IT-Sicherheit für die Produktion

Risikomanagement und Früherkennung mit IRMA

Betreiber kritischer Infrastrukturen (KRITIS) müssen ab einer bestimmten Unternehmensgröße rechtliche Vorgaben erfüllen, beispielsweise zum Stand der Technik. Anhand des KRITIS-Sektors Wasser/Abwasser wird in diesem Artikel aufgezeigt, wie dafür nötige Maßnahmen umsetzbar sind.

Von Dieter Barelmann, VIDEC Data Engineering GmbH

Der Gesetzgeber hat mit dem IT Sicherheitsgesetz bereits im Jahr 2015 den rechtlichen Rahmen zur Erhöhung der IT-Sicherheit für die unterschiedlichen Branchen vorgegeben. Laut der Zeitschrift Wirtschaftswoche plant das Bundesinnenministerium (BMI) im Rahmen des sogenannten IT-Sicherheitsgesetzes 2.0 die Meldepflicht von Unternehmen bei Angriffen auf ihre IT-Infrastruktur Ende 2019 zu verschärfen. Beispielsweise soll die Meldepflicht für erhebliche IT-Sicherheitsvorfälle auf weitere Unternehmen, bis in den Mittelstand hinein, übertragen werden. Diese Pflicht gilt bereits aktuell für Betreiber kritischer Infrastrukturen, wie zum Beispiel im Energie-, Wasser- und Gesundheitssektor.

So 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. In der Wasser-Abwasser-Branche wurde daraufhin vom Deutschen Verein des Gas- und Wasserfaches (DVGW) und der Deutschen Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (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 eines sicheren Betriebs zu erbringen.

Denn Betreiber kritischer Infrastrukturen sind nach dem BSI-Gesetz dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse nach Stand der Technik zu treffen und das auch gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durch Prüfungen oder Zertifizierungen aktiv nachzuweisen.

Die Branchenverbände DWA und DVGW stellen dazu allen Betreibern (nicht nur den KRITIS-Unternehmen) von Anlagen der Trinkwasserver- und Abwasserentsorgung den praktischen Handlungsrahmen als Mindeststandard mit dem Merkblatt W 1060/M1060 und dem IT-Sicherheitsleitfaden zur Verfügung.

Branchenstandard

Der branchenspezifische Sicherheitsstandard beschreibt verbindliche Rahmenanforderungen, die eine Vorgehensweise zur Risikoanalyse und -behandlung enthält (siehe Abbildung 2). Der Leitfaden beinhaltet eine Sammlung von Sicherheitsmaßnahmen zur Erreichung des im IT-Sicherheitsgesetz geforderten Stands der Technik für den Betrieb der eingesetzten 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.

Das bedeutet wiederum, dass sich nahezu jeder Betreiber 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.

IRMA

Ein effektives Informationssicherheits-Managementsystem basiert immer auf den drei Säulen organisatorische, technische und personelle Maßnahmen. Damit scheint die Umsetzung des Sicher-

heitsstandards auf den ersten Blick jedoch problematisch, da häufig die Budgets sowie die Fachkräfte fehlen, um ein durchgängiges Sicherheitsniveau und den im IT-Sicherheitsgesetz geforderten Stand der Technik umzusetzen.

An diesem Punkt hat das Unternehmen VIDEC angesetzt: Die Security-Appliance „Industrie Risiko Management Automatisierung" (IRMA) ist ein Industrie-Computer-System, das kontinuierlich vernetzte Produktionsanlagen überwacht, Informationen zu Cyberangriffen liefert und die Analyse und intelligente Alarmierung mittels einer übersichtlichen Management-Konsole ermöglicht. Cyberangriffe oder Ausfälle sind sofort sichtbar und können detailliert untersucht werden. Zusätzlich bietet das Produkt eine erhebliche Unterstützung und somit Kosteneinsparung bei der Umsetzung von IT-Richtlinien.

B3S und IRMA

Der in IRMA integrierte „B3S-Wasser" entspricht dem praktischen Handlungsrahmen, der im Merkblatt W 1060/M 1060 und dem IT-Sicherheitsleitfaden zur Verfügung gestellt wird. Anhand der Auswahl und Behandlung der Anlagentypen, der Anwendungsfälle, dem Gefährdungs- und Maßnahmenkatalog lässt sich der Standard mit IRMA anwenden.

So werden durch die Auswahl der Anlagentypen (Kanalisation, Kläranlage, Leitzentrale, Trinkwassergewinnungsanlage, Wasserwerk, Trinkwasseraufbereitungsanlage oder Wasserverteilsysteme) die notwendigen Anwendungsfälle zur Risikoanalyse zur Verfügung gestellt. Die relevanten Bedrohungskategorien/Gefährdungen werden angezeigt und die jeweiligen Maßnahmen für die betroffenen Abteilungen Organisation, Personal, Hard- und Software sowie Notfallvorsorge behandelt. Das besondere ist, dass diese Maßnahmen direkt zu den passenden Systemen/Assets behandelt und dokumentiert werden. Der Umsetzungsstatus ist dabei jederzeit sichtbar. Wie im Standard gefordert, besteht hier auch die Möglichkeit, direkt einen zugehörigen Eintrag im Modul „Risiko Management" individuell zu erstellen.

IRMA enthält bereits in der Basisversion die vier Kernfunktionen:

_____ 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 dadurch automatisch erkannt werden.

_____ Das Risikomanagement unterstützt die Mitarbeiter (IT und Automatisierer) bei der Bewertung eines jeden Assets und ermöglicht die standardkonforme Dokumentation für das Security-Management.

_____ die grafische Darstellung des gesamten Netzwerkes mit allen Querverbindungen in der Kommunikation sowie die Auswertungen zu jedem einzelnen Teilnehmer.

_____ Alarmierung von Anomalien, Änderungen und somit möglichen Angriffen automatisiert über direkte Verbindung (z. B. potenzialfreier Kontakt, SMTP) oder über ein Alarmierungssystem (z. B. AIP).

IT- und Betriebsverantwortliche sparen mit der Appliance IRMA bei der Aufnahme und Inventarisierung der IT-Assets Zeit und haben wenig Beratungsaufwand. Auch hilft ein integrierter Netzplan dabei, eine schnelle Übersicht der Anlage zu gewährleisten. Weitere Vorteile von IRMA sind:

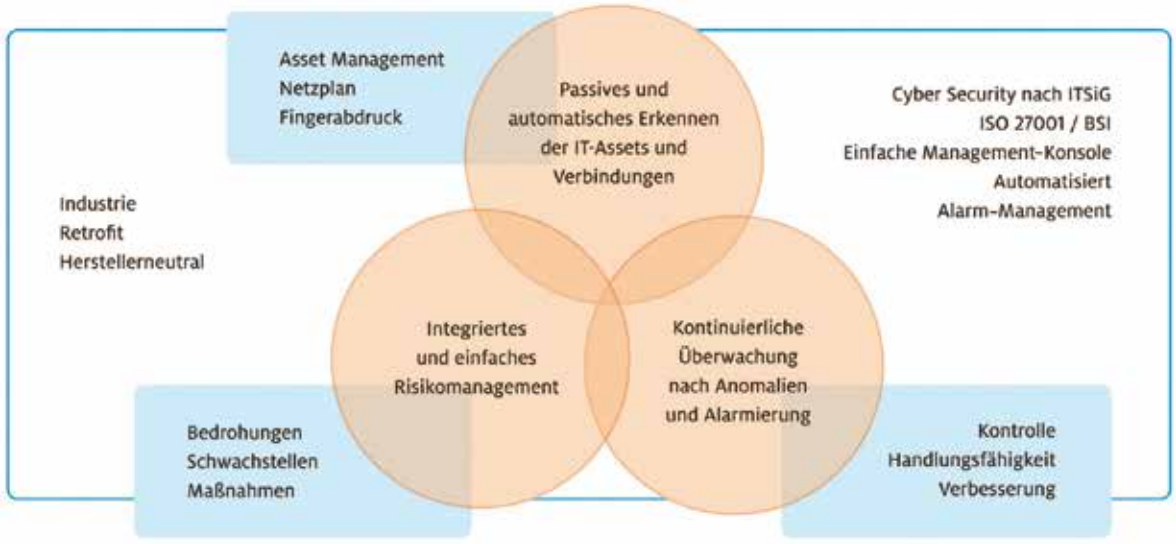

Abbildung 1: Aufbau von IRMA

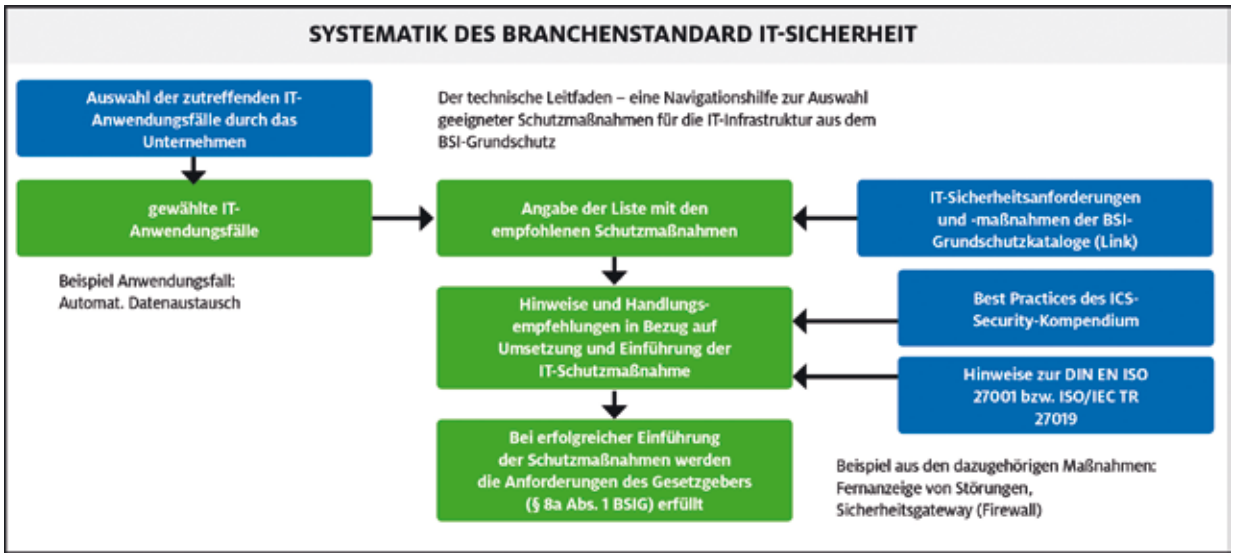

Abbildung 2: Systematik des Branchenstandards DVGW und DWA – M1060/W1060 (Bild: Deutscher Verein des Gas- und Wasserfaches e.V.)

_____ 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

_____ Kontinuierliche Aktualisierung aller Assets mit Netzplan in verschiedenen Sichten

Fazit

Der Schutz vor Cyber-Attacken, die Auswirkungen des IT-Sicherheitsgesetzes oder die unternehmerische Verantwortung für die Verfügbarkeit von echtzeitfähigen Produktionsanlagen (Automatisierungen) sind mehr denn je die aktuellen Anforderungen an die Betriebsleitung und Geschäftsführung. IRMA trägt dazu bei, die IT-Sicherheit in Unternehmen zu erhöhen und unterstützt bei der Umsetzung von Brachenstandards.

Für interessierte Unternehmen gibt es die Möglichkeit, einen Demo-Testlauf für ihre Anlage durchzuführen. Nach kurzer Einrichtung des Systems kann der Anwender bereits die ersten Ergebnisse seiner Anlage im Rahmen eines Workshops sichten. Bei sehr vielen dieser Testinstallationen offenbarten sich einige Überraschungen im Netzwerk. Offene Serviceschnittstellen oder sogar unbekannte Geräte im Netzwerk waren keine Seltenheit. ■

Messestand: Halle 9, Stand 9-506