Der IT-Sicherheits-leitfaden – aller Anfang ist leicht

Der Branchenstandard für die Wasser- und Abwasserwirtschaft wurde am 1. August 2017 als erster IT-Sicherheitsstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für einen KRITIS-Sektor anerkannt. Ab Ende August sollen ihn die Branchenverbände ihren Mitgliedern zur Verfügung stellen. Der branchenspezifische Sicherheitsstandard enthält verbindliche Rahmenanforderungen, die eine Vorgehensweise zur Risikoanalyse sowie eine Sammlung von Sicherheitsmaßnahmen enthalten, um den identifizierten Risiken zu begegnen.

Der erwartete IT-Sicherheitsleitfaden wird den Betreibern Kritischer Infrastrukturen einen praktischen Handlungsrahmen zur Erreichung des im IT-Sicherheitsgesetz geforderten Stand der Technik für den Betrieb der eingesetzten IT-Systeme geben.

Fünf Schritte des BSI-Grundschutzes

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

1. Infrastruktur-/Anlagenauswahl und -abgrenzung
Zunächst sind die relevanten Anlagen auf Basis der BSI-Kritis-Verordnung zu bestimmen und zuzuordnen.

2. Identifikation der relevanten IT-Systeme durch Inventarisierung der Werte (Assets)
Neben einem Inventarverzeichnis der vorhandenen IT-Systeme und -Komponenten sind auch die grundsätzlichen Zusammenhänge zwischen diesen zu dokumentieren.

3. Bestimmung und ggf. Ergänzung der Anwendungsfälle
Im IT-Sicherheitsleitfaden werden aktuell sechs Kategorien von Anwendungsfällen unterschieden, die entsprechend mit dem aktuellen Anlagenbestand auszuwählen sind.

4. 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.

5. 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.
Hierzu erklärt Arne Schönbohm, BSI-Präsident: „Als nationale Cyber-Sicherheitsbehörde treiben wir die Umsetzung des IT-Sicherheitsgesetzes erfolgreich voran. 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."

WannaCry, Petya & Co.: das war's noch nicht

Nach den jüngsten Cyber-Attacken wird derzeit die Angreifbarkeit der Automatisierungen in Produktionsanlagen und kritischen Infrastrukturen besonders intensiv in der Öffentlichkeit diskutiert. Für Hersteller, Dienstleister und Anwender stellen sich aber folgende Fragen: Wie hoch ist das Risiko für Industrieanlagen? Wie entwickeln sich die Bedrohungsszenarien durch Cyber-Angriffe weiter? Welche rechtlich notwendigen Sicherheitsmaßnahmen sind zu treffen?
Die Entwicklung von Angriffen beginnt in den 80er-Jahren zunächst recht unspektakulär und ohne große Schäden für die Endnutzer. Viren wurden zunächst über Disketten verbreitet. Mit der zunehmenden Vernetzung der Rechner etablierten sich auch die ersten Würmer. Die vormals von

Der Branchenstandard:	Das Was: Anforderungen und Ergebnisse im Branchenstandard	Das Wie Funktionale Anforderungen an ISMS-Werkzeuge zur organisatorischen und technischen Umsetzung
IT-Sicherheitsleitfaden (Branchenleitfaden)	Der IT-Sicherheitsleitfaden und das Merkblatt stellen zusammen das Regelwerk dar, das bei der Erfüllung nach Vorgaben des BSI-Gesetzes angewendet werden soll. Der Leitfaden beinhaltet die Kataloge zu den festgelegten Anwendungsfällen.	Inventarisierung: Aktuelle Übersicht aller IT-Assets und IC-Systeme (Asset-Register) sowie deren Kommunikationen (Netzstrukturplan) Auswahl der Anlagenkategorien (nach der BSI-Kritis-Verordnung) und Kennzeichnung aller relevanten Elemente Zuordnung der IT-Assets, Standorte und Abteilungen zu der Anlagenauswahl
IT-Sicherheitsleitfaden: Anwendungsfälle	Auswahl der relevanten Anwendungsfälle	Zuordnung der IT-Assets zu den Anwendungsfällen anhand der ausgewählten Anlagen.
IT-Sicherheitsleitfaden: Gefährdungen	Ableitung der Gefährdungen nach ISO27000, BSI-Grundschutz oder des BSI-ICS-Kompendium ggf. begründetes Streichen oder Hinzufügen von Gefährdungen	Auswahl der relevanten Gefährdungen für die Maßnahmenplanung und -umsetzung nach BSI-Grundschutzkatalog, aus dem „Best Practise“ des ICS-Security-Kompendium und den Hinweisen zur DIN EN ISO 27001 bzw. abgeleitet ISO/IEC TR27019.
IT-Sicherheitsleitfaden: Risikobewertung	Durchführen einer Risikoanalyse gem. IT-Sicherheitsleitfaden und in Anlehnung an ISO 27005	Beurteilung und Bewertung der Risiken: Abgrenzung zur allgemeinen Risikobetrachtung Risikoanalyse auf Basis der Gefährdungen Risikobewertung mit Priorisierung der zugrundeliegenden Gefährdungen Achtung: Notwendige Details zum Status von SCADA, Historian, HMI, Remote Access, SPS, PLC, OPC (Classic, UA) Fernwirktechnologien und weitere properitäre Technik sind zu berücksichtigen.
IT-Sicherheitsleitfaden: Maßnahmenermittlung	Risikobehandlung mit Maßnahmen ISO27000, BSI-Grundschutz und des BSI-ICS-Kompendium	Automatische Ableitung der Maßnahmen (Anwendungsfälle – IT-Assets) Ggf. Umsetzung eigener identifizierter Maßnahmen.
Merkblatt: Organisation	Merkblatt DVGW W1060 bzw. DWA 1060 (inhaltsgleich) Das Merkblatt ist die Grundlage des B3S W/a. Die Arbeit mit dem IT-Sicherheitsleitfaden setzt die Kenntnis des Merkblatts voraus. Im Merkblatt werden insbesondere die grundsätzlichen Schritte beschrieben, die zur Erfüllung der im BSI-Gesetz vorgegebenen Anforderungen notwendig sind.	Aktuelle Dokumentation, Reports, Berichte zu den Vorfällen Prozessbeschreibung und technische Unterstützung zur Aktualisierung und Erkennung von Änderungen, Abweichungen sowie möglichen Angriffen (Angriffserkennung nach ITSiG)
Handbuch zum Leitfaden: Zertifizierung	Beschreibt die Anwendung der im IT-Sicherheitsleitfaden bereitgestellten Kataloge und die empfohlene Vorgehensweise bei der Umsetzung.	Dokumentation und Maßnahmenplanung. Aktuelle Übersicht aller IT-Assets und IC-System (Asset-Register) sowie deren Kommunikationen (Netzstrukturplan) Maßnahmenplanung anhand der Gefährdungsanalyse zum Erreichen der Anforderungen als Nachweis zur Identifikation aller relevanten Maßnahmen.
Regularien und Nachweisführung gemäß §8a (3) BSIG	Sind ebenfalls Bestandteil des B3S W/A. Sie dienen der Konkretisierung, der in der Orientierungshilfe des BSI genannten Anforderungen in Bezug auf die Branche Wasser- und Abwasserwirtschaft.	Prozess zur Zertifizierung nach BSI-Vorgaben Erstellung der Nachweisdokumente zur kritischen Infrastruktur, der prüfenden Stelle, zur Prüfdurchführung sowie den Prüfergebnissen

sogenannten Script-Kiddies geschriebenen Schadprogramme entwickelten eine steigende Komplexität. Die ausgenutzten Schwachstellen z. B. in Office-Software durch Makro-Viren oder im Betriebssystem durch Trojaner wurden immer zahlreicher. Es beschäftigten sich immer mehr Informatiker und Ingenieure in Forschung, Entwicklung und staatlichen Sicherheitsinstitutionen mit der Ausnutzung von IT-Schwachstellen und natürlich auch mit deren Verhinderung.
IT-Sicherheit ist in den letzten Monaten vor dem Hintergrund neuer Cyberangriffe durch WannaCry, Petya und Co. noch stärker ins öffentliche Interesse gerückt. Hier 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. Dies ist ein eigentlich einfach zu verhindernder Angriff, da eine bekannte Schwachstelle (ETERNAL-BLUE) ausgenutzt wird. Ein Patchen, das heißt die Verwendung aktueller Software-Stände, hätte kein Eindringen zugelassen. Im Fall der Fälle hätte auch eine simple Maßnahme geholfen, die alle kennen: das Rückspielen einer aktuellen, sauberen Datensicherung.

Wurm → Virus/Trojaner → Ransom → APT

Aktuell stellen zielgerichtete Cyber-Angriffe (sog. Advanced Persistent Threats, APT) durch fortgeschrittene, gut organisierte und professionell ausgestattete Angreifer die höchste Gefährdung für Unternehmen dar. 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 (z. B. Cyber-Kriminalität oder Wirtschaftsspionage). An dieser Stelle seien zwei wesentliche Beispiele aus der aktuellen Praxis für Schadsoftware in der vernetzten Automatisierung und IT-Systeme für die Industrie genannt:

Stuxnet (2010)
Mit Stuxnet sind diese intelligenten Cyber-Angriffe in der Industrie angekommen. Diese gezielt entwickelte Schadsoftware für bestimmte Automatisierungen einer Branche findet fokussiert ihre Ziele. Dies erfolgt so intelligent, dass die eigene Verbreitung versteckt und Schäden erst viel später als Cyber-Angriff erkannt werden.

Industroyer (2017)
Seit Neuestem sind Industroyer im Fokus von Sicherheitsexperten. Diese missbrauchen keine Lücken in den ICS-Gerätschaften, sondern sprechen einfach in deren Sprache, indem sie die in Industrieumgebungen gängigen Kommunikationsprotokolle beherrschen. Dabei können Angreifer monatelang im Netzwerk aktiv sein und die 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.

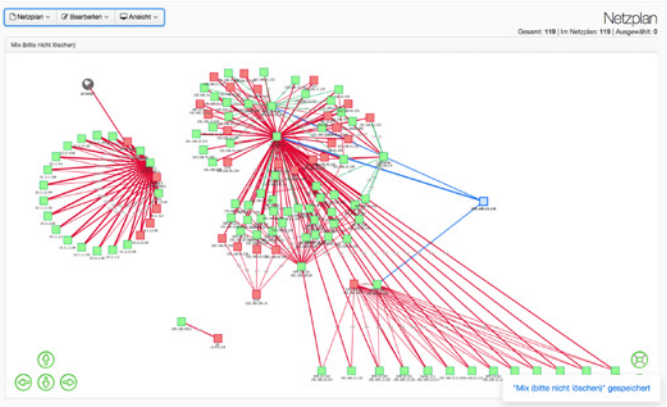
Übersicht zum ersten Branchenstandard Wasser / Abwasser

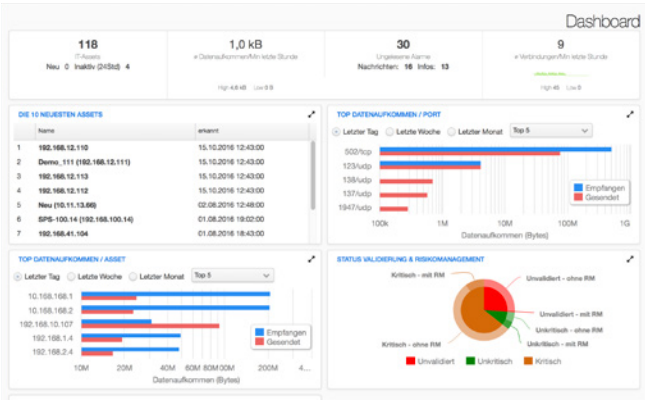
Der Branchenstandard in der Wasserwirtschaft ist kompatibel zu den ICS-Normen (internationaler Normenstandard), den Normen der ISO/IEC 27000-Reihe und dem BSI-Grundschutz.

IRMA - Ein Security-Produkt „Made in Germany“

Der Mehrwert und die Softfacts für eine Produktentscheidung

Neben den Diskussionen bezüglich Angriffen und Funktionen im Bereich Security gibt es einige weitere wichtige Aspekte, die in einer Gesamtbetrachtung nicht fehlen sollten.





Wenn sich jemand für eine Security Appliance entscheiden muss, stellt sich häufig die Frage nach der Herkunft. Sicherlich gibt es eine Reihe von Unternehmen, die nativ oder aus wirtschaftlicher Sicht den Stammsitz in den USA haben. Hier hat allerdings die Geschichte schon gezeigt, dass diese Lösungen nicht unbedingt in den entscheidenden Bereichen zum Einsatz kommen sollten. Die Konzeption und Entwicklung der Lösung IRMA der Firma Videc wurde bewusst in Deutschland entwickelt und dieser entscheidende Punkt „Security made in Germany" soll sich in Zukunft für einen deutschen Sicherheitsstandrad auch nicht ändern.

Zudem ist Videc auf das Thema Security für die Produktion und Versorgungsunternehmen spezialisiert. Die Basis dafür liegt in dem Know-how, das das Unternehmen seit 25 Jahren im Bereich Automatisierung in diesen Segmenten aufgebaut hat. Die sensiblen Strukturen der Automatisierung wurden von Beginn in den Grundkonzeptionen implementiert. Auf den Punkt gebracht bedeutet das für das Produkt IRMA das passive Scannen aller Assets im Netzwerk. Da in diesen Bereichen für Technologie und Personal andere Anforderungen vorliegen, hat Videc sich bei der Entwicklung des Produktes zusätzlich für eine sehr einfache Handhabung und für einen sehr geringen Pflegeaufwand entschieden – also easy to use. Dieser Aspekt trifft bei den meisten Security-Produkten nicht zu. Die Einarbeitung in das Produkt bedarf lediglich einer eintägigen Schulung - Grundkenntnisse im Bereich Security und Automatisierung vorausgesetzt.

Um die ersten und folgende Branchenstandards schnell und effizient zu erfüllen, sind folgende Funktionen entsprechend implementiert worden:

Inventarisierung

Damit startet in der Regel das Gesamtprojekt, denn: „Ich kann nicht schützen was ich nicht kenne". Durch das kontinuierliche Scannen des Netzwerkes lässt sich jedes Asset sofort erkennen, bestimmen und validieren. Damit sind alle Geräte jederzeit aktuell bekannt und lassen sich mit den wichtigen Informationen sofort in einem Report ausdrucken.

Aussagekräftige Reports

Einstellungen sowie Listen lassen sich einfach in Reports ausdrucken. Diese aktuellen Ist-Zustände werden häufig für Besprechungen oder aktuelle Maßnahmen benötigt. Die strukturierten Netzwerkdarstellungen lassen sich ebenfalls einfach integrieren

Risiken bewerten (integriertes Risikomanagement)

Jedes Asset lässt sich im integrierten Risikomanagement einfach bewerten. Entsprechend lassen sich notwendige Maßnahmen schnell und einfach sortieren und ausdrucken. Auswahlmöglichkeit der Anwendungsfälle und automatisierte Zuordnung der Gefährdungen und Maßnahmen innerhalb der integrierten Risikobewertung und -behandlung.

Überwachung des Netzwerkes

Jeder neue Teilnehmer wird unmittelbar erkannt. Servicemaßnahmen von externen Unternehmen lassen sich damit einfach kontrollieren, Assets ohne Befugnis unmittelbar auffinden. Zusätzlich bekommt man über die Filterkriterien eine schnelle Übersicht des Kommunikationsverhaltens. Eine Schnellübersicht erhält der User über den integrierten Netzplan, der unterschiedliche Einstellungen für diverse Sichten enthält.

Alarmierung bei Unregelmäßigkeiten

Eine der wichtigsten Funktionen ist die Alarmierung. Reagiert das Netzwerk außerhalb der validierten Einstellungen, kann IRMA unmittelbar eine Information an die zuständigen Mitarbeiter versenden.

Update- und Supportkonzept

Um das breit gefächerte Klientel optimal zu unterstützen, bietet das Unternehmen ergänzend zum Update-Service einen Support in unterschiedlichen Stufen (Level 1 bis 3) an. Dieses Konzept bietet Beratern, Systemhäusern wie auch Endkunden die optimale Unterstützung. Die notwendigen Schulungen – auch ohne Produkthintergrund – werden vom Unternehmen in regelmäßigen Abständen durchgeführt und sind auf eine lange und kontinuierliche Zusammenarbeit für eine zuverlässige Partnerschaft ausgerichtet.

Ab Mitte September ist das „Praxishandbuch IT Sicherheit - Leitfaden zum Branchen spezifischen Sicherheitsstandard der Wasserwirtschaft" kostenlos bei Videc erhältlich.

AUTOR

Dieter Barelmann
VIDEC GmbH
28203 Bremen
Tel.: +49 (0) 421-339500
DBarelmann@videc.de