In der Praxis: Der IT-Sicherheitsleitfaden für die Wasserwirtschaft

Die Branche Wasser/Abwasser hat bereits in den letzten Monaten erste Umsetzungserfahrungen im Hinblick auf eine geforderte Zertifizierung und den Stand der Technik nach dem IT-Sicherheitsgesetz (IT-SiG) gesammelt. Der Artikel beschäftigt sich mit den aktuellen Vorgaben sowie deren konkreter Umsetzung in aktuellen Projekten.

IT-Sicherheit ist in den letzten Monaten durch eine Vielzahl von destruktiven Cyberangriffen in den Fokus der öffentlichen Berichterstattung gerückt. Nun wurde am 1. August 2017 der Branchenstandard für die Wasser- und Abwasserwirtschaft als erster IT-Sicherheitsstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen KRITIS-Sektor anerkannt. Die Branchenverbände DWA und DVGW stellen dazu seinen Mitgliedern ein Merkblatt und den IT-Sicherheitsleitfaden zur Verfügung. Dieser branchenspezifische Sicherheitsstandard enthält verbindliche Rahmenanforderungen, die eine Vorgehensweise zur Risikoanalyse sowie eine Sammlung von Sicherheitsmaßnahmen, um den identifizierten Risiken zu begegnen. Die darin beschriebenen Mindestvorgaben sollten von allen Anlagenbetreibern umgesetzt werden – unabhängig davon, ob eine Anlage bereits heute eine kritische Infrastruktur ist oder nicht.

Hierzu erklärte Arne Schönbohm, BSI-Präsident: „Der branchenspezifische Sicherheitsstandard Wasser/Abwasser ist die Grundlage für mehr Cyber-Sicherheit in diesem für Staat, Wirtschaft und Gesellschaft lebenswichtigen Versorgungsbereich. Wie wichtig das notwendige Maß an IT-Sicherheit in der Digitalisierung ist, haben Cyber-Angriffe wie WannaCry oder Petya/NotPetya gezeigt, bei denen auch Unternehmen in Deutschland erhebliche Schäden erlitten haben." Bei dieser Art von Schadsoftware spricht man von Ransomware. Hierbei werden alle wichtigen Daten verschlüsselt. Eine Freigabe dieser Daten erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). In der Regel sind diese Daten verloren.

Der aktuelle BSI-Lagebericht stellt neben den bestehenden Ransomware-Angriffen die weiter zunehmende Anzahl an sogenannten Advanced Persistent Threats (APT) besonders in den Fokus. Diese sind meist sehr komplex und werden in mehreren Phasen durchgeführt. Das Ziel eines APT ist es, über eine längere Zeitdauer vertrauliche Informationen auszuspähen oder zielgerichtet Schaden anzurichten. Voraussichtlich werden zukünftig diese zielgerichteten Cyber-Angriffe durch gut organisierte und professionell ausgestattete Angreifer die höchste Gefährdung für Unternehmen sein (***Bild 1***).

Eine aktuelle Angriffsform für vernetzte Automatisierungsanlagen sind die Industroyer. Diese missbrauchen keine Lücken in den vernetzten Automatisierungsgeräteschaften, sondern sprechen einfach in deren Sprache, indem sie die in Industrieumgebungen gängige Kommunikationsprotokolle beherrschen. Dabei können Angreifer monatelang im Netzwerk aktiv sein und die notwendigen Informationen zusammentragen. Beispielsweise gehören Löschfunktionen, die sämtliche Spuren des Angriffs

Bild 1: Leitstand mit IT-Netzüberwachung

verwischen, Konfigurationsdateien löschen und das Betriebssystem des befallenen Windows-PC in einen nicht startfähigen Zustand versetzen, zum Funktionsumfang.

Kernelemente des IT-Sicherheitsleitfadens

Nach den jüngsten Cyber-Vorfällen bestätigt sich das Ziel der Bundesregierung mit dem IT-Sicherheitsgesetz die Verfügbarkeit und Sicherheit der IT-Systeme in Kritischen Infrastrukturen verbindlich zu regeln.

Der Branchenspezifischen Sicherheitsstandard Wasser/Abwasser enthält als konkrete Umsetzungsvorgabe neben den Merkblättern DVGW W 1060 (M) bzw. DWA M 1060 den IT-Sicherheitsleitfaden. Er gibt allen Betreibern (nicht nur den KRITIS) von Anlagen der Trinkwasserversorgung und Abwasserentsorgung einen praktischen Handlungsrahmen zur Erreichung des im IT-Sicherheitsgesetz geforderten Stand der Technik für den Betrieb der eingesetzten IT-Systeme.

Dabei orientiert sich der Standard am BSI-Grundschutz mit den fünf wesentlichen Schritten:

- Infrastruktur-/Anlagenauswahl und -abgrenzung
  Zunächst sind die relevanten Anlagen auf Basis der BSI-Kritisverordnung zu bestimmen und zuzuordnen.
- Identifikation der relevanten IT-Systeme durch Inventarisierung der Werte (Assets)
  Als wesentliche Vorarbeit ist zunächst ein Inventarverzeichnis der vorhandenen IT-Systeme, -Komponenten und Anwendungen zu erstellen. Darauf basierend ist die vollständige IT-Netzarchitektur in einem logischen und einem physischen Netzplan zu dokumentieren, in dem aktuellen Verknüpfungen zwischen den einzelnen Elementen eindeutig erkennbar sind.
- Bestimmung und ggf. Ergänzung der Anwendungsfälle
  Im IT-Sicherheitsleitfaden werden aktuell sechs Kategorien von Anwendungsfällen unterschieden, die entsprechend mit dem aktuellen Anlagenbestand auszuwählen sind.
- Risikobewertung auf Basis der mit den Anwendungsfällen verbundenen Gefährdungen
  Als Ergebnis dieses Schrittes sollen vornehmlich die konkreten Risiken zur weiteren Behandlung gefunden werden, die bei Eintritt des Schadens mit einer Einschränkung oder gar dem Ausfall des Anlagenbetriebs verbunden sind.
- Maßnahmen ermitteln und umsetzen
  Aus der Liste der relevanten Gefährdungen lassen sich die Maßnahmen ermitteln und nach deren Zuweisung zu den relevanten IT-Systeme/-Komponenten eine Priorisierung der Maßnahmenumsetzung anhand der Risikobewertung durchführen.

Wesentliches Kernelement dieser Umsetzungsvorgabe ist die Kenntnis über die produktive IT-Infrastruktur und deren Kommunikationsbeziehungen. Denn eine valide Risikobeurteilung kann nur über einen aktuellen Stand der vernetzen IT-Systeme und -Komponenten erfolgen und nachgewiesen werden. Dabei sind Netzpläne ein wichtiges Werkzeug, weil sie das Zusammenspiel der IT-Infrastruktur und -Anwendungen erkennen lassen.

Best Practice und Erfahrungen in der Wasserwirtschaft

Auch wenn der Branchenstandard Wasser/Abwasser erst im August verabschiedet wurde, gibt es bereits Erfahrungen bei der Einführung eines Informationssicherheitsmanagement in der Branche.

Dabei wird als wichtiger Erfolgsfaktor die Etablierung einer übergreifenden Verantwortung für Informationssicherheit sowohl für die Automatisierungs-IT als auch für die Büro-IT gesehen. „Trotz informationstechnischer Trennung der Steuerungsnetze Gas, Wasser, Abwasser wurde die Gesamtverantwortung für den Bereich IT-Sicherheit, auch für die Büro-IT, in einen eigenständigen Verantwortungsbereich gelegt“, so Dieter Meyer, Prokurist und Bereichsleiter für Versorgung und Erzeugung der StadtWerkegruppe Delmenhorst.

Neben der Etablierung eines Informationssicherheitsmanagement (ISMS) sowie eines Notfallmanagements sind insbesondere vor dem Hintergrund der gesetzlichen Meldepflicht der Umgang mit Sicherheitsvorfällen zu regeln und umzusetzen. Das frühzeitige Erkennen eines möglichen Sicherheitsvorfalls wird in der Regel das Schadensausmaß begrenzen, wenn nicht sogar den Schadenseintritt verhindern. Manipulationen, Vorbereitungen oder die Durchführung von Cyberangriffen lassen sich nur durch ein kontinuierliches Monitoring der vernetzten Systeme und des Datenverkehrs in Echtzeit erkennen. Aufgrund der notwendigen zeitkritischen Datenkommunikation in Produktionsanlagen ist aber jede zusätzliche Aktivität im Produktionsnetz oder gar das Verwerfen von Datenpaketen zu unterbinden. Denn diese kann die Echtzeitkommunikation stören oder Systeme zu Fehlfunktionen bis hin zum Ausfall der gesamten Produktionsanlage veranlassen. Daher ist das passive Scannen und Überwachen des Produktionsnetzes eine unabdingbare Anforderung an ein Überwachungssystem.

Hier existiert mit IRMA bereits ein etabliertes Produkt, mit dem sich der (Sicherheits-)Zustand der „IT-Anlage“ übersichtlich und ohne Experten-Knowhow visualisieren lässt (***Bild 2***). Das Risiko eines Systemausfalls wird erheb-

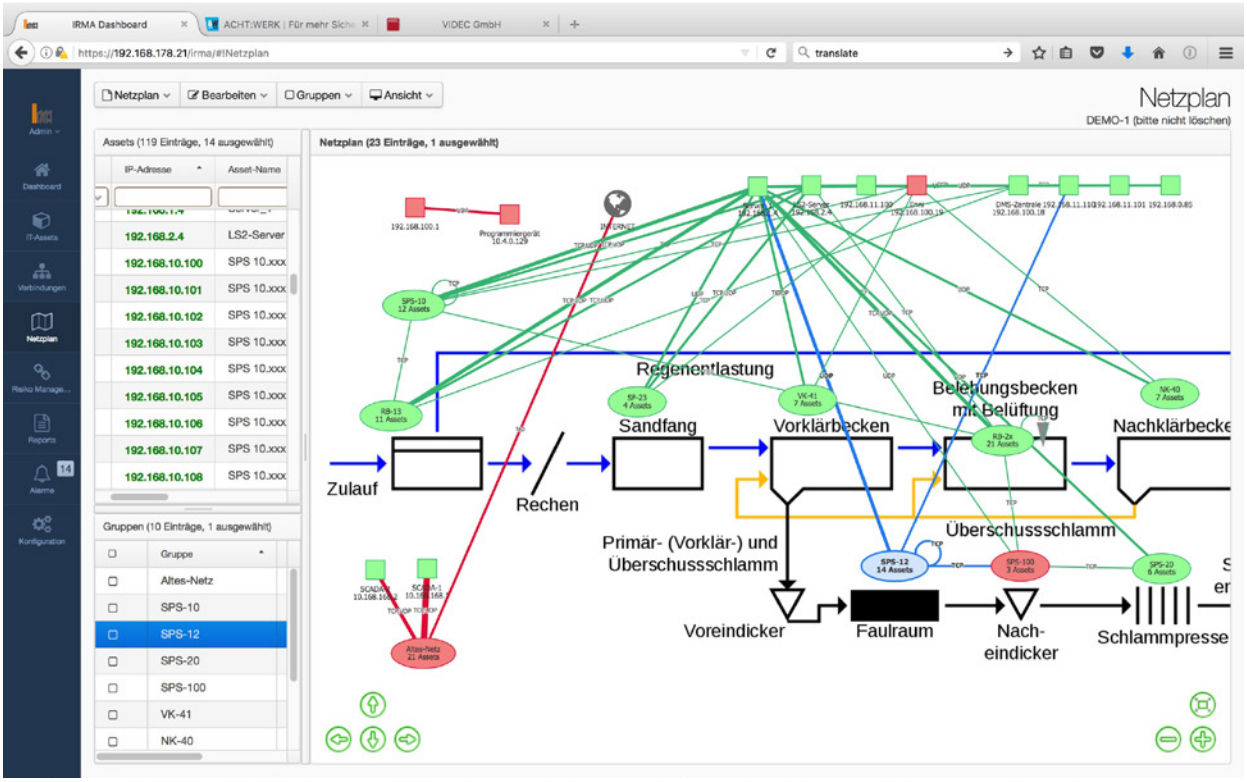

Bild 2: Netzplanstrukturplan in IRMA

lich minimiert. Bei anomalem Datenverkehr werden die Verantwortlichen automatisiert alarmiert und können handeln. Eine unmittelbare Meldung etwaiger Sicherheitsvorfälle an die Behörden ist damit möglich.

Um die im Branchenstandard geforderte Risikobewertung durchzuführen, sind zunächst alle vernetzten Anlagenbestandteile zu inventarisieren, denn nur was man kennt, kann man schützen. Unter wirtschaftlichen Gesichtspunkten sollte statt aufwendiger händischer Suche und Erfassung besser ein automatisiertes Erkennen über die Netzkommunikation ausnahmslos aller IT-Systeme erfolgen. Die Erstellung der geforderten Netzpläne kann dann auch gleich automatisiert erfolgen. Hierin liegt ein hohes Einsparpotenzial.

Ralph Bargmann (langjähriger BSI Auditor und Bereichsleiter IT, Organisation und Sicherheit der StadtWerkegruppe Delmenhorst): „IRMA ist eine weitere wichtige Sicherheitskomponente innerhalb der IT-Infrastruktur unserer Leit- und Automatisierungstechnik. Durch die kontinuierliche Überwachung haben wir die Sicherheit, dass etwaige Anomalien wie Falschkonfigurationen, Manipulationen oder Cyberangriffe erkannt und gemeldet werden. Mit Hilfe der IRMA stellen wir weiterhin sicher, dass sämtliche Komponenten („Assets") bekannt und damit zugelassen sind. IRMA ist damit ein wesentlicher Bestandteil für den sicheren und ordnungsgemäßen Betrieb unserer Prozessleitnetze." Mit Zuordnung der IT-Systeme zu den im Branchenstandard definierten Anwendungsfällen anhand des ausgewählten Anlagenbestandes lassen sich einfach die vorgeschriebenen Sicherheitsmaßnahmen ermitteln und umsetzen. Durch ein umfangreiches Reporting u.a. der Risikobewertung, Netzpläne, Alarme etc. innerhalb des Frühwarnsystems können Dokumentationspflichten effizient umgesetzt werden.

Auch Andreas Studemund, Leiter der Stabsstelle Automatisierungs- und Informationstechnik bei KASSELWASSER spricht sich für eine frühzeitige Einführung des Überwachungssystems aus: „Unsere Motivation IRMA einzuführen war die Erhöhung der Cybersecurity im Netzwerk für die Prozesssteuerung. Hier war das Ziel möglichst früh von Cyberattacken und ungewöhnlichen Netzwerkverhalten Kenntnis zu erlangen, um das interne Sicherheitsmanagement zu verbessern. Dieses Ziel wurde nach Abschluss der Systemeinführung erreicht. Da KASSELWASSER noch nicht zu KRITIS relevanten Unternehmen gehört, sehen wir die Einführung der IRMA als Vorbereitung auf kommende Anforderungen aus dem Branchenstandards Wasser/Abwasser oder einer möglichen späteren KRITIS Zugehörigkeit. IRMA ist jetzt neben Firewall und Network Access Control ein weiteres Standbein der Cybersicherheit in der Prozesssteuerung."

Fazit

Alle Betreiber im Sektor Wasser/Abwasser müssen mit der Genehmigung des Branchenstandards die Mindestanforderungen an die Informationssicherheit umsetzen. Man geht davon aus, dass in absehbarer Zeit die Höhe der Schwellwerte nach unten korrigiert werden müssen. Dabei sind geeignete Maßnahmen nach dem Stand der Technik wie die Erkennung und Abwehr von Cyberangriffen zu gewährleisten. Die ersten Erfahrungen zeigen, dass eine Übertragung der Gesamtverantwortung für die Informationssicherheit in der Organisation als sinnvoll und notwendig erscheint. Des Weiteren sind zu Beginn des kontinuierlichen Sicherheitsprozesses zunächst logische Netzstrukturpläne ein wichtiges Werkzeug, weil sie das Zusammenspiel der relevanten IT-Objekte veranschaulichen und beurteilbar machen. Durch die Etablierung eines effektiven Frühwarnsystems kann die Meldepflicht wirtschaftlich unterstützt werden. Mit dem Merkblättern DVGW W 1060 (M) bzw. DWA M 1060 sowie dem IT-Sicherheitsleitfaden sind die notwendigen Rahmenbedingungen des Branchenstandard bekannt. Eine sinnvolle und praktische Hilfe zu diesen Merkblättern bietet das Kurzhandbuch „IT Sicherheit“ von Phoenix Contact. In diesem „Leitfaden zum branchenspezifischen Sicherheitsstandard der Wasserwirtschaft“ werden notwendige Maßnahmen anschaulich erklärt und beschrieben. Sie erhalten dieses Kurzhandbuch auch über die VIDEC-Mitarbeiter.

AUTOREN

DIETER BARELMANN
VIDEC GmbH
28203 Bremen
Tel.: +49 421 339500
info@videc.de

STEFAN MENGE
Achtwerk GmbH & Co. KG
28277 Bremen
Tel.: +49 421 87847882
stefan.menge@acht-werk.de