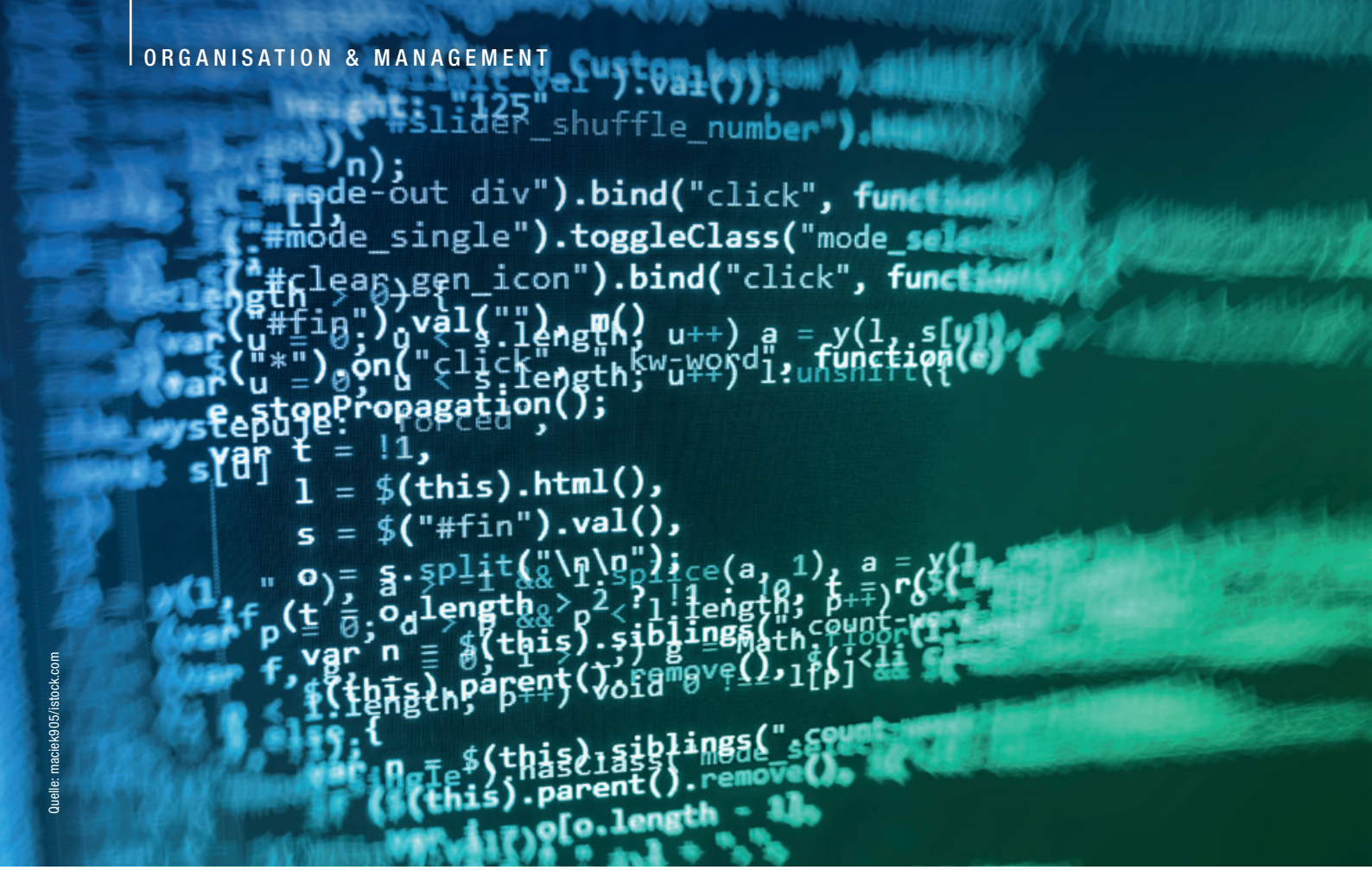

Quelle: maciek905/istock.com

Anforderungen an Wasserversorger und Abwasserentsorger

gemäß DVGW-Merkblatt W 1060 bzw. DWA-Merkblatt M 1060

Im Mai 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den gemeinsam von DVGW und der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA) entwickelten branchenspezifischen Sicherheitsstandard Wasser/Abwasser (B3S) genehmigt. Der B3S richtet sich in erster Linie an die Betreiber Kritischer Infrastrukturen, die bis Mai 2018 gegenüber dem BSI nachweisen müssen, dass sie den aktuellen Stand der IT-Technik einhalten. Ausgelegt ist der Standard allerdings so, dass er von allen Unternehmen der Wasserver- bzw. Abwasserentsorgung angewendet werden kann, um das interne Informationssicherheitsmanagement zu verbessern. In dem Beitrag werden die grundlegenden Anforderungen beschrieben, die sich aus der Anwendung des B3S in einem Unternehmen ergeben.

von: Raimund Alexander (DVGW CERT GmbH)

Betreiber Kritischer Infrastrukturen im Sektor Wasser haben mit dem Branchenstandard Wasser/Abwasser die Möglichkeit, die im BSI-Gesetz genannten Anforderungen umzusetzen, und können damit den Nachweis erbringen, den Stand der Technik für die relevanten informationstechnischen Systeme erreicht zu haben. Voraussetzung hierfür ist, dass die im DVGW-Merkblatt W 1060 (bzw. DWA-M 1060) dargestellten Anforderungen berücksichtigt und erfüllt werden. Der B3S Wasser/Abwasser dienst in diesem Zusammenhang als Basis für die Risikoabschät-

zung, Maßnahmenplanung und -umsetzung zum Schutz der IT-Systeme für den Anlagenbetrieb. Hierzu zählen die informationstechnischen Systeme, Komponenten, Prozesse und Daten von Wasserver- und Abwasserentsorgungsanlagen.

Gesetzlicher Rahmen

Aus dem § 8 a BSI-Gesetz (BSIG) ergeben sich auch organisatorische Anforderungen an die Betreiber Kritischer Infrastrukturen: So muss über die Verankerung einer Managementfunktion in der Organisation des Betreibers sichergestellt sein, dass der Stand der Technik erreicht und aufrechterhalten wird. Dazu muss ein entsprechendes Managementsystem im Unternehmen etabliert werden, beispielsweise durch die Einführung eines Informationssicherheits-Managementsystems. Auch können Betreiber Kritischer Infrastrukturen, die bereits ein Managementsystem nutzen, das Thema IT-Sicherheit ergänzend aufnehmen.

Um die Informationssicherheit dauerhaft zu kontrollieren, zu erhalten und zu verbessern, sind Verfahren und Regeln zwingend erforderlich. Deshalb ist grundsätzlich eine ganzheitliche Betrachtung des angestrebten Schutzniveaus im Rahmen eines Sicherheitskonzeptes durchzuführen: Hieraus können Informationsschutz- und Sicherheitsleitlinien abgeleitet werden, die – innerhalb der Organisation veröffentlicht – als Handlungsrahmen für die Mitarbeiter dienen. Damit der notwendige Schutz der informationstechnischen Systeme, Komponenten, Prozesse und Daten erreicht werden kann, sollte das Sicherheitskonzept auch Themen wie physische und umgebungsbezogene Sicherheit sowie Sicherheitsbereiche berücksichtigen.

Risikoabschätzung

Um den Schutzbedarf für Kritische Infrastrukturen ermitteln zu können, ist eine Risikoabschätzung für die in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) aufgelisteten Anlagentypen durchzuführen. Hierunter fallen in der Trinkwasserversorgung und Abwasserbeseitigung u. a. Gewinnungsanlagen, Wasserwerke, Kläranlagen und Leitzentralen. Weiterführende Informationen hierzu können der BSI-KritisV Anhang 2 entnommen werden.

Eine allgemeine Risikoabschätzung für die genannten Anlagentypen aus dem BSI-Gesetz Anhang 2 ist nicht Bestandteil des B3S, sondern vielmehr die mit dem Einsatz der Informationstechnik verbundenen Risiken beim Betrieb der Anlagen. Eine allgemeine Risikoabschätzung ist somit nicht Teil der Prüfung nach dem B3S und wird folglich nicht als Prüfpunkt im Prüfplan geführt.

Um eine Basis für die Risikoabschätzung zu erhalten, sind die Assets der Kritischen Infrastruktur zu dokumentieren und hier insbesondere IT-Komponenten und -Systeme sowie Prozesse. Als Grundlage hierfür ist ein generischer Netzplan zu erstellen, der auch die IT-Systeme enthalten muss. Darüber hinaus müssen auch der Verwendungszweck, die Schnittstellen und der Aufstellungsort dokumentiert werden. Die als relevant eingestuften Systeme sind so zu erfassen, dass sie eindeutig identifizierbar sind und ihre Funktion in Bezug auf den Anlagenbetrieb nachvollziehbar ist. Eine entsprechende Dokumentation ist eine wesentliche Voraussetzung für einen erfolgreichen Prüfprozess, da der Prüfer anhand des Netzstrukturplans die kritischen Infrastrukturkomponenten und deren funktionale Zusammenhänge erkennen kann.

Von zentraler Bedeutung ist die eindeutige Bestimmung der betroffenen Systeme und Abgrenzung zu anderen Anlagen und Anlagenteilen sowie Systemen. Damit kann der Prüfumfang exakt auf den Geltungsbereich der Prüfung abgebildet werden. Kommt es hier zu Abweichungen, kann unter Umständen die Prüfung bzw. das Prüfergebnis als nicht ausreichend bewertet werden.

Während einer Prüfung werden die ausgewählten Anwendungsfälle, das Gefährdungspotenzial und die zugehörigen Maßnahmen für Kritische Infrastrukturen begutachtet. Prüfungsrelevant sind in diesem Zusammenhang die IT-Systeme; hiervon ausgeschlossen sind Aspekte des Anlagenbetriebs, wie z. B. die Stromversorgung einer Anlage oder auch deren Zugang.

Informationssicherheit als Managementaufgabe

Da eine fortlaufende Verbesserung der Informationssicherheit gefordert ist, muss hierzu ein entsprechender Prozess im Unternehmen vorhanden sein. Dieser soll in geplanten Abständen die Neubewertung von Risiken in Bezug auf

bereits umgesetzte Maßnahmen sowie das Erkennen neuer Gefährdungen sicherstellen. Erreichen lässt sich diese Neubewertung mithilfe eines internen Audits, in dessen Rahmen das Gefährdungspotenzial der Anlagen im Bereich der Kritischen Infrastruktur bewertet wird. Damit lassen sich Risiken neu einstufen und umgesetzte Maßnahmen hinsichtlich ihrer Wirksamkeit bewerten bzw. erforderliche Maßnahmen identifizieren. Das interne Audit ermöglicht auch die Nachweisführung, ob die Organisation regelmäßig Informationen über die Wirksamkeit und Aufrechterhaltung der festgelegten Maßnahmen erhält.

Da Informationssicherheit auch eine Managementaufgabe ist, muss die oberste Leitung einer Organisation in geplanten Abständen die Wirksamkeit, Eignung und Angemessenheit der festgelegten Maßnahmen bewerten. Um das zu ermöglichen, müssen auch die Ergebnisse aus dem internen Audit in das Managementreview einfließen. Es ist die Aufgabe der obersten Leitung, die Risiken entsprechend ihrer Priorität zu bewerten und für die hieraus abgeleiteten Maßnahmen den Umsetzungsprozess verantwortlich zu begleiten. Hiermit kann der Nachweis der fortlaufenden Verbesserung der Informationssicherheit erbracht werden. Ein ausreichender Bewertungsprozess sollte dabei die Aspekte „Rückmeldung über die Informationssicherheitsleistung", „Ergebnisse der Risikobeurteilung", „Status von Maßnahmen vorheriger Managementbewertungen" und „Möglichkeiten zur fortlaufenden Verbesserung" berücksichtigen.

Umsetzungsplan

Festgelegte Maßnahmen sind in einem Umsetzungsplan zu erfassen und mit Zuweisung der Verantwortlichkeiten, der erforderlichen Ressourcen sowie der Termine für die Realisierung zu dokumentieren. Um den Nachweis der Umsetzung erbringen zu können, ist die inhaltlich korrekte, vollständige sowie fristgerechte Umsetzung von Maßnahmen geeignet zu dokumentieren.

Können die (basierend auf den im B3S definierten Anwendungsfällen entsprechend zugeordneten) Maßnahmen nicht durchgeführt werden, so ist das zu begründen und zu dokumentieren. Dabei gilt für Kritische Infrastrukturen: Die Akzeptanz eines Risikos mit einer mittleren oder hohen Eintrittswahrscheinlichkeit, das zum Ausfall einer Anlage führt, ist nicht zulässig. Wird während einer Prüfung ein solcher Fall festgestellt, muss das im Prüfbericht entsprechend als Abweichung dokumentiert werden. Dies gilt auch für den Abschluss von Versicherungen oder die Bildung von Rücklagen, also die Verlagerung von Risiken, da hiermit nicht der nach dem BSIG geforderte Stand der Technik erreicht wird.

Bei der Bewertung von Maßnahmen nach primär wirtschaftlichen Gesichtspunkten gilt für Kritische Infrastrukturen, dass für Maßnahmen, die als wirtschaftlich nicht angemessen bewertet wurden, alternative Maßnahmen mit einem ähnlich hohen Schutzniveau zu entwickeln und umzusetzen sind. Prüfungsrelevant sind auch die Qualifikationen des Personals, das am Umsetzungsprozess und der Durchführung von Maßnahmen beteiligt ist. Eine mögliche Nachweisführung für den ordnungsgemäßen Personaleinsatz besteht darin, geeignete dokumentierte Informationen wie Stellenbeschreibungen, Ausbildungsnachweise sowie Qualifikationsnachweise vorzulegen.

Steuerung der Informationssicherheit

Zum Nachweis der Steuerung von Informationssicherheit ist es erforderlich, dass Vorfälle, die nicht zum standardmäßigen Betrieb eines Services gehören, aufgezeichnet werden. Dazu zählen u. a. erkannte oder vermutete Sicherheitsvorfälle sowie Störungen in der Informationstechnik. Mittels eines IT Störungsmanagements (IT-Incident Management) lassen sich diese erfassen und in ausreichender Qualität dokumentieren. Der Bearbeitungsstand einer Störung und deren Behebung kann verfolgt werden, sodass das Unternehmen belegen kann, dass auf Störungen kontrolliert und geplant reagiert wird. Letzteres wird auch als wichtiges Element des fortlaufenden Verbesserungsprozesses bewertet und gilt daher als prüfungsrelevant.

Das BSIG fordert zwar nicht zwingend die Umsetzung eines Informationssicherheits-Managementsystems, wohl aber die Aufrechterhaltung der Kritischen Infrastruktur bzw. der kritischen Dienstleistung. Dies impliziert die Sicherstellung, das Erreichen sowie das Aufrechterhalten des Standes der Technik für die IT-Systeme des Anlagenbetriebs. Hier kann ein Managementsystem mit definierten Prozessen und einer gelenkten Dokumentation entsprechend unterstützen.

Nachweisführung

Essenziell für das Ergebnis einer Prüfung im Rahmen des § 8 a BSIG gemäß Branchenstandard B3S ist der Nachweis einer Risikoabschätzung, basierend auf den dokumentierten Assets. Diese Abschätzung muss die Elemente „Risikoidentifikation", „Risikoanalyse" und „Risikobewertung" umfassen, um als zielführend bewertet werden zu können. Die Organisation der Informationssicherheit ist in einer IT-Leitlinie zu beschreiben, die neben den Informationssicherheitszielen auch die Verpflichtung definiert, sowohl zutreffende Anforderungen mit Bezug zur Informationssicherheit als auch fortlaufende Verbesserungen der Informationssicherheit zu erfüllen. Sie ist innerhalb des Unternehmens bekannt zu machen und bildet damit den organisatorischen Rahmen für die Erstellung weiterer Regeln und Anweisungen zur Informationssicherheit. Da in der Regel die oberste Leitung die Sicherheitsrichtlinien verabschiedet, aber die Umsetzung durch nachgeordnete Personen erfolgt, müssen die Verantwortlichkeiten und Kompetenzen verbindlich festgelegt werden. Die Wirksamkeit der durchgeführten Maßnahmen ist zu überprüfen und nachzuweisen. Hieraus ergibt sich die Verpflichtung, die Ergebnisse der Überprüfung – also z. B. des internen Audits oder des Managementreviews – revisionssicher zu dokumentieren.

Fazit

Der branchenspezifische Standard B3S Wasser/Abwasser ermöglicht als spezifischer IT-Sicherheitsstandard den Schutz der IT-Systeme im Bereich der Kritischen Infrastrukturen. Somit ist der B3S ein Werkzeug, mit dessen Hilfe alle Unternehmen der Wasserver- und Abwasserentsorgung, unabhängig von ihrer Größe, einen Schutz für ihre informationstechnischen Systeme aufbauen können. Da Betreiber Kritischer Infrastrukturen mindestens alle zwei Jahre die Erfüllung der Anforderungen nach § 8 a Absatz 1 BSIG auf geeignete Weise nachzuweisen haben, können Unternehmen aus dem Sektor Wasserver- und Abwasserentsorgung diesen Nachweis mit der Umsetzung des B3S gegenüber dem BSI erbringen. ■

Der Autor

Dipl.-Ing. (FH) Raimund Alexander ist Auditor und Fachzertifizierer für Management-Systeme (DIN ISO/IEC 27001/ IT-Sicherheitskatalog) bei der DVGW CERT GmbH in Bonn.

Kontakt:
Raimund Alexander
DVGW CERT GmbH
Josef-Wirmer-Str. 1–3
53123 Bonn
Tel.: 0228 9188-839
E-Mail: alexander@dvgw-cert.com
Internet: www.dvgw-cert.com