatt W 1050 und die DVGW-Information Wasser Nr. 80 verwiesen. Sowohl DIN EN 15975-2 als auch das DVGW-Merkblatt W 1050 inklusive der DVGW-Information Wasser Nr. 80 sind gleichermaßen auch auf die Anlagen der Abwasserentsorgung anwendbar.

Trinkwasserver- und Abwasserentsorgungsunternehmen sind grundsätzlich Betreiber Kritischer Infrastrukturen, auch wenn der überwiegende Teil der Unternehmen derzeit nicht unter die BSI-Kritisverordnung (BSI-KritisV) fällt. Nicht bei allen diesen Unternehmen kann davon ausgegangen werden, dass entsprechende IT-Organisationen vorhanden sind, welche über umfassende Fachkenntnis verfügt. Insofern abstrahiert der IT-Sicherheitsleitfaden von IT-technischen Gegebenheiten und beschreibt in Anlehnung an die von der American Water Works Association (AWWA) beschriebene Vorgehensweise [2] generalisierte Anwendungsfälle, die allgemeinverständlich beschrieben werden. Diese Anwendungsfälle beschreiben grundsätzliche Infrastrukturkonfigurationen der IT-Systeme zum Betrieb der Anlagen, organisatorische Gegebenheiten sowie grundlegende Prozesse im betrieblichen Alltag, wie etwa die Wartung und Nutzung der IT-Systeme.

Mit den IT-Grundschutz-Katalogen des BSI (im Folgenden kurz „BSI-Grundschutz“ genannt) steht ein anerkannter und bewährter Standard für die Sicherheit von IT-Infrastrukturen zur Verfügung. Der BSI-Grundschutz stellt eine praktische Ausgestaltung insbesondere der Norm DIN ISO/IEC 27001 dar. Im Gegensatz zur Norm werden jedoch nicht nur die allgemeinen Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) beschrieben,

sondern ganz konkret ein Maßnahmenkatalog zur Verfügung gestellt, aus dem ersichtlich ist, bei welcher Gefährdung welche dieser Maßnahmen sinnvoll umgesetzt werden sollten.

Der IT-Sicherheitsleitfaden basiert vollständig auf dem BSI-Grundschutz unter Hinzuziehung des ICS-Security-Kompodiums des BSI [3]. Es werden die für die aufgeführten Anwendungsfälle relevanten Gefährdungen und die entsprechenden Maßnahmen aus dem BSI-Grundschutz referenziert. Die Liste der Gefährdungen wie auch die Auswahl der entsprechenden Maßnahmen wurden durch Fachleute aus den Bereichen Trinkwasserver- und Abwasserentsorgung in Abstimmung mit dem BSI gemeinsam erarbeitet. Diese Auswahl stellt somit den branchenspezifischen Ausschnitt aus dem BSI-Grundschutz dar.

Der IT-Sicherheitsleitfaden gibt die Gefährdungen und Maßnahmen nicht abschließend wieder, sondern stellt die „Best Practices“ für den Sektor Wasser dar. Aufgrund der Tatsache, dass er sich ausschließlich des BSI-Grundschutzes bedient, steht den Betreibern jederzeit die Möglichkeit offen, in der konkret gegebenen Situation – ergänzend zum IT-Sicherheitsleitfaden – weitere Maßnahmen aus dem BSI-Grundschutz aufzunehmen oder Maßnahmen durch andere, besser geeignete zu ersetzen. Der IT-Sicherheitsleitfaden ist so konzipiert, dass er auf allen Ebenen (Anwendungsfall, Gefährdung, Maßnahme) Ergänzungen oder Modifikationen zulässt. Dabei bildet ohne Ausnahme der BSI-Grundschutz die Basis.

Der IT-Sicherheitsleitfaden wurde bereits so angelegt, dass er mit geringem Aufwand an den modernisierten BSI-Grundschutz angepasst werden kann, der voraussichtlich Anfang 2018 veröffentlicht werden wird.

Da ausschließlich auf den BSI-Grundschutz verwiesen wird, ist der IT-Sicherheitsleitfaden auch jederzeit an die neuen Erkenntnisse in Fragen der IT-Sicherheit anzupassen. Hier setzt der

B3S WA ausdrücklich auf die fachliche Kompetenz der bundesweit führenden Organisation in Fragen der IT-Sicherheit und ist damit stets aktuell.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Ende Juni 2017 die Eignung des B3S WA offiziell festgestellt. Die inhaltsgleichen DVGW- bzw. DWA-Merkblätter sowie der IT-Sicherheitsleitfaden als webbasiertes Online-Anwendungstool werden voraussichtlich Ende August veröffentlicht. Derzeit in Arbeit sind noch die Regularien zur branchenspezifischen Nachweisführung, mit dem Betreiber Kritischer Infrastrukturen gemäß der BSI-KritisV der Branchen Wasser und Abwasser alle zwei Jahre die Einhaltung des Standes der Technik gegenüber dem BSI nachweisen müssen. ■

Literatur

- [1] Terhart, L., Wagner, K.: IT-Sicherheit in der Wasserversorgung – Branchenstandard IT-Sicherheit Wasser/Abwasser, in: DVGW energie | wasser-praxis, Ausgabe 12/2016, S. 134–136.
- [2] American Water Works Association (Hrsg.): Process Control System Security Guidance for the Water Sector, Washington DC (2014).
- [3] Bundesamt für Sicherheit in der Informationstechnik: ICS-Security-Kompodium, online unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompodium_.pdf.pdf?__blob=publicationFile&v=2, abgerufen am 12. Juli 2017.

Die Autoren

Dipl.-Ing. Uwe Marquardt ist Sachgebietsleiter Technische Koordination bei der GELSENWASSER AG und Obmann des DVGW W-GTK-2-8 IT-Sicherheit.

Dr. Ludger Terhart ist Abteilungsleiter Informationstechnologien bei Emschergenossenschaft/Lippeverband und Sprecher der DWA-Arbeitsgruppe WI 5.4 Cyber-Sicherheit.

Kontakt:

Kirsten Wagner
DVGW Deutscher Verein des Gas- und Wasserfaches e. V.
Technisch-wissenschaftlicher Verein
Josef-Wirmer-Str. 1–3
53123 Bonn
Tel.: 0228 9188-868
E-Mail: wagner@dvwg.de
Internet: www.dvgw.de