Leitstand mit
IT-Netzüberwachung

XXX

Der IT-Sicherheitsleitfaden für die Wasserwirtschaft ist da – und nun?

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 konkreten Best-Practice-Maßnahmen. Dabei werden praktische Erfahrungen aus aktuellen Projekten in der Wasserwirtschaft vorgestellt.

Das Thema IT-Sicherheit ist in den letzten Wochen vor dem Hintergrund von destruktiven Cyber-Angriffen auf die Wirtschaft durch WannaCry, Petya & Co. 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 Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall sowie DVGW Deutscher Verein des Gas- und Wasserfaches stellen dazu ihren Mitgliedern ein Merkblatt und den IT-Sicherheitsleitfaden zur Verfügung. Dieser branchenspezifische Sicherheitsstandard enthält verbindliche Rahmenanforderungen, 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 eine kritische Infrastruktur ist oder nicht.

Laut BSI ist der branchenspezifische Sicherheitsstandard Wasser/Abwasser 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 WannaCry, Petya & Co. spricht man von Ransomware, die wichtige Daten verschlüsselt. Eine Freigabe dieser Daten erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). In der Regel sind diese Daten verloren. Beispielsweise hielt ein Cyber-Angriff des Kryptotrojaners NotPetya im Sommer dieses Jahres u. a. den dänischen Konzern Maersk für mehrere Wochen in Atem: Containerterminals standen still, Schiffe konnten weder gelöscht noch beladen werden. Maersk hat nach eigenen Angaben 200 bis 300 Mio. US-Dollar Verlust durch den Angriff erlitten.

Der aktuelle BSI-Lagebericht stellt neben den bestehenden Ransomware-Angriffen die weiter zunehmende Anzahl an Advanced Persistent Threats (APT) besonders in den Fokus. Voraussichtlich werden zukünftig diese zielgerichteten Cyber-Angriffe durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer die höchste Gefährdung für Unternehmen sein. APTs 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. Diese Art von Cyber-Angriffen hat häufig einen professionellen Hintergrund, wie z. B. Cyber-Kriminalität oder Wirtschaftsspionage (Abb. 1).

> Eine valide Risikobeurteilung kann nur über einen aktuellen Stand der vernetzten IT-Systeme und -Komponenten erfolgen und nachgewiesen werden.

Mit Stuxnet sind im Jahr 2010 diese intelligenten Cyber-Angriffe in der Industrie angekommen. Die gezielt entwickelte Schadsoftware für vernetzte Automatisierungen und Produktionsanlagen findet fokussiert ihre Ziele. Dies erfolgt so intelligent, dass die eigene Verbreitung versteckt und Schäden erst viel später als Cyber-Angriff erkannt werden.

Seit 2017 ist Industroyer im Fokus von Sicherheitsexperten. Industroyer missbraucht keine Lücken in den vernetzten Automatisierungsgerätschaften, sondern spricht einfach in deren Sprache, indem es die in Industrieumgebungen gängige Kommunikationsprotokolle beherrscht. Dabei können Angreifer monatelang im Netzwerk aktiv sein und die notwendigen Informationen zusammentragen. Beispielsweise gehören Löschfunktionen, die sämtliche Spuren des Angriffs 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 branchenspezifische Sicherheitsstandard Wasser/Abwasser enthält neben den Merkblättern DVGW W 1060 (M) bzw. DWA M 1060 den IT-Sicherheitsleitfaden zur Konkretisierung der Umsetzungsvorgaben. 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 folgenden 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 aktuelle Verknüpfungen zwischen den einzelnen Elementen eindeutig erkennbar sind.
- **Bestimmung und gegebenenfalls 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-Systemen/-Komponenten eine Priorisierung der Maßnahmenumsetzung anhand der Risikobewertung durchführen.

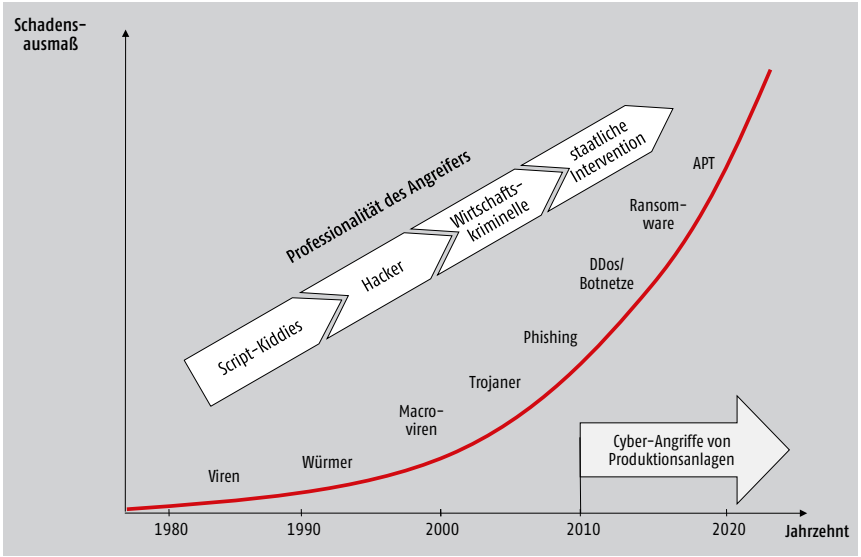


Abb. 1 – Die Entwicklung der Cyber-Angriffe

» Mit den Merkblättern des DVGW bzw. DWA sowie dem IT-Sicherheitsleitfaden sind die notwendigen Rahmenbedingungen des Branchenstandards bekannt – Unternehmen sollten daher sofort mit der Umsetzung beginnen! «

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 vernetzten 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 Informationssicherheitsmanagements 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. Die StadtWerkegruppe Delmenhorst berichtet, dass trotz informationstechnischer Trennung der Steuerungsnetze Gas, Wasser und Abwasser die Gesamtverantwortung für den Bereich IT-Sicherheit im Unternehmen, auch für die Büro-IT, in einen eigenständigen Verantwortungsbereich gelegt worden sei.

Neben der Etablierung eines Informationssicherheitsmanagements (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 Cyber-Angriffen 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 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.

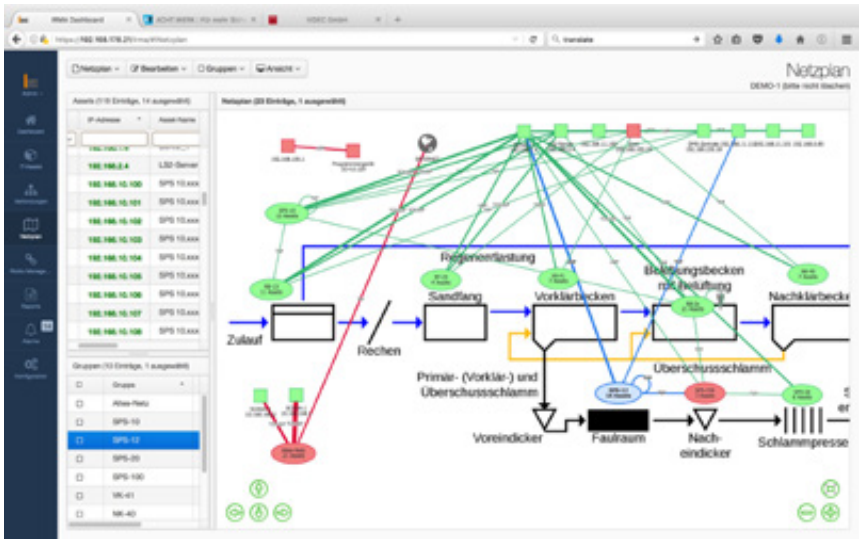
Hier existiert mit IRMA ein etabliertes Produkt, mit dem sich der (Sicherheits-)Zustand der „IT-Anlage“ übersichtlich und ohne Experten-Knowhow visualisieren lässt (Abb. 2). Das Risiko eines Systemausfalls wird erheblich minimiert. Bei anomalem Datenverkehr werden die Verantwortlichen automatisiert alarmiert 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. Hier liegt ein hohes Einsparpotenzial.

Die StadtWerkegruppe Delmenhorst berichtet hierzu, dass IRMA eine weitere wichtige Sicherheitskomponente innerhalb der IT-Infrastruktur der Leit- und Automatisierungstechnik des Unternehmens darstelle. Durch die kontinuierliche Überwachung habe man die Sicherheit, dass etwaige Anomalien wie Falschkonfigurationen, Manipulationen oder Cyber-Angriffe erkannt und gemeldet werden. Mithilfe von IRMA stelle das Unternehmen weiterhin sicher, dass sämtliche Komponenten („Assets“) bekannt und damit zugelassen sind. IRMA sei damit ein wesentlicher Bestandteil für den sicheren und ordnungsgemäßen Betrieb der 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 KASSELWASSER spricht sich für eine frühzeitige Einführung eines Überwachungssystems aus. Die Motivation, IRMA einzuführen, war hier die Erhöhung der Cyber-Security im Netzwerk für die Prozesssteuerung. Ziel sei gewesen, möglichst früh von Cyber-Attacken und ungewöhnlichem Netz-



XXX

Abb. 2 – Netzplanstrukturplan in IRMA

werkverhalten Kenntnis zu erlangen, um das interne Sicherheitsmanagement zu verbessern. Dieses Ziel sei nach Abschluss der Systemeinführung erreicht worden. Da das Unternehmen noch nicht zu KRITIS-relevanten Unternehmen gehört, sah es die Einführung von IRMA als Vorbereitung auf kommende Anforderungen aus dem Branchenstandard Wasser/Abwasser oder einer möglichen späteren KRITIS-Zugehörigkeit. IRMA sei jetzt neben Firewall und Network Access Control ein weiteres Standbein der Cyber-Sicherheit in der Prozesssteuerung.

Fazit

Alle Betreiber im Sektor Wasser/Abwasser müssen mit der Genehmigung des Branchenstandards die Mindestanforderungen an die Informationssicherheit umsetzen. Dabei sind geeignete Maßnahmen nach dem Stand der Technik wie die Erkennung und Abwehr von Cyber-Angriffen 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 Branchenstandards bekannt. Unternehmen sollten daher sofort mit der Umsetzung beginnen.

Danksagung

Die Autoren danken Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik, Dieter Meyer, Prokurist und Bereichsleiter für Versorgung und Erzeugung der StadtWerkegruppe Delmenhorst, Ralph Bargmann, langjähriger BSI-Auditor und Bereichsleiter IT, Organisation und Sicherheit der StadtWerkegruppe Delmenhorst sowie Andreas Studemund, Leiter der Stabsstelle Automatisierungs- und Informationstechnik bei KASSELWASSER, für ihre Statements.

Autoren

Dieter Barelmann
VIDEC Data Engineering GmbH
Contrescarpe 1
28203 Bremen
Tel.: 0421 33 950-0
dbarelmann@videc.de
www.videc.de

Stefan Menge
Achtwerk GmbH & Co. KG
Am Mohrenshof 11a
28277 Bremen
Tel.: 0421 878478-82
stefan.menge@acht-werk.de www.acht-werk.de