Der Branchenspezifische Sicherheitsstandard Wasser/ Abwasser (B3S WA) – Teil 2:

Anwendungshilfe zur Implementierung in einem kleinen Unternehmen

Laut dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) muss der „Branchenspezifische Sicherheitsstandard Wasser/Abwasser“ (kurz: B3S WA) alle zwei Jahre an den jeweils aktuellen Stand der Technik angepasst und seine Eignung anschließend durch das BSI (im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)) festgestellt werden. Nachdem der erste Teil des Fachbeitrags die Änderungen beschrieben hat, die sich bei der Überarbeitung 2021 ergeben haben, erläutert der vorliegende zweite Teil anhand eines praktischen Beispiels die Vorgehensweise bei einem kleinen kommunalen Wasserversorger.

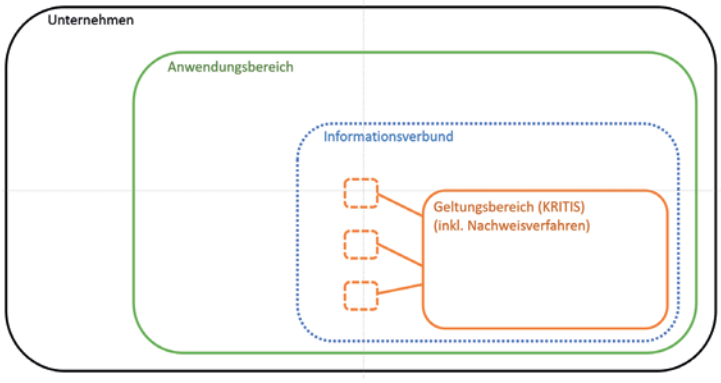
von: Daniel Fricke & Rainer Stecken (beide: DVGW Service & Consult GmbH)

Die Anwendung des IT-Sicherheitsleitfadens zum DVGW-Merkblatt W 1060 läuft seit der Veröffentlichung der ersten Version immer nach der gleichen Vorgehensweise ab. Das bleibt auch bei der Version 2021 erhalten.

Konkret sieht die Vorgehensweise wie folgt aus: Nachdem die Anlagen in der Wasserversorgung basierend auf dem Asset-Inventar bestimmt worden sind, werden die Anwendungsfälle für die Anlagen in der Version 2021 des B3S WA im IT-Sicherheitsleitfaden aus einer Liste von insgesamt 27 Anwendungsfällen ausgewählt. Ein Anwendungsfall ist z. B. „anlagenweites Netzwerkmanagement“ (NM2) oder „automatisierter Datenaustausch“ (PA5). Im Anschluss besteht dann die Möglichkeit, die Anforderungen aus dem IT-Grundschutz-Kompendium zum jeweiligen Anwendungsfall abzulesen. Im Unterschied zu der früheren Variante des BSI-Grundschutzes und den IT-Grundschutz-Katalogen, in denen Umsetzungshinweise zu Schutzmaßnahmen enthalten waren, werden im neuen IT-Grundschutz-Kompendium stattdessen Anforderungen und – soweit vorhanden – Umsetzungshinweise beschrieben. In den Anforderungen werden die Ziele angegeben und in den Umsetzungshinweisen wird aufgeführt, mit welchen Schutzmaßnahmen diese zu erreichen sind. Sobald die Anforderungen umgesetzt und dokumentiert sind, findet eine Restrisikobewertung statt. Für den Fall, dass nicht alle Risiken ausreichend reduziert sind, werden weitere Schutzmaßnahmen zur Risikoreduktion ange-

Definition des Geltungsbereiches:

- Kritische Infrastruktur (KDL)
- Informationsverbund
- Anwendungsbereich
- Unternehmen



Quelle: DVGW Service & Consult GmbH

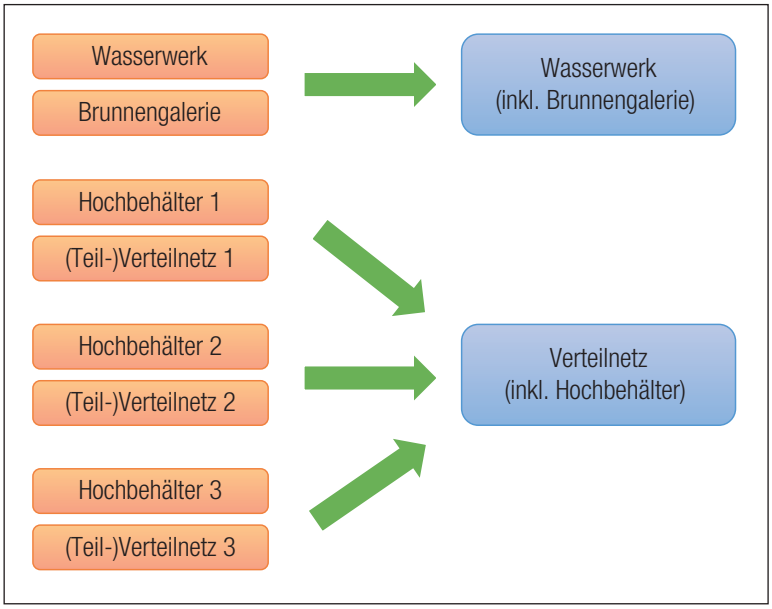
Abb. 1: Geltungs- und Anwendungsbereich des B3S WA

wendet und dokumentiert. Bei sogenannten Sub-KRITIS-Unternehmen, also Unternehmen, die unterhalb der Schwellwerte aus der KRITIS-Verordnung liegen und damit nicht gesetzlich reguliert sind, beginnt dann das „Leben“ der neu gewonnenen Informationssicherheit. Nach einer gewissen Zeit empfiehlt es sich, die jährliche Evaluierung durchzuführen.

Im IT-Grundschutz-Kompendium gibt es, je nach Sicherheitsbedarf, insgesamt drei Anforderungstypen. Dazu sei das IT-Grundschutz-Kompendium 2021 zitiert (S. 17): „Basis-Anforderungen müssen vorrangig umgesetzt werden, da sie mit geringem Aufwand den größtmöglichen Nutzen erzielen. Gemeinsam mit den Basis-Anforderungen erfüllen die Standard-Anforderungen den Stand der Technik und adressieren den normalen Schutzbedarf. Ergänzend dazu bieten die Bausteine des IT-Grundschutz-Kompendiums Vorschläge für Anforderungen bei erhöhtem Schutzbedarf.“ Genau daran orientiert sich die Version 2021 des B3S WA. Für kleine Unternehmen (Sub-KRITIS) sind die Basis-Anforderungen ein geeigneter Ansatz, um ein gutes Schutzniveau zu erreichen. KRITIS-Betreiber, die die Schwellenwerte der BSI-Kritisverordnung (BSI-KritisV) erreichen oder überschreiten, müssen zusätzlich die Standard-Anforderungen umsetzen, um die gesetzlichen Vorgaben zu erfüllen; in beiden Fällen jeweils für die identifizierten Anwendungsfälle. Das entsprechende B3S-Level unterscheidet daher zwischen den Kategorien A(lle) und zusätzlich K(ritische) Infrastruktur. Auf diese Weise verringert sich für kleine Unternehmen der Umsetzungsaufwand und der B3S WA wird zur einfachen Anwendung.

Im folgenden anonymisierten Beispiel, das der Verdeutlichung dieser Vorgehensweise dienen soll, wird von einem kleinen kommunalen Wasserversorger (KWV) ausgegangen. Dieser hat ein Wasserwerk mit ca. 3 Mio. m³ Wasserdurchsatz, sodass nur das B3S-Level „A“ zum Einsatz kommt. Die Brunnengalerie liegt auf dem Gelände des Wasserwerks und aufgrund der geografischen Lage gibt es mehrere Hochbehälter, die über eine Füllstandsmessung aufgefüllt werden. Die Teilbereiche des Verteilnetzes werden dann aus den Hochbehältern im freien Fall gespeist.

Nachdem die Geschäftsführung des KWV sich für die Umsetzung des B3S WA entschieden hat, wird eine Projektgruppe zur Umsetzung eingesetzt. Diese bildet sich im vorliegenden Fall aus der Wassermeisterin, dem Qualitätsmanagementbeauftragten und einem Vertreter der Geschäftsführung; zudem war ein DVGW-nahes Beratungsunternehmen beteiligt. Im Rahmen der Projektgruppe einigt man sich darauf, den Anwendungsbereich weitestgehend auf das ganze Unternehmen auszurollen (**Abb. 1**), damit die Regelungen unternehmensweise Gültigkeit haben. Der initiale Aufwand steigt dadurch damit unwesentlich, im laufenden Betrieb können sich im Gegenzug aber alle Mitarbeitenden über gleichlautende Regeln freuen.



Quelle: DVGW Service & Consult GmbH

Abb. 2: *Festlegung der Anlagen*

In den nächsten Terminen der Projektgruppe werden dann die Anlagen definiert. Nach einiger Diskussion steht fest, dass die verschiedenen Teilnetze zwar durchaus unterschiedlich sind, aber in der grundsätzlichen Betrachtung nicht unterschieden werden müssen. Daher werden die Anlagen wie in **Abbildung 2** gezeigt zusammengefasst.

Bei der Auswahl der Anwendungsfälle stellt sich schnell heraus, dass im Verteilnetz (aufgrund des freien Gefälles) kein steuernder Eingriff vorgenommen wird. Deshalb sind lediglich die Anforderungen der obligatorischen Anwendungsfälle OM1 (organisatorische Maßnahmen) und INF1 (Infrastruktur) zu erfüllen. Dabei handelt es sich auch um die einzigen Anwendungsfälle, die unabhängig von den Anlagenfestlegungen grundsätzlich immer auszuwählen sind.

INFORMATIONEN

Teil 1 des Fachbeitrags ist in Ausgabe 12/2021 dieser Fachzeitschrift erschienen.

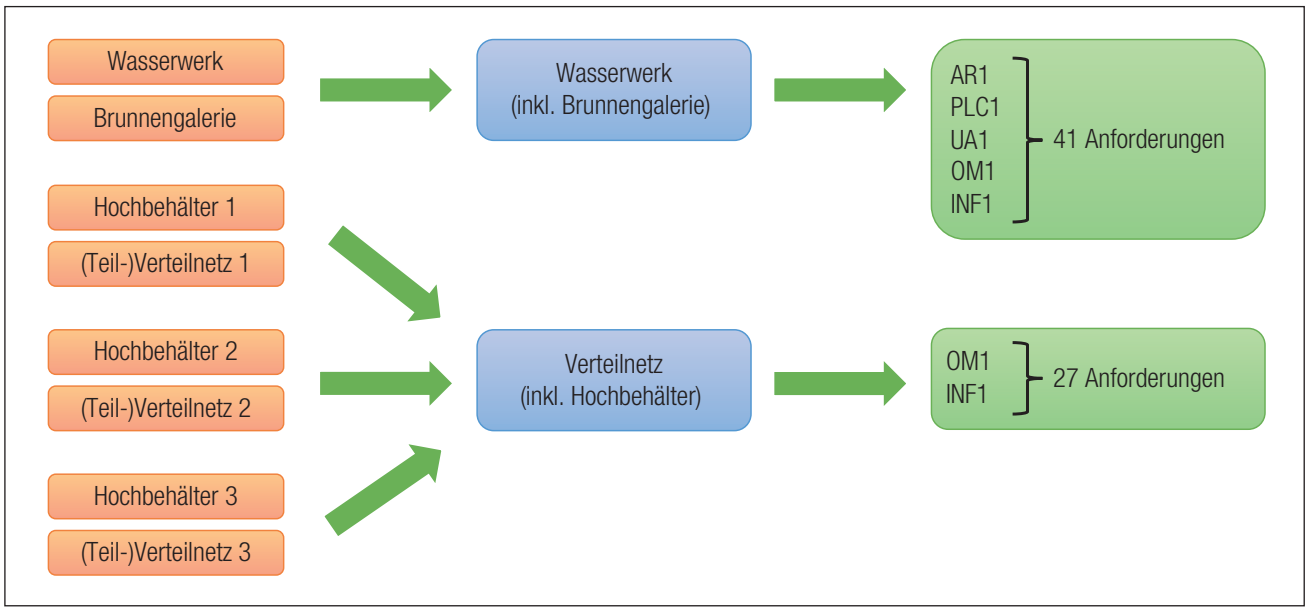


Abb. 3: *Übersicht über die Anzahl der Anforderungen*

Anders stellt sich die Situation im Wasserwerk dar: Neben OM1 und INF1 kommen hier die Anwendungsfälle AR1 (dediziertes Netzwerk), UA1 (Zugriff steuernd im gesicherten Kontrollraum) und PLC1 (lokale SPS-Programmierung) vor. Insgesamt ergeben sich damit 68 Anforderungen **(Abb. 3)**, wobei 27 dieser Anforderungen in beiden Anlagen umgesetzt werden müssen.

Da sich die OM1- und INF1-Anforderungen für das Wasserwerk und das Verteilnetz nicht unterscheiden, werden die entsprechenden Maßnahmen einheitlich für den KWV umgesetzt und dokumentiert. Die Art der Umsetzung der Anforderungen der Anwendungsfälle AR1, UA1 und PLC1 wird in einer Dienstanweisung zusammengefasst.

Als Kontrolldokument wird der Export aus dem IT-Sicherheitsleitfaden genutzt, der mit einigen Erweiterungen zum Grad der Erledigung, der Verantwortlichkeit und dem zeitlichen Horizont auch als Grundlage für die Bemessung des Projektfortschritts genutzt wird. Im Fall einer Auditierung bzw. dem Durchlauf eines Nachweisverfahrens kann ein solches Dokument auch gut genutzt werden, um die entsprechenden Arbeiten zentral zu dokumentieren. Im QM-System des KWV wird die Leitlinie zur Informationssicherheit als gelenktes Dokument hinterlegt und in Kraft gesetzt.

Der KWV hat die Umsetzung des B3S WA in knapp 6 Monaten geschafft. Dabei sind allerdings auch bei einigen Arbeitssitzungen „Blut, Schweiß und Tränen“ geflossen und es war eine klare Vorgabe von Seiten der Geschäftsführung erforderlich.

Informationssicherheit ist für alle Unternehmensgrößen wichtig und wird durch die Flexibilität der Version 2021 des B3S WA für die jeweils vorhandenen Anlagen und jede Unternehmensgröße optimal sichergestellt. Zudem wird durch seine Anwendung die Gefahr eines Organisationsverschuldens im Umfeld der Informationssicherheit sicher vermieden. Der Einsatz des IT-Sicherheitsleitfadens ist ein pragmatischer Ansatz, der kleine Wasserver- und Abwasserentsorgungsbetriebe optimal bei der Einführung von Informationssicherheit bzw. der Etablierung eines Schutzes unterstützt. ■

Die Autoren

Daniel Fricke ist Leiter der IT bei der DVGW Service & Consult GmbH in Bonn.

Rainer Stecken ist Berater für Informationssicherheit bei der DVGW Service & Consult GmbH in Bonn.

Kontakt:
Daniel Fricke
DVGW Service & Consult GmbH
Josef-Wirmer-Str. 1–3
53123 Bonn
Tel.: 0228 9188-743
E-Mail: daniel.fricke@dvgw-sc.de
Internet: www.dvgw-sc.de

YOUR WAY TO START NOW

START NOW
DAS YOUNG PROFESSIONAL PROGRAMM

JETZT ANMELDEN
ypp@dvgw.de

JETZT ALS MENTEE EINSTEIGEN UND DURCHSTARTEN

Lass Dich als Mentee im Young Professional Programm bei Deinem beruflichen Einstieg in die Energie- und Wasserbranche von Branchenprofis coachen und unterstützen! Melde Dich jetzt an und sei beim Auftakt ins Mentoring-Jahr 2022 dabei.

EIN PROGRAMM DES DVGW

www.dvgw.de/ypp