Quelle: BWB/Jack Simanzik

Erfahrungen bei der Implementierung

des branchenspezifischen Sicherheitsstandards Wasser/Abwasser in einem Wasserversorgungsunternehmen

Am 3. Mai 2018 ist die Frist abgelaufen, bis zu der die Betreiber kritischer Infrastrukturen einen Nachweis gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erbringen mussten. Dabei muss ein Nachweis darüber erbracht werden, wie die Informationssicherheit zum Schutz der betriebenen Kritischen Infrastrukturen sichergestellt wird. Betroffen von dieser Pflicht waren u. a. auch Betreiber von Wasserversorgungsanlagen, die einen Schwellenwert von 22.000.000 m³/a überschreiten. Die Berliner Wasserbetriebe (BWB) waren eines der ersten Unternehmen, welches den gesetzlichen Nachweis erbringen konnten. Im Interview berichten Claudia Weißenfels und Jan Goebel von der BWB über ihre Erfahrungen.

Frau Weißenfels, Herr Goebel, darf man den Berliner Wasserbetrieben gratulieren? Immerhin haben Sie erfolgreich ein System zum Schutz der Kritischen Infrastruktur in dem Bereich Wasserversorgung aufgebaut und konnten somit den Nachweis nach § 8 a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) gegenüber dem BSI erbringen.

Frau Weißenfels: Wir sind über das Auditergebnis sehr erfreut, da es beweist, dass wir auf dem richtigen Weg sind und wir mit den getroffenen Maßnahmen unseren gesetzlichen Verpflichtungen gerecht werden. Wir halten externe Evaluation für wichtig, da die Auditoren nicht zum Betrieb gehören und somit aus einer ganz anderen Perspektive unsere Konzepte be-

gutachten und wir auch auf diesem Wege weitere Impulse und Anregungen für eine Verbesserung erhalten.

Der Schutz unserer modernen digitalisierten Gesellschaft ist nicht mehr nur durch physische Angriffe, sondern auch abstrakt aufgrund von Cyberkriminalität bedroht. Das Hauptaugenmerk der gesetzlichen Verpflichtung liegt daher auch auf dem Schutz der modernen Informationstechnik, sowohl physisch als auch digital. Was halten Sie vor diesem Hintergrund von der gesetzlichen Verpflichtung? Sollte es nicht selbstverständlich sein, dass ein Unternehmen, welches sich mit Trinkwasser, unserem wichtigsten Lebensmittel beschäftigt, alles dafür tut, den Schutz der Kritischen Infrastruktur aufrechtzuerhalten?

Herr Goebel: Die Bereitstellung von sensiblen Dienstleistungen bringt eine besondere Verantwortung mit sich. Unternehmen, die solche Kritischen Infrastrukturen betreiben, sind verpflichtet, jegliches Risiko wie Ausfall oder Beeinträchtigung zu minimieren. Der Einsatz von Informationstechnologien wird immer mit Qualitäts- und Effizienzsteigerung verbunden, bedeutet aber auch ein verändertes Bedrohungs-Szenario für die jeweiligen Unternehmen und deren Kernprozesse. Die täglich wachsende Anzahl unterschiedlichster Gefahren und Risiken für die eingesetzte Informationstechnik und die Systeme ist heute eine große Herausforderung. Zudem haben die technischen Möglichkeiten für komplexe Angriffe stark zugenommen.

Quelle: BWB

Jan Goebel und Claudia Weißenfels

Das bedeutet, dass Sicherheitskonzepte und -maßnahmen ständig angepasst und erweitert werden müssen, was mit hohen finanziellen Belastungen einhergeht. Diese können im wirtschaftlichen Wettbewerb durchaus zu einem Interessenkonflikt führen. Es ist daher durchaus vorstellbar, dass aus wirtschaftlichen Gründen auf erforderlichen Schutz verzichtet wird. Deshalb ist es aus unserer Sicht sinnvoll, dass es zum einen besondere gesetzliche Verpflichtungen und Regelungen beim Betrieb Kritischer Infrastrukturen gibt und zum anderen deren Einhaltung kontinuierlich überprüft wird.

Sie haben für den Aufbau des Systems den sogenannten Branchenstandard Wasser/Abwasser (B3S), welcher aus dem DVGW-Merkblatt W 1060 bzw. dem DWA-Merkblatt M 1060 besteht sowie dem daran angegliederten IT-Sicherheitsleitfaden, gewählt. Dieser stellt jedoch nur eine Möglichkeit dar, ein den Anforderungen des BSI entsprechendes System aufzubauen. Warum haben Sie sich für den B3S entschieden?

Frau Weißenfels: Wir haben uns bereits umfassend mit anderen Standards wie z. B. der ISO 27001 auseinandergesetzt und diese auch in verschiedenen Bereichen eingeführt und zertifizieren lassen. Die Berliner Wasserbetriebe haben mit anderen Unternehmen aus der Branche an dem branchenspezifischen Sicherheitsstandard (B3S) Wasser/Abwasser mitgearbeitet. Wir wollten zum einen Erfahrungen mit der Anwendung des B3S Wasser/Abwasser sammeln und zum anderen unsere Sicherheitsprozesse und Maßnahmen mit den Branchenvorgaben abgleichen. Dabei konnten wichtige Erfahrungen für die Weiterentwicklung des Branchen-

standards gesammelt und Maßnahmen aus dem IT-Sicherheitsleitfaden bei uns umgesetzt werden.

Wann haben Sie begonnen, sich mit dem Thema zu beschäftigen? Gab es einen Zeitplan, an dem Sie sich bei der Umsetzung des B3S orientiert haben? Und haben Sie eventuell auch externe Hilfe für den Aufbau des Systems in Anspruch genommen?

Herr Goebel: Die Informationssicherheit ist bei den Berliner Wasserbetrieben seit Jahren ein zentrales Thema. Einige Systeme und Strukturen sind bereits seit 2011 nach der ISO 27001 zertifiziert. Die Anwendung und Umsetzung des B3S Wasser/Abwasser wurde mit der Veröffentlichung im September 2017 von einem fachübergreifenden Projektteam ausgesteuert und begleitet. Da der Auditierungs-Zeitpunkt frühzeitig angekündigt wurde, konnten wir unsere internen Zeitpläne entsprechend darauf abstimmen. Dabei haben wir uns während der gesamten Umsetzung eng mit dem BSI, unserer Prüfstelle und anderen Unternehmen ausgetauscht und abgestimmt.

Welches waren für Sie die größten Herausforderungen bei der Einführung eines Systems zum Schutz Kritischer Infrastrukturen gemäß dem B3S?

Frau Weißenfels: Der systematische Ansatz des B3S Wasser/Abwasser hat uns grundsätzlich vor keine grundlegend neuen Herausforderungen gestellt, da unser Unternehmen wegen seiner Rolle und Verantwortung als Kritische Infrastruktur seit jeher Informationssicherheits-Managementsysteme (ISMS) in diesen Unternehmensbereichen eingeführt hat. Die Prüfung der umzusetzenden BSI-Maßnahmen aus dem IT-Sicherheitsleitfaden dagegen war eine größere Herausforderung. Da die Berliner Wasserbetriebe über eine Vielzahl von kritischen Systemen und Anlagen verfügen, haben wir innerhalb des Projektes eine Datenbank zur Prüfung und als Auditierungsunterstützung erstellt. Dabei wurden über 2.000 Anforderungen formuliert, die systemspezifisch von Fachexperten bewertet und in der Datenbank dokumentiert werden mussten. Dies war ein größerer Aufwand als zu Beginn erwartet. Wir konnten aber durch die Anwendung des B3S Wasser/Abwasser und die damit verbundene Prüfung einige Prozessabläufe weiter verbessern und schärfen

In jedem Unternehmen gibt es Schnittstellen zwischen den verschiedenen Bereichen. Welche Schnittstellen gab es in Ihrem Unternehmen, die Sie betrachtet haben? Entstanden hierdurch neue Herausforderungen; mussten Sie z. B. Bereiche neu strukturieren um diese besser von der Kritischen Infrastruktur abzugrenzen?

Herr Goebel: Bereits seit dem Jahr 2015 haben wir eine zentrale Abteilung, die sich mit der Unternehmenssicherheit beschäftigt. Diese Abteilung koordiniert Arbeitsgruppen und Gremien rund um das Thema Sicherheit. Die sicherheitsrelevanten Bereiche sind durch bestehende Konzepte zur Unternehmenssicherheit identifiziert. Somit kam es nicht zu der Notwendigkeit, weitergehende Abgrenzungen vorzunehmen. Da die Risikosituation und die Technologie jedoch einer ständigen Veränderung ausgesetzt sind, wird es zwangsläufig zu Anpassungen von Zuständigkeiten und Verantwortungen kommen. In unserem Fall halten sich diese Anpassungen aber in einem überschaubaren Rahmen.

Der B3S ist bekanntlich so aufgebaut, dass er unabhängig von der Unternehmensgröße von allen Unternehmen in der Wasserversorgung und Abwasserreinigung angewendet werden kann. Würden Sie daher auch den Unternehmen, die (noch) nicht dazu verpflichtet sind, einen Nachweis gegenüber dem BSI zu erbringen, empfehlen, ein System nach dem B3S aufzubauen und im Anschluss eine unabhängige Prüfung durch eine Konformitätsbewertungsstelle durchzuführen?

Frau Weißenfels: Auch ohne gesetzliche Verpflichtung können Informationssicherheits-Managementsysteme einen großen Mehrwert an Sicherheit für Unternehmen und deren Kernprozesse liefern. Dieser Sicherheitsgewinn ist oftmals sogar wirtschaftlich und mithilfe eines Risikomanagements und einer „Return on Security Investment"-Methodik nachzuvollziehen. Außerdem fördert ein regelmäßiges Nachweisverfahren den kontinuierlichen Verbesserungsprozess im Unternehmen und erzeugt einen ständigen Bedarf, zusätzliche Maßnahmen zur weiteren Verbesserung der Sicherheit umzusetzen oder vorhandene Verfahren zu modifizieren.

Was die meisten Betreiber Kritischer Infrastrukturen nicht wissen, ist, dass das Nachweisverfahren über die Einführung eines Systems zum Schutz Kritischer Infrastrukturen gemäß dem B3S keine Zertifizierung ist und auch nicht mit einer Bestätigung des Systems abschließt. Das hat den folgenden Hintergrund: Das BSI behält es sich vor, die endgültige Entscheidung darüber zu treffen, ob eine Organisation einen ausreichenden Schutz ihrer Kritischen Infrastruktur gewährleistet oder

nicht. Zertifikate oder Bescheinigungen sind daher für das BSI nicht bindend und werden auch nicht von diesem als Nachweis anerkannt. Vielmehr verlangt das BSI als Ergebnis des Nachweisverfahrens eine Liste aller Mängel, die im Prüfverfahren aufgetreten sind, sowie einen kurzen Bericht der Prüfstelle, in dem diese eine Bewertung vornimmt. War das Ganze nicht auch für Sie etwas irritierend? Was würden Sie sich wünschen, wenn Sie an dem Nachweisverfahren gegenüber dem BSI (nicht dem Nachweisverfahren nach B3S) etwas ändern könnten?

Herr Goebel: Insgesamt waren wir mit dem Nachweisverfahren zufrieden. Das BSI hat frühzeitig detaillierte und verständliche Orientierungshilfen veröffentlicht, sodass wir eine Vorstellung davon hatten, wie das Nachweisverfahren ablaufen wird. Bei offenen Fragen haben wir uns immer direkt an das BSI und unsere Prüfstelle gewandt.

Das Nachweisverfahren ist in diesem Jahr erstmalig in Deutschland durchgeführt worden. Sicherlich gibt es einige wenige Themen, die bis zum nächsten Nachweisverfahren nochmal präzisiert werden könnten – z. B. ob es sinnvoll ist, die Betreiber bzw. die Prüfstellen zu verpflichten, alle Anlagen eines Verbundsystems einer Vorort-Prüfung zu unterziehen. Hier würden wir uns wünschen, dem Auditor die Freiheit einzuräumen, Anlagen aus einem Verbundsystem auszuwählen und diese dann einer genauen Prüfung zu unterziehen. Auch würde ein zeitlicher Orientierungsrahmen, wie lange eine gewissenhafte Auditierung pro registrierter Anlage dauern sollte, helfen, die Zeitpläne und Abstimmungen vor dem Audit besser zu planen.

Wünschenswert für den auditierten Betrieb wäre darüber hinaus auch ein verwertbares Prüfergebnis. Bislang endet das Audit mit einer Liste aller Mängel, die im Prüfverfahren aufgetreten sind, sowie einem kurzen Bericht der Prüfstelle, in dem diese eine Bewertung vornimmt. Das momentane Verfahren sieht vor, dass das BSI sich die endgültige Entscheidung vorbehält, ob eine Organisation einen ausreichenden Schutz ihrer Kritischen Infrastruktur gewährleistet oder nicht. Das Audit liefert für diese Entscheidung also nur die Grundlage. Dies kann zu Irritationen bei der Auditierung führen.

Nun haben Sie zwei Jahre Zeit, bis Sie erneut einen Nachweis über die Funktionalität Ihres Systems gemäß B3S gegenüber dem BSI erbringen müssen. Gibt es konkrete Maßnahmen, die Sie bis dahin angehen möchten?

Frau Weißenfels: Für uns gilt: Nach dem Audit ist vor dem Audit. Bei einem integrierten kontinuierlichen Verbesserungsprozess finden sich immer wieder Maßnahmen und Prozessoptimierungen. Und ja, natürlich wurden bei der Auditierung auch einige Verbesserungspotenziale festgestellt, die zu konkreten Handlungsbedarf führen. Dabei geht es oft um Standardisierungen und Vereinfachungen.

Was würden Sie abschließend Unternehmen raten, die sich gerade damit beschäftigen, ein System zum Schutz ihrer Kritischen Infrastruktur gemäß dem B3S aufzubauen?

Herr Goebel: Nach unserem Kenntnisstand bietet der B3S Wasser/Abwasser insgesamt eine gute Orientierung und Arbeitshilfe für einen systematischen Aufbau eines Informationssicherheits-Managementsystems. Ein systematischer und methodischer Aufbau ist die Basis für ein funktionierendes und nachhaltiges ISMS. Themen wie Risiko- oder Qualitätsmanagement spielen dabei eine zentrale Rolle und müssen entsprechend mit beachtet werden.

Natürlich muss jedes Unternehmen selbst entscheiden, in welcher Tiefe oder auch mit welchen Ergänzungen der B3S Wasser/Abwasser jeweils zur Anwendung kommt. Hier spielen Unternehmensstruktur und -organisation eine wichtige Rolle. In unserem Falle haben wir neben den B3S Wasser/Abwasser auch die ISO 27001 in einigen Strukturen implementiert. ■

Das Gespräch führte Jan Feldhaus von der DVGW CERT GmbH.