05 | 2020

Jahrgang 161 | ISSN 0016-3651 | B 5399

Vulkan-Verlag
www.gwf-wasser.de

gwf Wasser + Abwasser

Fokus: Wasserorientierte Stadtplanung, Regenwasser-management

TITELSTORY

Cybersecurity für die Wasserwirtschaft: Schützen, was wichtig ist

INTERVIEW

mit Dr. Maike Beier über zukunftsfähige resiliente Städte

FACHBERICHTE

- Ökotoxizität von Bachsedimenten
- Bewertung von Handlungsoptionen zur Minimierung von Fehlanschlüssen

Cybersecurity für die Wasserwirtschaft: Schützen, was wichtig ist

Die Zahl der Angriffe auf Automatisierungs- und IT-Systeme steigt stetig. Anlagenplaner und -betreiber legen mittlerweile großen Wert auf den Schutz ihrer Systeme vor Manipulationen und Schadsoftware, auch in der Wasser- und Abwasserwirtschaft. Damit in industriellen Anwendungen die Anlagensicherheit jedoch nicht zu Lasten der Anlagenverfügbarkeit geht, braucht es geeignete Lösungen, mit denen Cybersecurity ein integraler Bestandteil von Anlagenplanung und Anlagenbetrieb wird und Sicherheitsmaßnahmen auf die jeweiligen Rahmenbedingungen zugeschnitten werden können.

Anbindung von Außenstationen mittels Fernwirktechnik – teilweise über öffentliche Kommunikationsnetze – IT-Schnittstellen zu Behördensysteme, Internettechnologien sowie der Einsatz mobiler Geräte: All diese Funktionen, einschließlich der umfassenden Vernetzung der Gewerke, helfen die Anlageneffizienz zu erhöhen sowie die Überwachung und Steuerung von Prozessen und Anlagen zu erleichtern. Daher sind Automatisierungssysteme mittlerweile stärker mit der IT-Landschaft vernetzt als es vielen Anlagenbetreibern auch und gerade in der Wasser- und Abwasserwirtschaft bewusst ist. Neben den Vorteilen, die dadurch erreicht werden, birgt die voranschreitende Vernetzung aber auch Risiken: Während früher proprietäre Netze vorherrschten, wachsen heute auf Basis moderner Standards wie Ethernet, TCP/IP und Mobilfunk die Büro- und Automatisierungswelt immer näher zusammen. Dadurch werden auch die Systeme in der Prozessleittechnik anfälliger für Angriffe von außen.

Angesichts dieser Entwicklungen hat der Gesetzgeber in vielen Ländern reagiert und fordert Anlagenbetreiber zum Handeln auf. So ist seit 2015 in Deutschland das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme“ in Kraft. Es verpflichtet Betreiber besonders gefährdeter Infrastrukturen – sogenannter kritischer Infrastrukturen, unter anderem aus den Bereichen Energie, Wasser, Gesundheit oder Telekommunikation –, ihre Netzwerke besser vor Hacker-Angriffen zu schützen. Für einige der darin erfassten kritischen Infrastrukturen – beispielsweise Kläranlagen mit mehr als 500.000 Einwohnerwerten oder Trinkwasserversorgung

Die Blaupausen sowie die entsprechende Dokumentation zur sicheren Konfiguration von Leitsystem und Kommunikation für die Erfordernisse der Branche Wasser/Abwasser/Entsalzung wurden im April 2020 erstmalig durch den TÜV-Süd nach IEC 62443-3-3 zertifiziert.

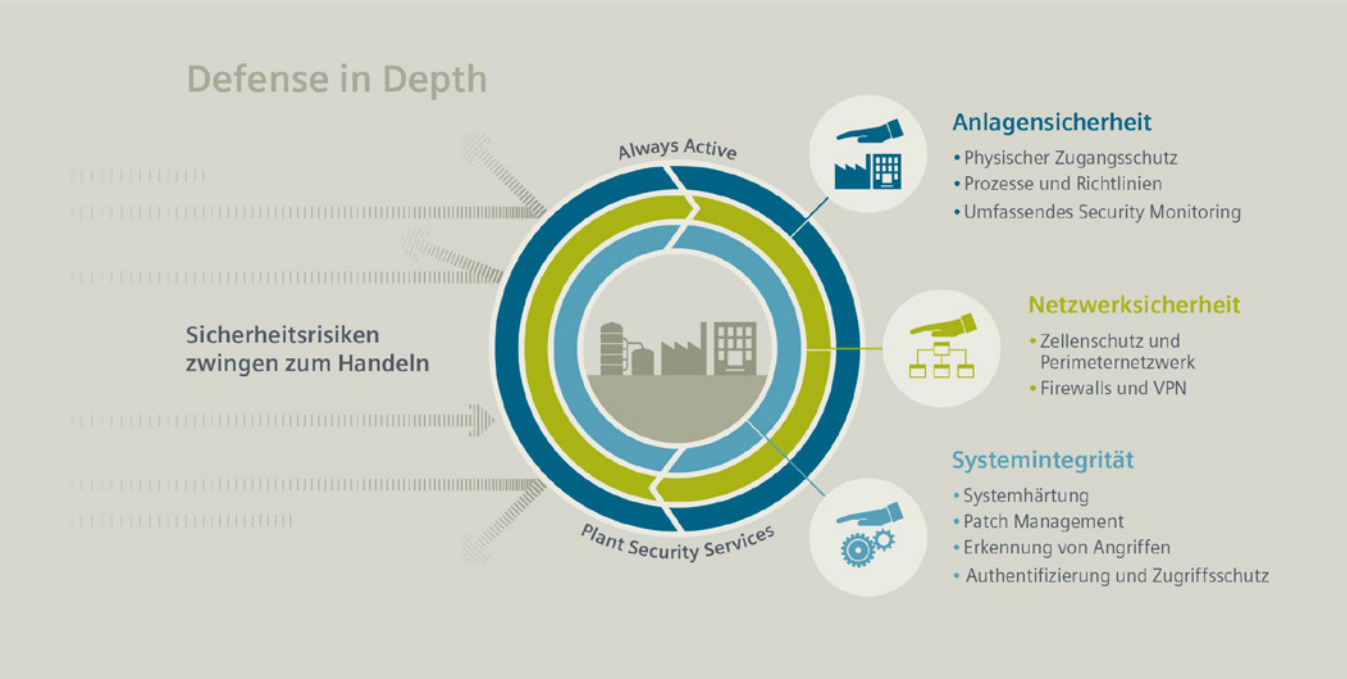
über 22 Mio. m^3/Jahr, jeweils einschließlich der Leitwarte – schreibt das Gesetz ab November 2016 eine Meldepflicht für sicherheitsrelevante Vorfälle sowie ab Mai 2017 Mindeststandards bei der Cybersecurity vor. Zusätzlich enthält der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) – basierend auf dem internationalen Standard ISO 27001 – einen Sicherheitsleitfaden für Anlagenbetreiber zur Konkretisierung der zuvor beschriebenen Umsetzungsvorgaben.

Bedrohungen ernst nehmen – und angemessen reagieren

Dass eine reale Bedrohung vorliegt, zeigen beispielsweise die Hackerangriffe auf Systeme zur Wasserversorgung in der Schweiz im November 2018, deren Ausgangspunkte in London und Korea lokalisiert werden konnten. Welche Auswirkungen eine Cyberattacke haben kann, zeigte sich im Mai 2017. Innerhalb nur weniger Tage infizierte der WannaCry Kryptowurm laut Expertenschätzungen mehr als 10.000 Organisationen und über 200.000 Rechner in 150 Ländern – und das, obwohl dank einiger günstiger Umstände der Angriff schnell eingedämmt werden konnte. Das eigentlich Bedenkliche an der Schadensbilanz von WannaCry war, dass die Schadsoftware Schwachstellen ausnutzte, für die es eigentlich bereits Patches gab. Offensichtlich waren diese nicht eingespielt, oder Unternehmen nutzten noch ältere Systeme, die nicht mehr gepatcht werden konnten. Dabei sollten zuverlässige und regelmäßige Backups, eine durchdachte Strategie für die industrielle Security – inklusive speziell geschützter Zonen für kritische Systeme – und das regelmäßige Patchen von IT- und Automatisierungskomponenten eigentlich selbstverständlich sein.

Warum sind dennoch Systeme in der Automatisierungs- und Leittechnik oft nicht so gut geschützt, wie es technisch möglich und notwendig wäre? Einige Antworten finden sich im Whitepaper „Cyber Security: Abwehr von Bedrohungen mit einem ganzheitlichen Sicherheitsansatz" der ARC Advisory Group von 2017. Hier werden als Barrieren für eine bessere Industrial Security unter anderem die teilweise Überalterung bei gleichzeitig zunehmender Offenheit der industriellen Automatisierungstechnik genannt. Daneben ist im Bereich des Managements sowie bei den Anwendern oft noch keine ausreichende Sensibilisierung vorhanden. Aber auch der vermehrte Einsatz von Off-the-Shelf Systemen für die IT, eine fehlende Ausbildung der Mitarbeiter sowie ein mangelndes Verständnis für den Lebenszyklus von Sicherheitssystemen erschweren einen besseren Schutz industrieller Systeme. Dies führt laut der ARC Group dazu, dass viele Unternehmen die Maßnahmen zur Planung und Implementierung von Industrial Security als zu komplex wahrnehmen. Und tatsächlich stellen die oft sehr speziellen Umgebungen bei Industrieanlagen eigene Anforderungen. Industrial Security Lösungen und Services müssen den Spagat zwischen auf den ersten Blick widersprüchlichen Anforderungen schaffen: Ein Produktionsnetz muss zu 100 % verfügbar sein, ein Not-Aus-Signal muss stets ohne Verzögerung ankommen, eine Sollwertvorgabe für einen kritischen Regler muss im Millisekundenbereich in bestimmten Laufzeiten verarbeitet werden. Regelmäßige Viren- und Security-Checks, jede Autorisierung und Authentifizierung eines Datentelegramms erhöhen die Systemlast aber unter Umständen so stark, dass die Echtzeitfähigkeit darunter leidet.

Daher bedarf es in Industrieanlagen wie Wasserwerken oder Kläranlagen spezieller Lösungen für die Cybersecurity, die sich



Tiefengestaffelte Verteidigung – „Defense in Depth" – als übergreifendes Schutzkonzept, nach den Empfehlungen der IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

von den in der IT etablierten Ansätzen deutlich unterscheiden. Gerade im Bereich kritischer Infrastrukturen hat die Systemverfügbarkeit – zum Beispiel für die Sicherstellung der Wasserversorgung – oberste Priorität. Einige Anbieter von Automatisierungssystemen haben auf diese Anforderung reagiert und bieten entsprechende Produkte und Services an. So unterstützt Siemens Betreiber von Anlagen in der Wasserwirtschaft mit einem umfangreichen Portfolio bei der Analyse des Sicherheitsstatus und dem Erstellen und Umsetzen eines Sicherheitskonzeptes. Das Industrial-Security-Konzept umfasst industrietaugliche Security-Produkte für Systemintegrität und Netzwerksicherheit. Hinzu kommen Services für die Analyse der Sicherheitslage sowie die Einrichtung und das Management von Security-Systemen, einschließlich eines Frühwarnsystems zur kontinuierlichen Überwachung von Industrieanlagen, zum Beispiel bezüglich Anomalien in der Netzwerkkommunikation. Darüber hinaus liefert das Unternehmen forensische Analysen der Vorfälle. Dadurch können Unternehmen ihrer Meldepflicht bei sicherheitsrelevanten Vorfällen gegenüber den Behörden nachkommen. Um Sicherheitsrisiken zu minimieren, setzt Siemens mit dem „Defense in Depth"-Konzept auf eine tiefengestaffelte Verteidigung, die von der Betriebs- bis zur Feldebene reicht. Das Konzept basiert auf drei Komponenten: Anlagensicherheit, Netzwerksicherheit sowie Systemintegrität nach den Empfehlungen der IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung, der auch von nationalen Behörden wie zum Beispiel dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für Hersteller von Produkten und Systemen empfohlen wird.

Zusätzlich entwickelt und verbessert Siemens laufend seine Produkte, Systeme und Lösungen hinsichtlich industrieller Sicherheit, inklusive der Zertifizierung gemäß IEC 62443. So hat es 2016 als erstes Unternehmen die TÜV SÜD Security-Zertifizierung nach IEC 62443-4-1 für den übergreifenden Entwicklungsprozess von Produkten der Automatisierungs- und Antriebstechnik, einschließlich der Industriesoftware, erhalten. Mittlerweile sind mehr als 30 Entwicklungsstandorte zertifiziert und damit alle für die Wasserwirtschaft relevanten Produktfamilien, wie zum Beispiel Scalance Kommunikation, Simatic Hardware sowie die Systeme WinCC und PCS 7 abgedeckt.
Im gleichen Jahr hat TÜV SÜD die im Prozessleitsystem Simatic PCS 7 implementierten Security-Funktionen sowie die Konformität von Entwicklungs- und Integrationsprozessen entsprechend IEC 62443-3-3 bzw. 62443-4-1 geprüft und bestätigt. Regelmäßige, wiederkehrende Audits – zuletzt im November 2019 – stellen sicher, dass Simatic PCS 7 die geforderten Standards weiterhin erfüllt. Damit ist beispielsweise die fortlaufende Analyse der Produkte und Systeme bezüglich sicherheitsrelevanter Kriterien gewährleistet und der kontinuierliche Test sowie die Auslieferung von Security-Patches sichergestellt; dies umfasst auch enthaltene Fremdkomponenten und -software.

Engineering für sichere Anlagen und Systeme

Für einen umfassenden Schutz von Anlagen sollten die Betreiber Sicherheitsaspekte bereits von der Systementwicklung bis in die Betriebsphase einer Lösung beachten. Die Reihe des führenden Standards für Industrial Security IEC 62443 definiert dabei fünf Lebenszyklusphasen: Produkt- oder Systementwicklung, Spezifikation, Integration und Inbetriebnahme, Be-

trieb und Instandhaltung und schließlich Stilllegung. Für jede dieser Phasen definieren die Standards klare Verantwortlichkeiten und Ziele, wobei die verschiedenen Sicherheitsaspekte zwischen den verschiedenen Partnern – Produktherstellern, Systemintegratoren und Anlagenbetreiber – koordiniert werden müssen. Defense in Depth, also der tiefengestaffelte Schutz eines Systems durch mehrere Sicherheitsebenen und -maßnahmen, bringt es mit sich, dass die Entwickler unterschiedliche und sehr verschiedene Security-Themen berücksichtigen müssen: von der Netzwerksicherheit über die Nutzerauthentifizierung bis hin zur sicheren Systemkonfiguration und der Härtung des Betriebssystems, inklusive entsprechender Logsysteme, Verschlüsselungstechnologien und sicherer Kommunikationskanäle. Für jedes dieser Themenfelder existieren zahlreiche Lösungsmöglichkeiten, Werkzeuge und Best Practices, aber oft mangelt es dem jeweiligen Projektteam schlicht an der Zeit oder auch am entsprechenden Fachwissen, die beste Option für die jeweilige Anwendung auszuwählen. Einer der häufigsten Fallstricke bei der Entwicklung einer Industrial-Security-Lösung ist es daher, sich auf einige Themen zu fokussieren und andere außer Acht zu lassen.

Um dem entgegenzuwirken und das Engineering von Industrial-Security-Lösungen zu unterstützen, hat Siemens mehrere Referenzlösungen (Blaupausen) für Automatisierungs- und Leitsysteme entwickelt. Diese erlauben einen sicheren Entwurf entsprechend des internationalen etablierten Standards IEC 62443. Wesentliche Grundlage bildet das nach IEC 62443-3-3 zertifizierte Prozessleitsystem Simatic PCS 7 und das Simatic Net-Portfolio, bestehend aus Switches, Routern und Firewalls.

Siemens hält seit November 2018 außerdem ein Zertifikat gemäß IEC 62443-2-4 zu den Security-relevanten Fähigkeiten, die Betreibern als Dienstleistungen im Zuge des Applikationsengineerings sowie der Integrations- und Instandhaltungstätigkeiten einer Automatisierungslösung angeboten werden können. Damit verfügen Projektteams über Referenzen zu relevanten Quellen und folgen einem entsprechenden Prozess, der sicherstellt, dass im Zuge des Engineerings alle Security-relevanten Dokumente fortlaufend gepflegt und sämtliche Methoden vollständig angewandt werden.

Darüber hinaus bietet das Unternehmen – als einer der erster System- und Lösungsanbieter überhaupt – erweiterte Blaupausen speziell für die Branche Wasser/Abwasser/Entsalzung, die beispielsweise Security-Komponenten und -maßnahmen zur verschlüsselten und somit sicheren Kommunikation per Fernwirktechnik über öffentliche Netze enthalten. Diese erweiterten Blaupausen sowie die entsprechende Dokumentation zur sicheren Konfiguration des Leitsystems wurden im April 2020 erstmalig nach IEC 62443-3-3 zertifiziert und stehen neben den Siemens-Projektteams auch externen Systemintegratoren zur Verfügung.

Damit unterstützt Siemens Integratoren und Partner bei Planung, Entwurf und Implementierung sowie Versorgungsunternehmen beim sicheren Anlagenbetrieb für die Wasser- und Abwasserwirtschaft.

Sicherheit beruht auf Erfahrung

Bei der Entwicklung der Blaupausen stand nicht zuletzt das Wissen Pate, das das Unternehmen im Laufe von zahlreichen Industrial-Security-Projekten in den vergangenen zehn Jahren gesammelt hat. Das Industrial-Security-Portfolio bündelt die Expertise der Security-Experten von Siemens in zertifizierten Produkten und Systemen und in einem reproduzierbaren Prozess, der ein reproduzierbares Ergebnis liefert. Der Anlagenbetreiber erhält ein sicheres System, das auf seine spezifischen Anforderungen abgestimmt ist und nach IEC 62443 zertifiziert werden kann. Im Anlagenbetrieb unterstützen ihn die Security-Dokumente bei der Pflege der Lösung – und er kann zusätzlich Support durch die Security-Experten bei Siemens erhalten. Da sich Bedrohungsszenarien ständig verändern, darf der Schutz einer Prozessanlage vor externen Angriffen und unbefugten Zugriffen keine einmalige Maßnahme sein, sondern muss als fortlaufender Prozess verstanden werden. Daher bietet Siemens neben Security Produktlinien auch Industrial Security Services. Diese reichen von Analysen der Sicherheitslage (Security Assessment) über die Einrichtung von Schutzmaßnahmen wie Firewalls oder Virenschutzprogrammen (Security Implementation) bis hin zur kontinuierlichen Überwachung von Anlagen mit den Manage Security Portfolio. Diese Security Assessments – also das ISO 27001 und auch das Assessment gemäß IEC 62443-2-1 – decken hierbei die B3S WA Anforderungen zu ISO 27001 und ISMS ab. Stellen die Siemens-Experten ein erhöhtes Risiko fest, warnen sie Kunden und geben Empfehlungen für proaktive Gegenmaßnahmen. Zusätzlich überwacht bei Siemens ein eigenes Netzwerk aus Security-Spezialisten und speziell geschulten Automatisierungs- und IT-Experten laufend aktuelle und neue Bedrohungen, analysiert Produkte und Systeme fortlaufend auf mögliche Schwachstellen und implementiert proaktiv Gegenmaßnahmen, damit Prozessleitsysteme und Automatisierungslösungen auch in Zukunft optimal gegen Angriffe geschützt sind.

Autor:
Thomas Stör
Siemens AG
thomas.stoer@siemens.com
www.siemens.de/wasser