Umsetzung des IT-Sicherheitsleitfadens von DVGW und DWA - M1060/W1060

Am 1. August 2017 wurde der Branchenstandard für die Wasser- und Abwasserwirtschaft als erster IT-Sicherheitsstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen KRITIS-Sektor anerkannt. Doch wie sieht es mit der Umsetzung aus? Im folgenden Beitrag werden einige Schritte auf dem Weg für eine sinnvolle Implementierung in wasserwirtschaftlichen Betrieben vorgestellt.

Der Gesetzgeber hat mit dem IT-Sicherheitsgesetz (ITSiG) in 2015 den rechtlichen Rahmen gesetzt, um unter anderem die Vorgaben für die unterschiedlichen Branchen zu initiieren.

Rechtliche Anforderung

In der Wasser- und Abwasserbranche wurde daraufhin von DVGW und DWA der erste branchenspezifische Sicherheitsstandard (B3S) entwickelt. Allen Betreibern von Anlagen der Trinkwasserver- und Abwasserentsorgung wird empfohlen, diesen Branchenstandard umzusetzen, da die Betreiber jederzeit in der Lage sein müssen, den Nachweis für einen sicheren Betrieb zu erbringen. Betreiber Kritischer Infrastrukturen sind sogar nach BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik = BSI-Gesetz = BSIG). dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse nach Stand der Technik zu treffen und dies auch gegenüber dem BSI durch Prüfungen oder Zertifizierungen aktiv nachzuweisen. Die Branchenverbände DWA und DVGW stellen dazu allen Betreibern (nicht KRITIS) von Anlagen der Trinkwasserver- und Abwasserentsorgung diesen praktischen Handlungsrahmen als Mindeststandard mit dem Merkblatt W 1060/M1060 und dem IT-Sicherheitsleitfaden zur Verfügung.

Branchenstandard gibt Orientierung

Dieser branchenspezifische Sicherheitsstandard beschreibt verbindliche Rahmenanforderungen, die eine Vorgehensweise zur Risikoanalyse und -behandlung enthält (***Bild 1***). Der Leitfaden beinhaltet eine Sammlung von Sicherheitsmaßnahmen zur Erreichung des im IT-Sicherheitsgesetz geforderten Stand der Technik für den Betrieb der ein-

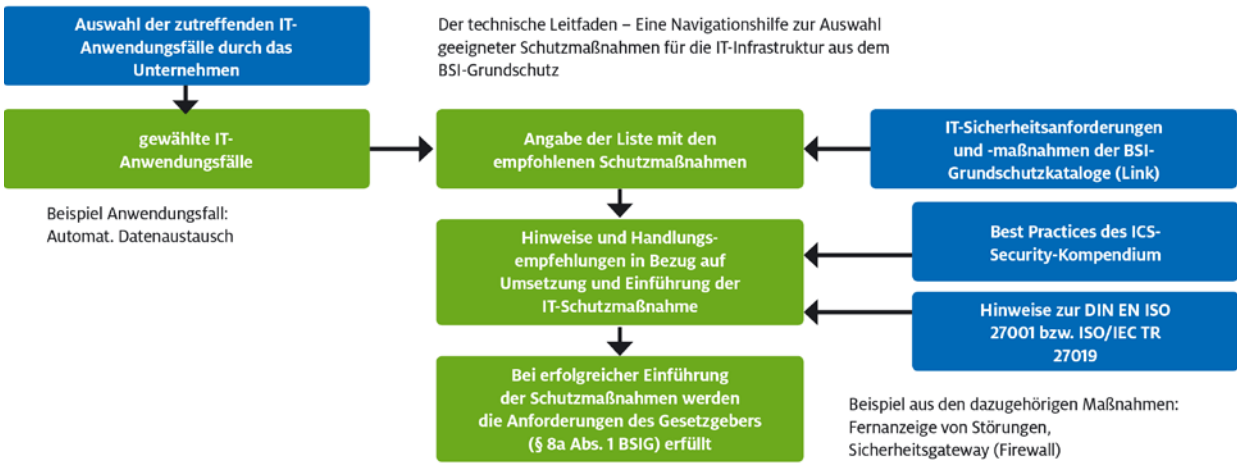

Bild 1: Systematik des Branchenstandards

Bild 2:Einsatz von IRMA in einem Leitstand

gesetzten IT-Systeme. Die darin beschriebenen Mindestvorgaben (A-Maßnahmen) sollten von allen Anlagenbetreibern umgesetzt werden – unabhängig davon, ob eine Anlage bereits heute eine Kritische Infrastruktur ist oder nicht. Ein großer Schritt in die richtige Richtung. Jedoch bleibt die Festlegung der betroffenen Anlagen (z. B. nach ihrer Größe) nicht unbedingt sinnvoll, da Cyberangriffe etc. in der Regel auf die Gesamtheit aller Anlagen abzielen. In dem Falle würde auch die Summe der potenziell betroffenen kleinen und mittleren Anlagen das Funktionieren der Ver- und Entsorgung, ja des Gemeinwesens, gefährden. Das bedeutet wiederum, dass sich nahezu jede Anlage um diese Thematik zu kümmern hat. Dabei sind Aussagen wie: „Uns betrifft das nicht" oder „Wir sind nicht im Internet, wir haben eine Insellösung" in keinem Fall ausreichend. Denn es reicht schon eine Fernwartung oder der direkte Zugriff über einen kompromittierten Laptop eines Dienstleisters, um Angreifern ein mögliches Einfallstor zu öffnen. Ein effektives Informationssicherheits-Managementsystems basiert immer auf den drei Säulen:

- Organisatorische Maßnahmen
- Technische Maßnahmen (wird nachfolgend beschrieben)
- Personelle Maßnahmen

IT-Sicherheit bequem und Rechtssicher managen

Damit scheint die Umsetzung des Sicherheitsstandards auf den ersten Blick jedoch etwas problematisch, da häufig die Budgets sowie die Fachkräfte fehlen, um ein durchgängiges Sicherheitsniveau und den im ITSiG geforderten Stand der Technik umzusetzen. An diesem Kernpunkt der methodischen Vorgaben, und seinem bereits vorhandenem Asset- und Risikomanagement hat das Softwareunternehmen Videc in der Produktweiterentwicklung für den Bereich IT-Sicherheit angesetzt. Herausgekommen ist dabei IRMA, Industrie Risiko Management Automatisierung (***Bild 2***). Mit einfach bedienbaren Werkzeugen können damit die grundlegend notwendigen Maßnahmen geplant, die Umsetzung unterstützt und dokumentiert werden.
Die DWA-/DVGW-Umsetzungshinweise (IT-Sicherheitsleitfaden und Merkblatt W 1060/M1060) beinhalten Handlungsempfehlungen u. a. für konkrete Anwendungsfälle, sogenannte Usecases, und Risikoermittlung für verschiedene Bedrohungen (*Nummerierung gemäß M/W 1060 Merkblatt):

1. Dokumentation der Assets (7.2*)

Zur Bestandsaufnahme zeigt IRMA automatisch alle (auch die nicht dokumentierten und unbekannten) Komponenten und Datenverbindungen auf.

2. Bestimmung der Anwendungsfälle (7.3*)

In IRMA erfolgt zunächst die Auswahl der relevanten Anlagentypen und die Zuordnung der Anwendungsfälle. Auf dieser Basis werden die korrespondierenden Gefährdungen automatisiert aufgelistet und können individuell ergänzt oder bei nicht-Relevanz abgewählt werden.

3. Risikoanalyse (7.4*)

Die Risikoanalyse erfolgt direkt in IRMA in Anlehnung an

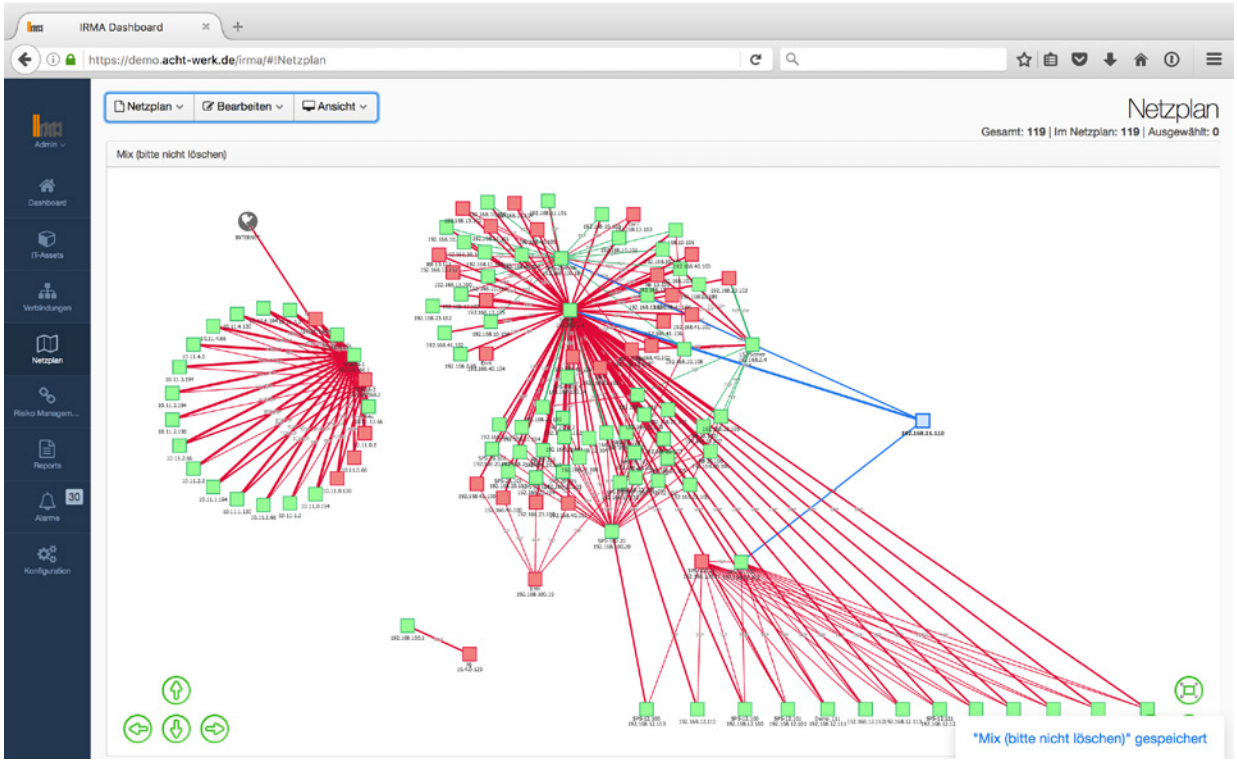

Bild 3: Netzplan in IRMA

ISO 27005 für die relevanten Gefährdungen in direktem Bezug auf die betroffenen IT-Assets.

4. Risikobewertung (7.5*)

In IRMA werden die Ermittlung der Werte für die Eintrittswahrscheinlichkeit und den Grad der Einschränkung des Anlagenbetriebs dokumentiert.

5. Festlegung der Maßnahmen (8.1*)

IRMA listet anhand der ausgewählten Anwendungsfälle automatisiert die im B3S festgelegten Maßnahmen des BSI-IT-Grundschutzes. Diese Maßnahmen werden nun den relevanten IT-Assets manuell zugeordnet. Damit erhält jeder IT-Asset Owner eine Liste der relevanten Maßnahmen und kann die Umsetzung strukturiert planen und dokumentieren. Der Umsetzungsgrad ist in IRMA durch die Verantwortlichen jederzeit überprüfbar.

6. Umsetzung der Maßnahmen (8.3*)

In IRMA wird die Umsetzung der festgelegten Maßnahmen geplant und nachverfolgbar dokumentiert.

7. Nachweis der Wirksamkeit und Dokumentation (8.4*)

Mit IRMA erstellen können alle notwendigen Reports zur nachweisbaren Dokumentation ohne Zusatzaufwand exportiert werden.

Diese Schritte sind nach den Vorgaben der DWA und DVGW im Produkt abgebildet. IRMA enthält bereits in der Basisversion immer die vier Kernfunktionen:

a) Die automatische Erkennung der Assets (Teilnehmer) im Netzwerk. Diese Funktion ist passiv, bedeutet, dass kein Teilnehmer aktiv angefragt wird. Ein wichtiger Aspekt, da viele alte Geräte auf solche Abfragen sehr sensibel reagieren und neue Teilnehmer ohne Gefährdung der Verfügbarkeit automatisch erkannt werden.

b) Das Risikomanagement unterstützt die Mitarbeiter (IT und Automatisierer) bei der Bewertung eines jeden Gerätes.

c) Die grafische Darstellung des gesamten Netzwerkes mit allen Querverbindungen in der Kommunikation, sowie die Auswertungen zu jedem einzelnen Teilnehmer (***Bild 3).***

d) Alarmierung automatisiert über direkte Verbindung (z. B. Potentialfreier Kontakt, SMTP) oder über ein Alarmierungssystem (z. B. AIP)

Für den Interessierten bietet Videc die Möglichkeit, einen Demo-Testlauf für eine Anlage zu bekommen. So können die zahlreichen Funktionen von IRMA einfach und sicher getestet werden (***Bild 4***). Nach kurzer Einrichtung des Systems kann der Anwender bereits die ersten Ergebnisse seiner Anlage im Rahmen eines Workshops sichten.

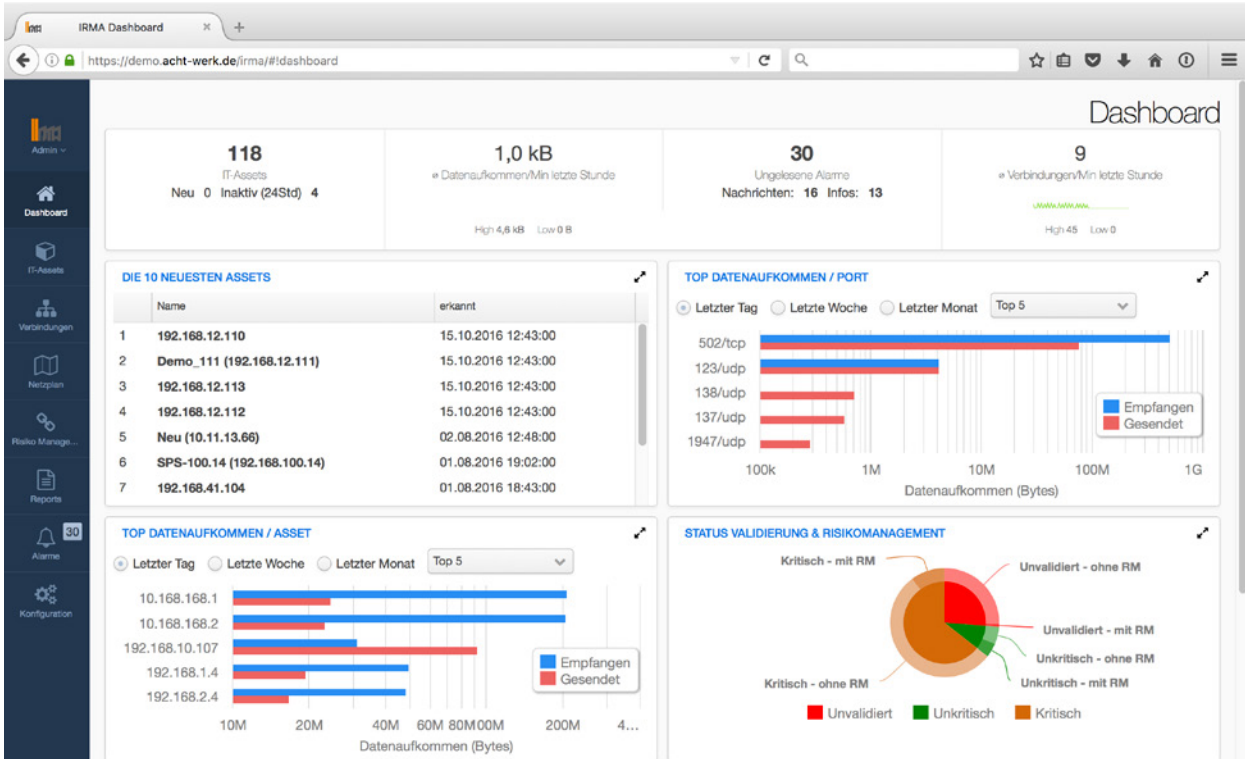

Bild 4: Funktionen. Netzplan. Dashboard

Bei sehr vielen dieser Testinstallationen offenbarten sich einige Überraschungen im Netzwerk. Offene Serviceschnittstellen oder sogar unbekannte Geräte im Netzwerk waren keine Seltenheit.

Ralph Bargmann Bereichsleitung IT, Organisation und IT Sicherheit StadtWerke Delmenhorst GmbH äußert sich zum Einsatz von IRMA wie folgt: „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.“

Alle Vorteile für den IT- und Betriebs-Verantwortlichen

- Zeitersparnis zur Aufnahme und Inventarisierung der IT-Assets ohne wesentliche Beratungsaufwände – betriebsbereit schon nach einer Stunde
- Wirtschaftliche Aufbereitung des geforderten Netzstrukturplanes durch automatisierte Erstellung im Analyseprozess: übersichtlich und jederzeit aktuell
- Integriertes Risikomanagement mit strukturierter und immer aktueller Auflistung der Risiken und festgelegten Maßnahmen je IT-Asset für den jeweiligen Anlagenverantwortlichen als Checkliste
- Erfüllen der ITSiG-Meldevorgaben: Erkennen von Sicherheitsvorfällen durch die kontinuierliche Beobachtung der IT-Infrastruktur. Die Alarmierung erfolgt automatisiert.
- Angriffserkennung und somit unmittelbare, direkte Handlungsfähigkeit für die Betriebsleitung, schnelle Ursachen und Datenerfassung für eine unkomplizierte Meldung und die kontinuierliche Aktualisierung aller Assets mit Netzplan in verschiedenen Sichten

AUTOR

DIETER BARELMANN
VIDEC GmbH
28203 Bremen
Tel.: +49 (0) 421-339500
info@videc.de