# Branchenspezifischer Sicherheitsstandard Wasser/Abwasser als technische Grundlage für die Informationssicherheit

*Jan Feldhaus (Bonn)*

*Die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall (DWA) und der Deutsche Verein des Gas- und Wasserfaches (DVGW) haben zur Sicherung der Versorgungssicherheit in der Abwasserbeseitigung und Wasserversorgung im vergangenen Jahr gemeinsam das DWA-Merkblatt M 1060 bzw. DVGW-Merkblatt W 1060 und die Web-Applikation „IT-Sicherheitsleitfaden" herausgebracht. Sowohl in der Wasserversorgung als auch in der Abwasserentsorgung hat sich der Sicherheitsstandard als technische Grundlage für die Branchen bewährt.*

## Abwasserbranche – kritische Infrastruktur, Informationssicherheit?

Anlagen zur Abwasserbeseitigung werden von dem Gesetzgeber als kritische Infrastruktur angesehen. Ein Ausfall der Abwasserbeseitigung kann schwerwiegende Folgen für die Bevölkerung haben. Ohne eine funktionierende Abwasserbeseitigung können sich Krankheiten und Seuchen rasch verbreiten. Somit stellen Anlagen zur Abwasserbeseitigung in ihrer Funktion kritische Infrastrukturen dar, die eine kritische Dienstleistung erbringen, welche für unsere moderne Gesellschaft unverzichtbar ist.

Der Schutz der Anlagen ist zu gewährleisten. Wichtig ist, dass keine Informationen, mit denen diese Funktionsfähigkeit der Anlagen gestört werden kann, in unbefugte Hände gelangen. Der Schutz der Bevölkerung beginnt bereits mit der Informationssicherheit innerhalb einer Organisation, auch wenn es sich „nur" um die Abwasserbeseitigung handelt.

Die Betreiber müssen daher Maßnahmen zur Informationssicherheit ergreifen. Gemäß den gesetzlichen Vorgaben des BSI-Gesetzes (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) hatte ein Teil der in Deutschland ansässigen Unternehmen aus der Abwasserbranche bis zum 03.05.2018 einen Nachweis zu erbringen, wie die Informationssicherheit zum Schutz der betriebenen kritischen Infrastruktur sichergestellt wird. Bei den Betroffenen handelte es sich um die Betreiber großer Abwasserbeseitigungsanlagen. Den Betreibern kleinerer Anlagen wird geraten, sich ebenfalls ihrer Verpflichtung gegenüber der Bevölkerung bewusst zu sein und ebenfalls Maßnahmen einzuleiten.

## Ist der branchenspezifische Sicherheitsstandard Wasser/Abwasser die Lösung?

Mit dem von DWA und DVGW entwickelten branchenspezifischen Sicherheitsstandard Wasser/Abwasser (B3S WA) haben Unternehmen die Möglichkeit, ein ihren Ansprüchen entsprechendes Informationssicherheitsmanagementsystem (ISMS) aufzubauen, welches die gesetzlichen Anforderungen erfüllt und dem Stand der Technik entspricht. Die Stärke des B3S WA liegt darin, dass er nicht das Unternehme als Ganzes betrachtet, sondern seine Anwendung auf einzelne Anlagen erfolgen kann.

In den gemäß § 8a BSIG durchgeführten Nachweisverfahren konnte festgestellt werden, dass der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) die Prüfgrundlage darstellt, welche am besten auf die Belange der Abwasserbranche abzielt. Andere Prüfgrundlagen wie z. B. die ISO 27001 oder der IT-Grundschutzkatalog, die beide um branchenspezifische Prüfungen ergänzt werden müssten, haben im Rahmen von Prüfungsverfahren bzw. Nachweisverfahren mehrfach zu Klärungsbedarf zwischen dem Begutachter und dem Unternehmen geführt.

## Informationssicherheit unabhängig von der Unternehmensgröße

Es müssen sich allerdings nicht nur die Betreiber großer kritischer Infrastrukturen auf geänderte Bedingungen in einer modernen digitalisierten Welt einstellen. Auch Betreiber kleinerer oder mittlerer kritischer Infrastrukturen sind ihren Kunden gegenüber verantwortlich, den Schutz der Versorgungs- bzw. Entsorgungssicherheit zu gewährleisten. Ein weiterer Vorteil des B3S ist daher, dass dieser so aufgebaut ist, dass er unabhängig von der Ausbaugröße einer kritischen Infrastruktur angewendet werden kann. Auch die Betreiber kleinerer oder mittlerer Abwasserbeseitigungsanalagen können den B3S WA anwenden.

Das gemeinsam von DWA und DVGW e. V. entwickelte DWA Merkblatt M 1060 bzw. DVGW-Merkblatt W 1060 und die Web-Applikation „IT-Sicherheitsleitfaden", der sogenannte branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA), bildet dabei den „Stand der Technik" ab und stellt eine Anweisung dar, wie dieser in den Unternehmen umgesetzt werden kann.

## Das ISMS als grundlegendes Element

Ein grundlegendes Element, welches von den Anwendern des B3S WA verlangt wird, ist ein Informationssicherheitsmanagementsystem (ISMS). Dabei ist zu beachten, dass es keine Vorgaben zum ISMS innerhalb des B3S WA gibt. Im Merkblatt wird unter Punkt 6 das Thema Managementsysteme aufgegriffen und darauf hingewiesen, welche Mindestanforderungen gefordert sind. Unter Punkt 6.2 wird beschrieben; „Die Einführung und gegebenenfalls Zertifizierung eines ISMS ist für die Sektoren Wasser / Abwasser nicht vorgeschrieben. Allerdings ist für die Betreiber kritischer Infrastrukturen die Aufstellung und Einführung von Verfahren und Regeln, um die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern, zwingend erforderlich."

Die einzige Möglichkeit den Anforderungen gerecht zu werden und nachhaltig die Sicherheit der kritischen Infrastruktur zu gewährleisten, stellt somit ein grundlegendes ISMS dar. Ein solches ISMS muss mindestens beinhalten:

- Dokumentation der Assets
- Regeln und Verfahrensanweisungen (z. B. zum Umgang mit Störfällen, für kritische Verfahren)
- Risikoanalyse
- Maßnahmenpläne (z. B. inkl. Verantwortlichkeiten, Termine, Beschreibung der Maßnahme, Stand der Umsetzung)
- Lenkung durch die oberste Leitung (z. B. Bewertung der Risiken sowie der Umsetzung von Maßnahmen, Managementreview)

Ein ISMS z. B. nach DIN ISO/IEC 27001 oder IT-Grundschutzkatalog muss nicht eingeführt werden. Aber es bedarf mindestens eines einfachen (Informationssicherheits-) Managementsystems.

## Die Risikoanalyse als Schlüssel

Dass Unternehmen mit einem gewissen Risiko leben müssen, ist natürlich nicht von der Hand zu weisen. Aber dieses sollte so gering wie möglich gehalten werden. Zum Schutz der kritischen Infrastruktur und vor allem zur Minimierung der Ausfallwahrscheinlichkeit ist daher eine umfassende Risikoanalyse notwendig.

Hierin liegt eine der Stärken des B3S WA. Die Basis für eine tiefgreifende Risikoanalyse bildet dabei der IT-Leitfaden zum B3S WA. Mit Hilfe der im IT-Leitfaden hinterlegten 22 Anwendungsfälle können für jede Anlage Maßnahmen ermittelt werden, die für einen umfangreichen Schutz der kritischen Infrastruktur notwendig sind. Aus der durchgeführten Risikoanalyse ergeben sich Eintrittswahrscheinlichkeiten für jedes Risiko, mittels derer festgelegt wird, welche Maßnahmen einer dringenden Umsetzung bedürfen und welche Maßnahmen eventuell auch nicht umgesetzt werden müssen. Die bedeutendsten Faktoren bei dieser Risikobewertung sind die Ausfallwahrscheinlichkeit der Anlage sowie die Auswirkungen des Ausfalls auf den dauerhaften Anlagenbetrieb. Das heißt zum Beispiel, wie häufig kommt es vor, dass es durch ein bestimmtes Risiko zu einem Ausfall kommt, oder wie schnell der Ausfall wieder behoben werden kann. Eine solche Risikoanalyse muss dokumentiert werden und einer regelmäßigen Überwachung unterliegen. Nur somit ist eine fortlaufende Verbesserung gewährleistet.

Die beschriebene Risikoanalyse stellt dabei nur eine Mindestanforderung dar. Eine tiefergehende Analyse ist immer möglich. Dem Unternehmen steht es frei zu entscheiden, nach welcher Methode eine Risikoanalyse durchgeführt wird.

## Bewusstsein und Nachhaltigkeit schaffen

Der Erfolg eines jeden Managementsystems wächst mit der Akzeptanz durch die Mitarbeiter. Wichtig ist, diese von vornherein in die Prozesse mit einzubinden. Dabei sollten die Mitarbeiter auch aktiv beteiligt werden, in dem sie z. B. die Verantwortung für die Umsetzung von Maßnahmen übernehmen oder bei der Bewertung von umgesetzten Maßnahmen mit eingebunden werden.

Ziel ist es einen kontinuierlichen Verbesserungsprozess (KVP) aufzubauen und das System ständig weiter zu entwickeln um auch zukünftig den Anforderungen an den Stand der Technik zu genügen. Eine zentrale Rolle spielt ein Maßnahmenplan, mit dem die wesentlichen Informationen dokumentiert werden die für einen erfolgreichen KVP notwendig sind.

Im Maßnahmenplan muss neben der definierten Maßnahme mindestens festgehalten werden:

- Wer trägt die Verantwortung für die Umsetzung der Maßnahme?
- In welchem Zeitraum soll die Maßnahme umgesetzt werden?
- Vorgaben zur Bewertung der Wirksamkeit einer Maßnahme. (Wann? Wie? Wer?)

Der Maßnahmenplan kann des Weiteren

- eine Ursachenanalyse zu festgestellten Mängeln (z. B. aus internen und externen Audits) sowie
- Zielvorgaben die mit einer Maßnahme erreicht werden sollen

beinhalten.

In jedem Fall trägt ein guter Maßnahmenplan immer dazu bei, Transparenz zu schaffen und Fortschritte aufzuzeigen. Faktoren, welche die Akzeptanz bei den Mitarbeitern im Unternehmen steigern.

Darüber hinaus muss auch die oberste Leitung eines Unternehmens ihren Beitrag zum Gelingen leisten. Sie hat regelmäßig den Fortschritt des ISMS zu beurteilen, um gegebenenfalls gegensteuern können. Ein probates Mittel ist dabei ein jährliches Managementreview, in dem die oberste Leitung das ISMS bewertet. Hier hat sich gezeigt, dass wenn die Unternehmensleitung engagiert die umzusetzenden Themen angeht, auch die Mitarbeiter entsprechend motiviert die notwendigen Aufgaben bearbeiten.

## Fazit

Der B3S WA hat sich in der Praxis als sehr gute Lösung für die Informationssicherheit erwiesen. Es sollte zukünftig als branchenspezifischer Standard von allen Unternehmen in der Abwasserbeseitigungsbranche angewendet werden. Die Anwendung bietet ein Mindestmaß an Informationssicherheit. Damit verbunden sollten die Unternehmen in regelmäßigen Abständen eine unabhängige Begutachtung durchführen lassen, um zu überprüfen, ob der Schutz der kritischen Infrastruktur nach den Anforderungen des B3S WA noch ausreichend gewährleistet ist.

## Autor

*Jan Feldhaus*
*Teamleitung Managementsysteme*
*DVGW CERT GmbH*
*Josef-Wirmer-Straße 13, 53123 Bonn*

*E-Mail: feldhaus@dvgw-cert.com* KA