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.

Fernüberwachung von Außenbauwerken, Zugriff auf Anlagendaten über das Internet und mobile Geräte: All diese Funktionen und die umfassende Vernetzung von Maschinen und Prozessen helfen, die Anlageneffizienz zu erhöhen, 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 und TCP/IP Büro- und Automatisierungswelt immer näher zusammen. Dadurch werden auch die Systeme in der Prozessleittechnik anfälliger für Angriffe von außen.

Angesichts dieser Entwicklungen hat auch 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, so genannter 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, schreibt das Gesetz seit November 2016 eine Meldepflicht für sicherheitsrelevante Vorfälle sowie seit Mai 2017 Mindeststandards bei der Cybersecurity vor. Zusätzlich enthält der branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) einen Sicherheitsleitfaden zur Konkretisierung der zuvor beschriebenen Umsetzungsvorgaben. Dieser Sicherheitsleitfaden basiert auf dem internationalen Standard ISO 27001 und der Etablierung eines Informationssicherheitsmanagements.

Bedrohungen ernst nehmen – und angemessen reagieren

Welche Auswirkungen eine Cyberattacke haben kann, zeigte sich zum Beispiel 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 dies, obwohl dank einiger günstiger Umstände der Angriff schnell eingedämmt werden konnte. Das 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 trotzdem Systeme in der Automatisierungs- und Leittechnik oft nicht so gut geschützt, wie es technisch möglich 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 zunehmende Offenheit der industriellen Automatisierungstechnik genannt. Daneben ist oft im Bereich des Managements und bei den Anwendern noch keine ausreichende Sensibilisierung vorhanden. Aber auch der vermehrte Einsatz von Off-the-Shelf Systemen für die IT und 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 Unternehmen 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 Prozent 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. 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. Darüber hinaus liefert Siemens 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 ISA 99/IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

Zusätzlich verbessert Siemens laufend seine Produkte und Lösungen hinsichtlich industrieller Sicherheit,

Bild 1: Siemens hat als erstes Unternehmen eine auf IEC 62443-4-1 basierende TÜV SÜD-Zertifizierung für den übergreifenden Entwicklungsprozess von Siemens-Produkten der Automatisierungs- und Antriebstechnik, einschließlich der Industriesoftware, erhalten.

inklusive der Zertifizierung gemäß IEC 62443. So hat Siemens 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 (***Bild 1***). Mittlerweile sind 25 Entwicklungsstandorte zertifiziert. Im gleichen Jahr hat TÜV SÜD die im Prozessleitsystem Simatic PCS 7 implementierten Security-Funktionen und die Konformität von Entwicklungs- und Integrationsprozessen geprüft und bestätigt. Regelmäßige, wiederkehrende Audits stellen sicher, dass Simatic PCS 7 die geforderten Standards erfüllt.

Engineering für sichere Anlagen und Systeme

Für einen umfassenden Schutz von Anlagen sollten die Betreiber Sicherheitsaspekte bereits von der Systementwicklung an bis hin zum Austausch einer Lösung beachten. Die Reihe des führenden Standards für Industrial Security IEC 62443 definiert dabei fünf Lebenszyklusphasen: Produkt- oder Systementwicklung, Spezifikation, Integration und Inbetriebnahme, Betrieb und Instandhaltung und schließlich Stilllegung. Für jede dieser Phasen definieren die Standards klare Verantwortlichkeiten und Ziele, wobei die verschiedenen Sicherheitsaspekte zwischen den verschiedenen Projektpartnern 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 Kanäle (***Bild 2***). 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 entgegen zu wirken und das Engineering von Industrial-Security-Lösungen zu unterstützen, hat Siemens mehrere Standardlösungen (Blaupausen) für Automatisierungs- und Leitsysteme entwickelt. Die Blaupausen sind vom TÜV gemäß IEC 62443 zertifiziert und unterstützen Projektteams mit Referenzen zu relevanten Quellen sowie einem entsprechenden Prozess, der sicherstellt, dass im Zuge des Engineerings alle Security-Dokumente erstellt werden, die der IEC 62443-2-4 Standard fordert. Basis dieser Blaupausen ist eine IEC 62443-3-3 zertifizierte Standardarchitektur für ein Leitsystem auf Basis von Simatic PCS 7 (Bild 1). Für die Branche Wasser/Abwasser ist darauf aufbauend eine entsprechend angepasste Standardlösung in Entwicklung. Diese Blaupause wird auch externen Systemintegratoren zur Verfügung stehen.

Sicherheit beruht auf Erfahrung

Bei der Entwicklung der Blaupausen stand nicht zuletzt das Wissen Pate, das Siemens 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

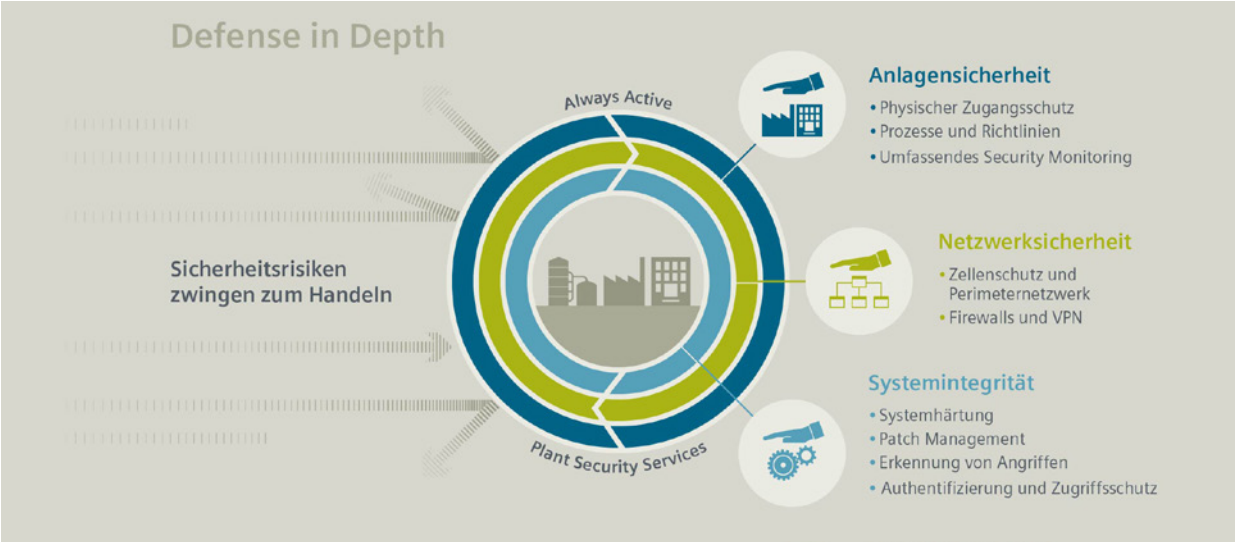

Bild 2: Tiefengestaffelte Verteidigung – „Defense in Depth" – als übergreifendes Schutzkonzept, nach den Empfehlungen der ISA99 / IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

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 Systeme auf mögliche Schwachstellen hin und entwickelt passende Gegenmaßnahmen, damit die Prozessleitsysteme und Automatisierungslösungen auch in Zukunft optimal gegen Angriffe geschützt sind.

AUTOR

JOCHEN CHRIST
Project Manager
Siemens AG
80333 München
Tel.: +49 1722343573
jochen.christ@siemens.com