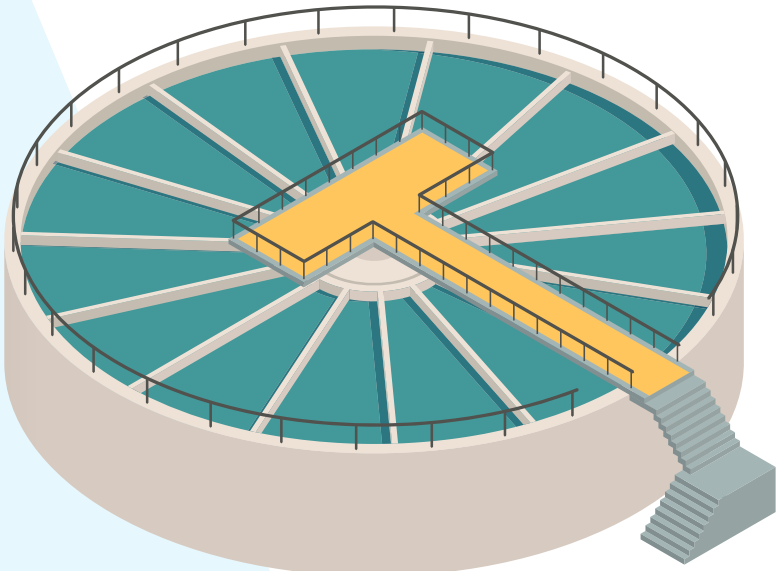
STORMSHIELD

Cybersicherheit in sensiblen Umgebungen:

Eintauchen in die Wasser-wirtschaft

Whitepaper



Drei Tage ...

so lange kann ein Mensch ohne Trinkwasser überleben. Ein Beleg dafür, wie wichtig diese Ressource ist.



Aber auch für landwirtschaftliche und industrielle Aktivitäten sowie für klassische Haushalte wird Wasser benötigt. Wie lange könnten Unternehmen weiterarbeiten, wenn ihnen die Wasserversorgung abgedreht würde? Diese Frage wird vor allem im Kontext der globalen Erwärmung immer dringlicher.

Es liegt in der Verantwortung der Wasserversorger – der lokalen Behörden und der privaten Unternehmen im Rahmen des öffentlichen Dienstleistungsauftrags –, dass es gar nicht erst dazu kommt. Sie tragen damit eine doppelte Verantwortung gegenüber der Bevölkerung und der Umwelt. Einerseits müssen sie die Kontinuität der Trinkwasserversorgung gewährleisten und zugleich Gesundheitsrisiken verhindern. Andererseits liegt es in ihrer Verantwortung, sich um Abwasser zu kümmern und dabei Umweltverschmutzungen zu vermeiden.

In Frankreich beispielsweise ist der Sektor sensibel genug, um vom für Ökologie zuständigen Ministerium koordiniert und täglich von einem Sektorkoordinator von ANSSI überwacht zu werden.

Dieses dichte industrielle Ökosystem, das aus Trinkwassergewinnungsanlagen und Kläranlagen besteht, von denen einige auf europäischer Ebene als Essential Service Operators (ESO) eingestuft werden, ist jedoch auf alternde Infrastrukturen und Technologien angewiesen, die es anfällig machen. Darüber hinaus sind diese Betriebssysteme heute einem viel stärkeren Cyberrisiko ausgesetzt, da sie unter dem Einfluss der Digitalisierung der Branche und des Aufkommens neuer Technologien zunehmend mit dem Computernetzwerk verbunden sind.

Dieses Phänomen der IT/OT-Konvergenz spiegelt sich in der Implementierung von Ethernet IP auch in Fabriken oder in der Entwicklung von Cloud-Lösungen für die Industrieüberwachung wider. Dabei handelt es sich zugleich um eine attraktive Angriffsfläche ist für Cyberangreifer, die mit traditionellen IT-Technologien oft besser vertraut sind als mit spezifischen Industrieprotokollen.

Darüber hinaus haben sich in den letzten Jahren, ob in den USA oder in Israel, Beispiele für Cyberangriffe gegen Wasserversorger vervielfacht. Auf der ganzen Welt werden sich Unternehmen der Wasserwirtschaft, staatliche

Einrichtungen und Verteidigungsorganisationen zunehmend der Notwendigkeit bewusst, die Cybersicherheit ihrer kritischen Infrastruktur, sensiblen Daten und Betriebsumgebungen zu gewährleisten. Dieses erhöhte Cyberrisiko spiegelt auch die Fragilität eines Sektors wider, der Opfer von Unterfinanzierung geworden ist. In Europa wie auch auf der anderen Seite des Atlantiks werden Wasserinfrastrukturen daher meist von kleinen Organisationen verwaltet und erwirtschaften geringe Margen.

Ihre industriellen Anlagen, die sich viel langsamer amortisieren als ein Büronetzwerk, sind oft mit SPS der alten Generation ausgestattet, was ihre Anfälligkeit erhöht. Und da sich die Investition in Cyberausrüstung direkt auf den Preis pro Liter Wasser auswirkt, müssen diese Organisationen auch die Kosten unter Kontrolle halten, um den Zugang für die Bevölkerung aufrechtzuerhalten.

Aufgrund mangelnder Ressourcen und thematischer Unkenntnis haben sich die Betreiber von Wassernetzen lange Zeit auf den Schutz der Gesundheit der Bevölkerung konzentriert und die ihrer Informationssysteme zurückgestellt.–

Ziel dieses Whitepapers ist es daher, IT-Managern und dem gesamten Systemumfeld von Subunternehmern (Integratoren und Herstellern) der Branche zu ermöglichen, in den neuesten Stand der Technik rund um das Thema Cybersicherheit der Wasserwirtschaft einzutauchen.

Zu diesem Zweck werden wir auf den folgenden Seiten die Probleme in diesem Sektor beleuchten und mögliche Lösungen vorschlagen.

Inhalt

Zahlen zum Merken

• **Infografiken –** Kartografie der Welt des Wassers

TEIL I.
Warum sollte die Wasserwirtschaft das Cyberthema ernst nehmen?

TEIL II.
Auf dem Weg zu (Cyber-) Kriegen um Wasser?

• **Kundeninterview Nr. 1 –** Standpunkt: Cybersicherheit, ein Reflex, der in der Wasserwirtschaft zu Leben erwacht

TEIL III.
Was sind die konkreten Cybersicherheitsprobleme in der Wasserwirtschaft?

• **Infografiken –** Die wichtigsten Schwachstellen des Sektors

TEIL IV.
Welche Cybervorschriften gelten für die Wasserwirtschaft?

TEIL V.
Und was ist mit morgen?

• **Kundeninterview Nr. 2 –** Ein verteiltes Netzwerk sichern

Zahlen
zum Merken

33.200

Wasserentnahmestrukturen, die in Frankreich erfasst sind (FP2E, 2019). Um Verschmutzungen zu vermeiden, sehen die Wassergesetze von 1992 und 2006 drei Wassereinzugsgebiete (unmittelbare, nahe und entfernte) sowie ein System zur Vermeidung diffuser Verschmutzungen in diesen Wassereinzugsgebieten vor. Derzeit keine Erwähnung von Cybersicherheit.

40 bis

Dies ist die **Leckrate** der Wasserverteilungsnetze in den Städten New York, London und Rom (im Vergleich zu durchschnittlich 20 bis 25 % anderswo – laut Les Échos Investir, 2021). All dies sind Lücken, die durch Fernmanagement und vorausschauende Wartung geschlossen werden sollen.

400

Bewohner aus Chatsworth (North Georgia, USA) konnten 2013 mehrere Tage lang kein Leitungswasser verwenden. Der Grund: ein Eingriff in das Überwachungssystem einer Trinkwasserinstallation in der Stadt und eine Änderung der Einstellungen der Fluor- und Chlorwerte.

46

Die Anzahl der erfolglosen Versuche im Jahr 2000, in die Informationssysteme einer australischen Kläranlage einzudringen. Unglücklicherweise gelang es dem ehemaligen technischen Zulieferer der Anlage beim 47. Versuch, die Kontrolle über die Anlage zu übernehmen und das Abwasser in einen See zu leiten.

3

Die Zahl der Cyberkrisen im Zusammenhang mit Wasser, die allein Israel im Jahr 2020 erlitt. Zwischen April und Dezember betrafen Cyberangriffe Pump- und Wasseraufbereitungsstationen, Wasserpumpen und einen Recyclingwassertank.

Mehr als 3 von 5 Schwachstellen

in industriellen Informationssystemen können zur völligen Nichtverfügbarkeit des Produktionsmittels führen, wenn sie richtig genutzt werden. Und 72 % davon können aus der Ferne ausgenutzt werden. *(Claroty, 2020).*

52 %

der Weltbevölkerung werden bis 2050 unter Wasserstress zu leiden haben (Vereinte Nationen, 2019). Dadurch werden die bereits bestehenden strategischen Probleme im Zusammenhang mit dieser Ressource noch verstärkt.

x2

Betriebliche Systeme in der Wasserwirtschaft sind mehr als doppelt so anfällig wie im Gesundheitssektor *(Claroty, 2020)*.

Infografik

Kartografie der Welt des Wassers

Der Wasserkreislauf ist alles andere als reibungslos, von der Entnahme über die Nutzung und Aufbereitung bis hin zum Transport. Tauchen Sie ein in eine unvollständige Liste von Akteuren der Wasserwirtschaft.

Das Trinkwassernetz

Rohwasserentnahme
(Grundwasser, Gewässer, Flüsse)

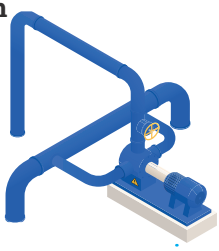




Trinkwasseraufbereitung
(Trinkwassergewinnungsanlagen, Entsalzungsanlagen)

Speicherung von Trinkwasser
(hauptsächlich Wassertürme)





Vertrieb
über ein Netz von Rohrleitungen

Orte des Verbrauchs oder der Nutzung

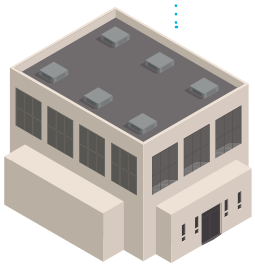
Wohnhäuser, Geschäfte und Unternehmen



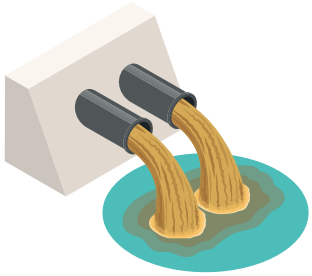


Bauernhöfe und Viehzuchtbetriebe

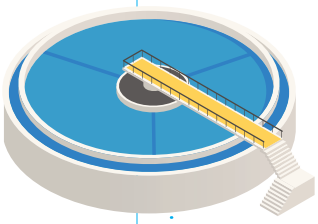
Die Industrien



Das Netz zur Aufbereitung des Abwassers

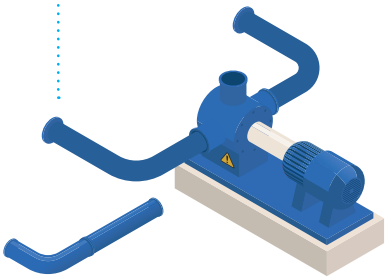


Sammlung:
Kanalisation für Haushaltsabwässer



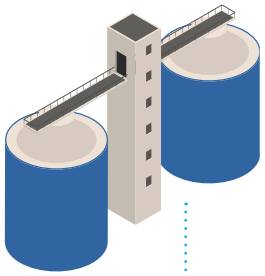
Aufbereitung:
Wasseraufbereitungs-anlagen

Kläranlagen oder kommunale Wasseraufbereitungsanlagen mit Klärteichen

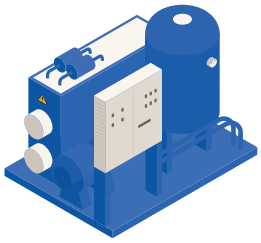


Abwasser:
Ableitungssysteme für gereinigtes Wasser

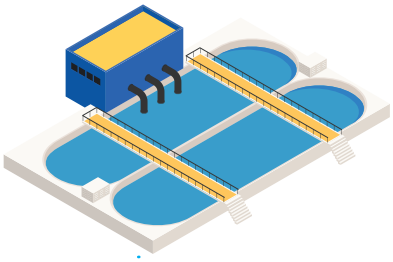
Das Regen-wassernetz



Pumpstationen für den Hochwasserschutz

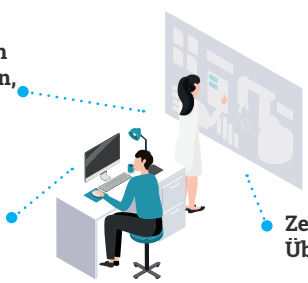


Pumpstationen für Straßenwasser



Rückhaltebecken

Innerhalb verschiedener Intrastrukturen mischen Informationssysteme oft eine Vielzahl verschiedener Elemente. All diese Elemente stellen eine erhebliche Angriffsfläche für Cyberangriffe dar.



Anlagevermögen (Arbeitsstationen, Server usw.)

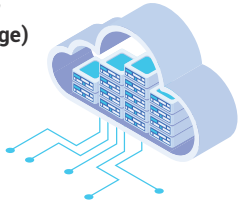
Nomadische Stationen

Zentrale Überwachungsstation



Systeme zur Fernsteuerung

Kommunizierende Sensoren für das IIoT (Internet der industriellen Dinge)



Cloud-Umgebungen

Warum sollte die Wasserwirtschaft das Thema „Cybersicherheit“ ernst nehmen?

Teil I.

Zwischen öffentlicher Gesundheit, Umweltverschmutzung und Geopolitik sind Fragen der Cybersicherheit im Wassersektor besonders kritisch. Doch trotz der vielfältigen Risiken, die insbesondere durch die Veralterung der Netze verursacht werden, tut sich die Branche schwer, digitale Sicherheitsreflexe zu entwickeln.



Zwei Haupttypen von Akteuren betreiben die Wasserinfrastruktur: lokale Behörden und beauftragte private Unternehmen. Daher ist es schwierig, ein einheitliches Bild der Berücksichtigung dieser Themen zu zeichnen, insbesondere der Investitionen in die Cybersicherheit. Ein zentraler Punkt jedoch, wenn mehr als 3 von 5 Schwachstellen im industriellen Informationssystem bei richtiger Ausnutzung zur vollständigen Nichtverfügbarkeit des Produktionswerkzeugs führen können (Quelle: Claroty-Bericht 2020).

Zu wenig aktualisiert und in die Jahre gekommen, weisen die operativen Systeme der Wasserwirtschaft mehr als doppelt so hohe Anfälligkeiten im Vergleich zum Gesundheitssektor auf (laut demselben Bericht von Claroty).

Doch nur wenige Wasserversorger kommunizieren offen über die Cyberangriffe, die sie vereiteln oder denen sie zum Opfer fallen. Im Gegensatz zu anderen Branchen wie dem Transport- oder Energiesektor beginnt der Wassersektor gerade erst, sich zusammenzuschließen, um diese Fragen der Cybersicherheit zu diskutieren. Nichtsdestotrotz können wir die Überwachungsarbeit des seit 2002 aktiven ISAC-Netzwerks Water in den USA oder der Scientific and Technical Association for Water and the Environment (ASTEE) in Frankreich anführen, die 2021 eine Arbeitsgruppe für Cybersicherheit initiiert hat.

Dennoch ist der Sektor nicht immun, wie uns der Fall einer Wasserversorgung in Florida im Februar 2021 vor Augen führte. Der aufsehenerregende vereitelte Cyberangriff in der Kleinstadt Oldsmar zeigt die mangelnde Sicherheit einer Reihe von Wasserinfrastrukturen: Der Cyberkriminelle konnte einen unzureichend gesicherten Zugangspunkt (TeamViewer) ausnutzen und die Natriumhydroxid-Einstellungen zur Regulierung des pH-Werts im Wasseraufbereitungsnetz

> ***In einer zunehmend vernetzten Welt, die durch die COVID-19-Epidemie zu raschen Veränderungen gezwungen ist, kann ein Cybersicherheitsproblem schnell zu einem Sicherheitsproblem werden und in einigen Extremfällen sogar die nationale Sicherheit bedrohen“***
>
> **Khobeib Ben Boubaker**
> Head of Industrial Security Business Line bei Stormshield

ändern. Zum Glück für die 15.000 Einwohner von Oldsmar entdeckte ein Stationsbeamter schnell die Anomalie (11.100 Teile pro Million statt 100) und korrigierte die Konzentration. Die in diesen Umgebungen eingebauten Sicherheitsvorkehrungen können zwar als Schutz dienen, aber die Geschichte der Cyberangriffe auf die Welt des Wassers zeigt uns, dass Cyberkriminelle wissen, wie sie diese umgehen können.

Obwohl historisch und kulturell bedingt **die persönliche Sicherheit immer Vorrang vor der IT-Sicherheit** im Wassersektor hatte, verschmelzen die beiden Themen heute zunehmend. **Die Besonderheit der Cyberbedrohung in der Welt des Wassers** liegt in den Beweggründen der Cyberangreifer. Dieser sensible Bereich ist nicht sehr lukrativ und wird nur selten zur Gewinnerzielung genutzt. Sie kann jedoch für öffentlichkeitswirksame Aktionen missbraucht werden, wie ein Beispiel im Januar 2021 in Kalifornien zeigte: Einem Cyberkriminellen gelang es, einige der Programme zu löschen, die von einer Anlage zur Trinkwasseraufbereitung in der San Francisco Bay Area verwendet wurden.

Der Angriff auf die Wasserinfrastruktur einer Region bleibt aber vor allem ein wichtiges Instrument zur realen Destabilisierung, das für politische Zwecke genutzt werden kann, wie wir im nächsten Abschnitt sehen werden.–

Auf dem Weg zu (Cyber-) Kriegen um Wasser?

Teil II.

Als lebenswichtige Ressource nimmt Wasser in den internationalen Beziehungen seit jeher einen strategischen Platz ein. Diese geopolitische Dimension wird durch den Klimawandel verstärkt, der das blaue Gold zu einer immer kostbareren Ressource macht.



In einer Zeit, in der Wasserversorgungs- und -aufbereitungsanlagen meist mit anderen Netzwerken, diesmal Computern, verbunden sind, nimmt ihre Anfälligkeit zu. In Europa erklärt dies, warum bestimmte Infrastrukturen des Sektors den Status von Essential Service Operators (ESO) haben und regulatorischen Empfehlungen entsprechen müssen. In Frankreich beispielsweise wird dieser Status durch den Status „Betreiber von entscheidender Bedeutung" ergänzt, der mit strengen regulatorischen Auflagen verbunden ist.

Die Cybersicherheit im Wassersektor ist daher besonders wichtig, da sie zur Sicherheit einer Aktivität beiträgt, die für das Überleben und die Gesundheit der Bevölkerung notwendig ist. Sichere Infrastrukturen zeichnen folglich auch die Unabhängigkeit eines Landes aus.–

Das Beispiel Israel und die drei Angriffswellen innerhalb eines Jahres

Der geopolitische und geografische Kontext Israels verschärft Probleme bezüglich der Wasserversorgung. Diese Situation hat das Land dazu veranlasst, genau wie die Golfstaaten auf Technologie zu setzen. So stammen 80 % des in Israel verbrauchten Trinkwassers aus Entsalzungsanlagen.

Im März 2020 vereitelte Israel eine Reihe von Cyberangriffen, die darauf abzielten, die industriellen Kontrollsysteme mehrerer israelischer Wasseranlagen zu übernehmen. Ziel dieser Angriffe wäre es gewesen, den Chlorgehalt im Wasser zu erhöhen (um es folglich für die Konsumenten zu vergiften) und die automatische Abschaltung der Pumpen auszulösen. Berichten zufolge hatten mehrere tausend Einwohner während einer Periode hoher Temperaturen keinen Zugang zu Wasser. Die israelische Regierung machte Berichten zufolge den Iran dafür verantwortlich und führte als Vergeltung einen Cyberangriff auf den iranischen Hafen Shahid Rajaee durch.

Zwei Monate später richtete sich eine zweite Angriffswelle gegen landwirtschaftliche Wasserpumpen, ohne dass es zu Schäden kam. Im Dezember 2020 schließlich gelang es iranischen Cyberangreifern, in die Verwaltung eines Wassertanks einzudringen, indem sie eine schlecht gesicherte Mensch-Maschine-Schnittstelle (HMI) ausnutzten. Diese israelischen Beispiele zeigen, in welchem Ausmaß Cyberangriffe mittlerweile zum Arsenal von Staaten im Rahmen von mehr oder weniger offenen Konflikten oder der Sammlung von Informationen gehören. In einem anderen Bereich wurden kürzlich Russland und China nach den Cyberangriffen auf die Europäische Arzneimittelagentur (EMA) im Jahr 2020 angeprangert.–



Ist der Wassersektor bereit für eine Cyberkriegsführung?

Das Cybersicherheitsniveau in der Wasserindustrie ist allgemein sehr unterschiedlich ausgeprägt. Obwohl einige Betreiber bereits seit mehreren Jahren in ihren Ausschreibungen Hinweise bezüglich Cybersicherheit geben, wird das Cyberrisiko von den lokalen Behörden noch immer kaum berücksichtigt. Dies erklärt zum Teil, wie relativ einfache Angriffe manchmal industrielle Systeme infizieren können. Dennoch scheint die gesamte Wasserwirtschaft nun entschlossen zu sein, mit anderen Bereichen wie dem Energie- oder dem Bankensektor gleichzuziehen, die zuvor bereits dafür sensibilisiert worden sind.

„In Frankreich haben die Ministerien und die ANSSI seit der Verabschiedung des Gesetzes über die militärische Planung und der europäischen Network-and-Information-Security-Richtlinie (NIS) die lokalen Behörden und die betroffenen Unternehmen sehr für dieses Thema sensibilisiert", erklärt David Giorgis, Leiter der IT- und IoT-Sicherheit für die französische Region und Leiter der Industrial IT bei Suez France. *„Bisher wurde die Cybersicherheit in den Ausschreibungen der Gebietskörperschaften – von einigen Ausnahmen abgesehen – nur sehr kurz erwähnt. Heute nimmt das Thema oft mehrere Seiten ein, und es werden fundierte Antworten erwartet. Dies ist für die Zukunft ein beruhigendes Zeichen eines wachsenden Bewusstseins und einer steigenden Kompetenz."*–

Interview mit dem Kunden

Standpunkt: Cybersicherheit, ein Reflex, der in der Wasserwirtschaft zu Leben erwacht

David Giorgis, Leiter der Abteilung IT- und OT-Sicherheit sowie Industrial IT bei SUEZ Frankreich, kann die Entwicklungen in der Wasserwirtschaft aus erster Reihe beobachten. Wir konnten ihm ein paar Fragen stellen und mit ihm unter die Oberfläche der Cybersicherheit des Sektors tauchen.

David Giorgis – *„Etwa 90 % der Cybervorfälle, die wir beobachten, betreffen Geschäftscomputer, also Büroautomation, Workstations, E-Mail und Anwendungen. Es muss erwähnt werden, dass die Daten von Millionen von Direktkunden in unserem CRM vorhanden sind und dass unser IS unter anderem für die Verbrauchskontrolle zugänglich sein muss. Dies sind alles Werte, die es zu schützen gilt – zusätzlich zu den klassischen Schwachstellen, etwa bei Messaging-Systemen..*

Glücklicherweise wurde bei den IT-Projekten von SUEZ der Ansatz ‚Security by Design' systematisch umgesetzt. Bei reinen Industrieprojekten war dieser Reflex noch nicht überall vorhanden, da sie oft lokal verwaltet werden und die Cybersicherheit allmählich Teil der Kultur wird. Das bedeutet, dass diese IoT-Projekte immer sicherer werden. Aus diesem Grund implementiert SUEZ ein globales Cybersicherheitskonzept, um eine maximale Betriebsleistung zu erreichen. Die Schwierigkeit bei dem Versuch, betriebliche Systeme cybersicher zu machen, liegt häufig in den Industrieprotokollen. Einige große Hersteller haben in der Tat Besonderheiten in die Standardprotokolle eingebracht, und die Sicherheits-Tools werden immer besser, um diese zu verstehen. Die Analyse ist daher begrenzt, während der Anbieter der Cybersicherheitslösung ein spezifisches Modul entwickelt. Daher ist es wichtig, dass die Akteure des Sektors zusammenarbeiten."

Im Rahmen seiner Tätigkeit arbeitet David Giorgis regelmäßig mit den kommunalen Kunden von SUEZ France zusammen. Wir haben ihn gefragt, welche Empfehlungen im Bereich der industriellen Cybersicherheit von Wasserprojekten am häufigsten ausgesprochen wurden:

DG – *„Eine neue Zusammenarbeit beginnt immer mit einer Analyse der bestehenden Situation, um sicherzustellen, dass die verfügbaren Informationen der Realität entsprechen. Danach wird in der Regel eine Verhandlungsphase eingeleitet, um veraltete Geräte zu erneuern und vorhandene Geräte zu aktualisieren. In Wirklichkeit geht es darum, ‚so aktuell wie möglich' zu sein: Manchmal sind wir gezwungen, auf alten Betriebssystemen zu bleiben, weil die Geschäftsanwendungen nicht mit den neuesten Versionen dieser Betriebssysteme kompatibel sind.*

Der andere wichtige Bereich, in dem Verbesserungen möglich sind, ist die Segmentierung des operativen Netzes. Das ist eine große Aufgabe. Außerdem ist es notwendig, die industrielle IT von der Management-IT zu trennen, was für SUEZ eine wichtige Regel ist, oder in Ausnahmefällen dafür zu sorgen, dass die Verbindungspunkte zwischen beiden sicher sind. Dies erfordert die Einrichtung einer grundlegenden Sicherheitsbasis (Antivirus, Updates, Firewall usw.). Dies sind sehr klassische Maßnahmen für die Welt der Management-Informationssysteme, aber immer noch neu für den industriellen Sektor im Allgemeinen und den Wassersektor im Besonderen."

Angesichts des Umfangs der Aufgabe stellt sich die Frage, wie sich die Teams vor Ort fühlen: Empfinden sie die Cybersicherheit generell als Hindernis für ihre Projekte?

DG – *„In den letzten Jahren wurde viel mehr über die Herausforderungen der Cybersicherheit gesprochen, sodass sich die industriellen Teams insgesamt der Bedeutung dieses Themas sehr bewusst sind. Ich möchte hinzufügen, dass die Rolle des Verantwortlichen für die Sicherheit von Informationssystemen nicht darin besteht, ein Projekt zu stoppen, sondern es so zu begleiten, dass es diese und jene Sicherheitsbedingungen einbezieht. Unsere Philosophie ist es, industrielle IT-Spezialisten vor Ort zu kompletten, sicheren und nationalen Paketlösungen zu führen. Unsere zentralen Teams und unsere Tochtergesellschaft SUEZ Smart Solutions, die sich auf industrielle Systeme und deren Cybersicherheit spezialisiert hat, stehen ihnen auch bei der Umsetzung dieser Lösungen zur Seite."*–

Ein pragmatischer und kooperativer Ansatz, der darauf abzielt, die Cybersicherheit als echte Unterstützungsfunktion in der täglichen Arbeit der operativen Teams zu positionieren.

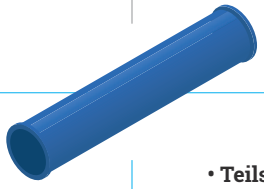
Welche Probleme gibt es im Zusammenhang mit der Cybersicherheit in der Wasserwirtschaft?

Teil III.

Was macht die Wasserwirtschaft – abgesehen von staatlichen oder kriminellen Motiven – zu einem bevorzugten Ziel für Cyberangreifer? Wir haben die wichtigsten Cyberprobleme, mit denen der Sektor konfrontiert ist, unter drei Gesichtspunkten aufgelistet: menschlich, technologisch und operativ.



Einleitend sei darauf hingewiesen, dass die Cybersicherheit in der Welt des Wassers im Wesentlichen darauf abzielt, die Verfügbarkeit und Integrität industrieller Prozesse zu gewährleisten. Der Begriff der Vertraulichkeit wird ebenfalls herangezogen, allerdings im weniger kritischen Kontext der Kundenbeziehungen: Die Integrität der Daten ist im Rahmen der Telemetrie von großer Bedeutung, um die Genauigkeit der Rechnungsstellung zu gewährleisten, aber der Einsatz steht in keinem Verhältnis zu der Tatsache, dass beispielsweise die Trinkwasserversorgung gewährleistet werden muss.



Menschliche Perspektive

• Erhebliche menschliche Risiken, die mit dem Sektor verbunden sind
Wie im vorangegangenen Abschnitt dargelegt, sind die Trinkwasserversorgung und die Abwasseraufbereitung kritische Tätigkeiten, da sie für das Überleben und die Gesundheit der Menschen notwendig sind. Die Folgen eines Dammbruchs oder einer Wasserverschmutzung wären dramatisch.

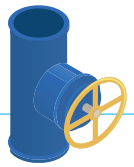
• Das Risiko von Fehlern oder böswilligen Handlungen
Aus diesen Gründen ist die menschliche Komponente, sei sie nun das Ergebnis eines Fehlers oder einer vorsätzlichen böswilligen Handlung, eine der am meisten gefürchteten Komponenten für Industrieunternehmen und Betreiber. Dies führt zur Entwicklung verschiedener Szenarien für eine optimale Betriebssicherheit.

• Teils komplexe Kooperationen
Aus Unternehmenssicht bedeutet das koordinierte Management von IT- und operativer Cybersicherheit, dass die Bedürfnisse des Automatisierungsingenieurs erfüllt und gleichzeitig die vom CISO oder IT-Sicherheitsmanager identifizierten Risiken reduziert werden. Aus organisatorischer Sicht kommt es häufig vor, dass mehrere Akteure beispielsweise für dieselbe Stadt arbeiten. Letztere haben möglicherweise selbst einen Teil der Verwaltung im Haus behalten. Es handelt sich also um ein echtes wasserwirtschaftliches Ökosystem, das lernen muss, zusammenzuarbeiten.

• Industrielle Cybersicherheit oft außerhalb des Geltungsbereichs
Wie in anderen Branchen ist es üblich, dass betriebliche Cybersicherheitsteams eher dem Betriebsleiter als dem IT-Leiter des Unternehmens unterstellt sind. In einigen anderen Fällen wird der IT-Manager Cyberregeln empfehlen, die der Betreiber des Dienstes anwenden kann. Oder auch nicht.–

> ***Industrielle Netzwerke werden bei der Bewertung von Cybersicherheitsrisiken oder bei der Wiederherstellung nach einem Cyberangriff manchmal übersehen"***

Tarik Zeroual
Global Account Manager bei Stormshield



Technologische Perspektive

• Unscharfe Grenze zwischen IT- und industrieller Cybersicherheit
Mit dem Ende des öffentlichen Telefonnetzes migriert die Wasserwirtschaft allmählich zu Kommunikationstechnologien wie Ethernet, 4G und sogar 5G. Diese Entwicklung ist Teil eines weltweiten Trends, der in den letzten Jahren zur Konvergenz zwischen IT und OT geführt hat. Industrielle Netze sind daher stärker gefährdet als früher, da sie über das Computernetz in die Reichweite eines potenziellen Cyberangriffs geraten sind.

• Ein zu sicherndes Internet der industriellen Dinge (IIoT)
IIoT bezieht sich auf jedes verbundene Objekt, das Informationen (Temperatur, offenes Ventil, Chlorgehalt usw.) an eine Maschine sendet. Diese relativ preiswerten „intelligenten" Sensoren lassen sich leicht in bestehende Systeme integrieren, was ihren Erfolg in industriellen Umgebungen erklärt. Leider sind sie auch sehr anfällig, da die Cybersicherheit in der Konzeptionsphase noch zu selten berücksichtigt wird.

• Ausweitung des Schutzes auf virtuelle Umgebungen
Mit der Einführung der Cloud, die insbesondere durch das IIoT mit Daten gefüttert wird, und der Nutzung virtueller Maschinen wurde ein wesentlicher Teil der IT von Wasserunternehmen ausgelagert. Es ist daher notwendig, diese Cloud-Verbindungen zu sichern, um Cyberangriffe auf die Infrastruktur von Industriestandorten zu verhindern. Vorausgesetzt, es wird klar festgelegt, wer zwischen den Geschäftsbereichen und den verwalteten Diensten dafür verantwortlich ist.–

> ***Die vorausschauende Wartung ist eine der wichtigsten betrieblichen Anwendungen des IIoT. Die Daten der Sensoren werden für vorausschauende Berechnungen verwendet, um unnötige Wartungsarbeiten zu vermeiden und die Ausfallwahrscheinlichkeit zu verringern"***

Tarik Zeroual
Global Account Manager bei Stormshield



Betriebliche Perspektive

• Große Unterschiede bei den Reifegraden
In Europa variiert das Ausmaß, in dem die Cybersicherheit von Wasserinfrastrukturen berücksichtigt wird, sehr stark – je nachdem, wie aufgeklärt die zuständige Behörde ist und welche Ressourcen ihr zur Verfügung stehen.

• Multisite im Zentrum der Cyberkomplexität des Sektors
In der Praxis ist die Sicherung kritischer Wasserinfrastrukturen nicht einfach, da es sich um einen stark dezentralisierten Sektor handelt, der mehrere Standorte zur Versorgung des gesamten Landes benötigt. Internetverbindungen und Fernwartung sind also problematische Aspekte in Bezug auf Fernzugriffsmethoden, die es ermöglichen, das ordnungsgemäße Funktionieren der entfernten Standorte zu gewährleisten.

• Eine schwierige Cyberimplementierung vor Ort
Aufgrund ihrer verstreuten Verteilung unterliegen einige Infrastrukturen der Wasserwirtschaft besonderen Einschränkungen, etwa in Bezug auf Feuchtigkeit oder Temperatur.

• Empfindliche Produktionsanlagen
Es ist nicht ungewöhnlich, dass ein automatisiertes System in einer Kläranlage bereits 10, 15 oder sogar 20 Jahre alt ist. Diese in die Jahre gekommenen Anlagen verfügen nur selten über integrierte Cyberschutzmechanismen und verwenden Industrieprotokolle, die nicht sehr sicher und daher anfällig sind.

• Eine durchlässige Netzarchitektur
Diese Systeme sind noch zu oft nach einer „flachen" Netzarchitektur organisiert, also ohne Partitionierung oder Segmentierung. Eine echte Gefahr angesichts der Verbreitung von Malware.

• Der Zwang zur Echtzeit
Die Empfindlichkeit dieser Anlagen ist auch auf den operativen Zwang zur Echtzeit zurückzuführen. In der Wasserwirtschaft kommt es darauf an, jeden Vorgang sofort auszulösen und somit die Zeit zwischen Anweisung und Aktion zu minimieren. Sicherheitseinrichtungen müssen daher eine möglichst geringe Latenzzeit aufweisen, um den industriellen Prozess nicht zu stören. Dies könnte in der Tat zu einem Produktionsstillstand führen.

• Eine Vielzahl von Akteuren, die die Sichtbarkeit verwischen können
Das Alter der meisten industriellen Wassersysteme bedeutet, dass der derzeitige Betreiber nicht immer die Kontrolle über die Historie der Veränderungen hat. Die Inanspruchnahme zahlreicher Dienste-Anbieter, Betreiber oder Integratoren trägt ebenfalls dazu bei, das Phänomen zu verstärken.–

> ***„Diese verteilten Netze sind auch anfälliger für physisches Eindringen. Das bedeutet, dass wir über Cybersicherheit anders denken müssen. Dieses Sicherheitsproblem erhöht die Komplexität des Cybersicherheitskonzepts für eine Wasseraufbereitungsanlage oder einen Wasserturm"***

Vincent Nicaise
Industrial Partnership and Ecosystem Manager bei Stormshield

Infografik

Die primären Schwachstellen des Sektors

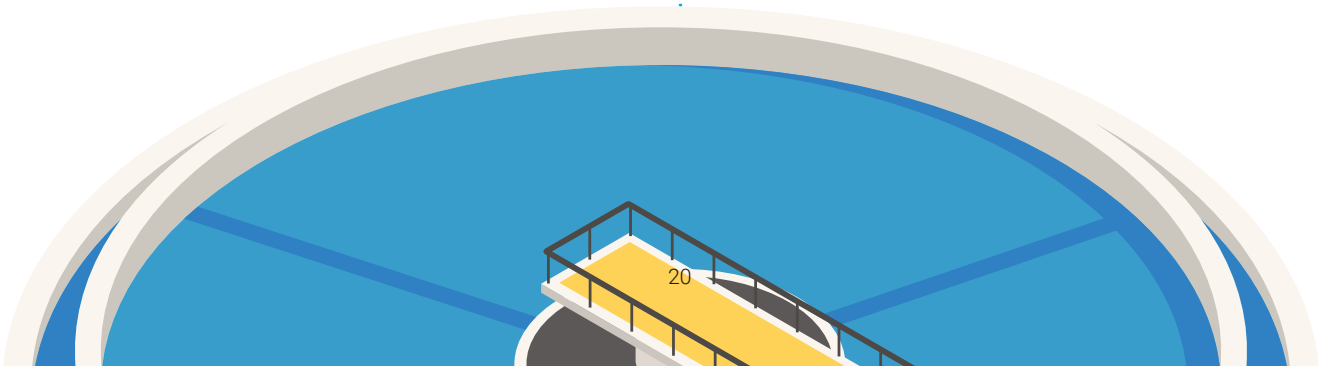
In den letzten Jahren waren Cybersecurity-Experten besonders besorgt über die Einführung des „Industriellen Internets der Dinge“ (IIoT). Dies sollte jedoch nicht über eine Reihe struktureller Schwachstellen in diesen industriellen Systemen hinwegtäuschen.

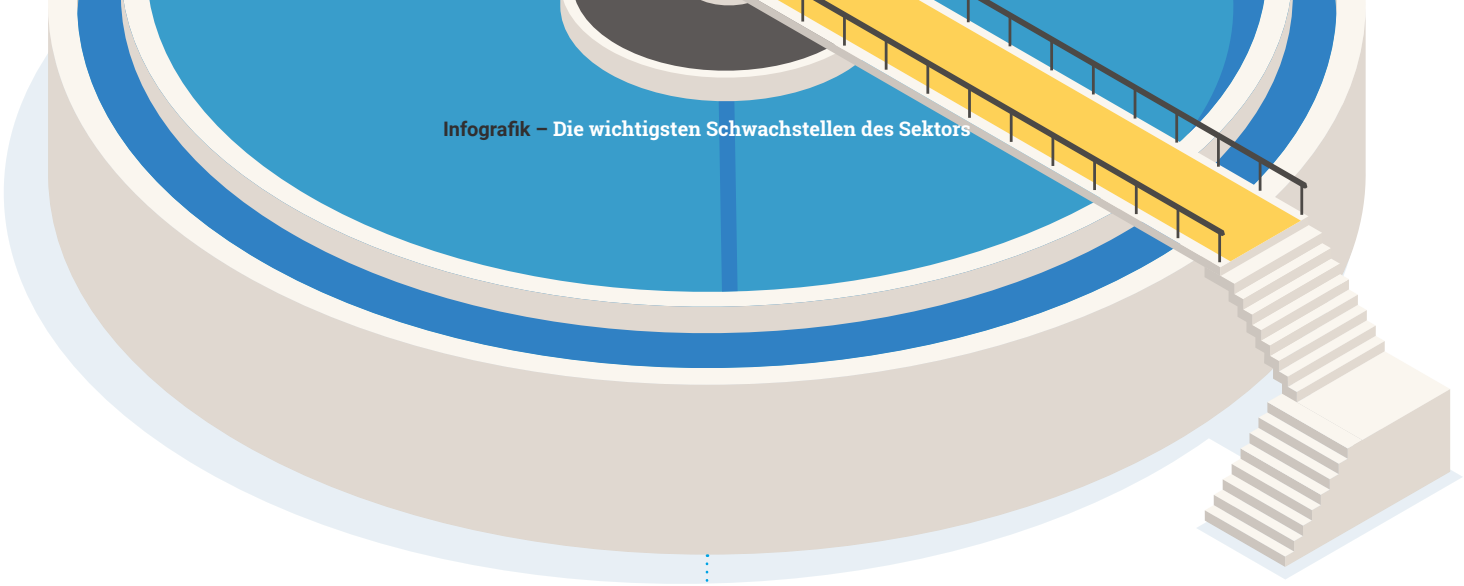
Industrielle Kontrollsysteme (ICS – „*Industrial Control Systems*“) als Ganzes können auf mehreren Ebenen Schwachstellen aufweisen:

In Betriebsmitteln (Software, Hardware und Firmware), etwa uneinheitlichen, veralteten und/oder unsicheren Technologien

Dazu gehören, in keiner bestimmten Reihenfolge, das industrielle Prozessleitsystem (DCS für „Distributed Control System“), die Mensch-Maschine-Schnittstellen (HMI), die speicherprogrammierbaren Steuerungen (SPS), die SCADA-Steuerungs- und Datenerfassungslösungen und andere Überwachungs-Software sowie die IIoT-Sensoren und Cloud-Plattformen, mit denen sie kommunizieren. Das Ganze bildet eine erhebliche Angriffsfläche.

Im Februar 2020 wurde eine Sicherheitslücke in den C-More-HMI-Touchpanels des amerikanischen Herstellers AutomationDirect entdeckt. Diese werden unter anderem von Betreibern in der Wasserwirtschaft verwendet. Durch Ausnutzung dieser Schwachstelle (CVE-2020-6969) könnten Cyberkriminelle Anmeldedaten und andere sensible Informationen in ungeschützten Projektdateien entdecken.





Infografik – Die wichtigsten Schwachstellen des Sektors

Im Netzwerk und seiner Peripherie

Industrielle Netzwerke sind häufig in einer flachen Architektur aufgebaut und nicht immer nach den Grundsätzen der Segmentierung voneinander getrennt. Netzwerkgeräte sind nicht nur eine Brutstätte für Malware, sondern werden auch täglich von neuen Schwachstellen geplagt – weil sie veraltet sind und nicht ausreichend aktualisiert werden. Solche Schwachstellen können sich auch aus der Fernverwaltung ergeben, die immer noch zu oft auf ungesicherte Weise erfolgt.

In Betriebssystemen von Überwachungs- oder Programmierstationen

Diese nicht verbundenen Systeme sind aus Cyberperspektive veraltet, weil sie nicht aktualisiert werden.

In Protokollen

Die Verwendung von unverschlüsselten und unsicheren Protokollen wie Modbus ist in der industriellen Überwachung üblich.

Bei Anwendern

Nicht alle Betreiber und Instandhalter, die für industrielle Prozesse zuständig sind, sind sich der Problematik der Cybersicherheit bewusst. Benutzerrichtlinien, Passwörter und Zugangsverwaltung sind Elemente, die in industriellen Systemen zu selten eingesetzt werden.–

Welche Cybervorschriften gelten für die Wasserwirtschaft?

Teil IV.

Neben den strengen Gesundheits- und Umweltvorschriften unterliegt der Wassersektor auch nationalen und internationalen Cybervorschriften.



> ***Mit der Umsetzung der Dekrete im Jahr 2016 begannen wir eine Beschleunigung der Cybermaßnahmen auf Seiten der französischen Betreiber zu beobachten. Auf kommunaler Ebene hat es etwas länger gedauert und wir haben die ersten Entwicklungen zu diesem Thema zwischen 2017 und 2018 gesehen“***

Khobeib Ben Boubaker
Head of Industrial Security Business Line bei Stormshield

Neben den strengen Gesundheits- und Umweltvorschriften unterliegt der Wassersektor auch nationalen und internationalen Cybervorschriften.

Angesichts der oben beschriebenen Probleme im Bereich der öffentlichen Gesundheit ist es leicht zu verstehen, warum die Tätigkeit bestimmter Akteure des Sektors als kritisch angesehen wird. In Frankreich haben die für die Trinkwasserversorgung und -verteilung zuständigen Akteure den Status von OIV (Operateurs d'importance vitale – Betreibern von entscheidender Bedeutung) im Sinne des französischen Militärplanungsgesetzes (2013). Sie müssen daher die 20 Regeln einhalten, die im genannten Gesetz für die kritischsten invasiven Arten festgelegt sind: Zuordnung der invasiven Arten, Überwachung, Identifizierungs- und Authentifizierungsregeln, Meldung von Vorfällen, Einsatz qualifizierter Sicherheitslösungen auf höchster Ebene usw.

Auf europäischer Ebene können sie gemäß der Network-and-Information-Security-Richtlinie (NIS) (2016) auch als ESO („Essential Service Operators“ – Betreiber wesentlicher Dienste) bezeichnet werden. Frankreich war ein wenig voraus, als es die Richtlinie in nationales Recht umsetzte, um den Bereich der Abwasserentsorgung einzubeziehen: Eine europäische Harmonisierung ist in Sicht, da dieser Bereich bei der für Ende 2021 geplanten Überarbeitung der Richtlinie ebenso wie die Abfallwirtschaft in den Text aufgenommen werden soll.

Schließlich werden einige Strukturen, oft kleine Gemeinschaften, weder als OIV noch als OSE betrachtet: Sie sind nicht gesetzlich verpflichtet und gehen daher nach ihren Möglichkeiten und ihrem Bewusstsein für die Bedrohung vor. Um sie dabei zu unterstützen, hat die ANSSI mehrere Leitfäden für bewährte Praktiken veröffentlicht, die eine Selbsteinschätzung und Selbstabsicherung ermöglichen. Und für diejenigen, die noch weiter gehen wollen, gibt es zahlreiche Normen – darunter die internationale Norm für industrielle Cybersicherheit IEC 62443-3-3 und der US-amerikanische NIST-Standard –, die zur Bestimmung des erforderlichen Sicherheitsniveaus herangezogen werden können.–

Und was ist mit morgen?

Teil V.

Die digitale Technologie ist ein wichtiger Hebel für den Schutz des Wassers: Nur das Notwendige zu entnehmen, den ökologischen Fußabdruck der Anlagen zu optimieren, oder die Lieferung von Qualitätswasser ohne Leckagen zu gewährleisten, sind Herausforderungen, die in den kommenden Jahren an Bedeutung gewinnen werden.



Im Wassersektor werden immer mehr Technologien eingesetzt, um mithilfe von maschinellem Lernen den Betrieb von Bohrungen und Pumpen zu optimieren, schwache Signale, die auf Dürre hindeuten, zu erkennen oder Wassermengen vorherzusagen.

Mit der fortschreitenden Digitalisierung der Branche werden die Grenzen zwischen IT und OT weiter verschwimmen, was die Cyberrisiken, denen der Sektor bereits jetzt ausgesetzt ist, zusätzlich erhöht. Die Wasserwirtschaft muss daher unbedingt ihr Cybersicherheitsniveau anheben und ihre Widerstandsfähigkeit gegenüber Cyberangriffen ausbauen, die immer häufiger und heftiger werden.

Eine gut informierte Öffentlichkeit und verschärfte Vorschriften

In Zukunft muss die Cybersicherheit daher ein integraler Bestandteil der Aufrechterhaltung des industriellen Prozesses sein. Dies ist ein großes Unterfangen, da fast alle bestehenden Einrichtungen gesichert werden müssen. Um diesen Prozess zu begleiten, wird der Trend in den nächsten Jahren darin bestehen, den rechtlichen Rahmen für die Cybersicherheit zu stärken, so David Giorgis. Für den Leiter der IT- und OT-Sicherheit sowie der industriellen IT bei SUEZ France ist die bevorstehende Überarbeitung der Network-and-Information-Security-Richtlinie (NIS) ein erster Schritt, dem zahlreiche Klarstellungen etwa im Militärprogrammgesetz folgen werden. Die grenzüberschreitende Zusammenarbeit muss eines der Hauptanliegen dieser neuen Verordnungen sein, deren Ziel es laut ANSSI ist, „*die Cyberresilienz der Europäischen Union und ihrer Mitglieder zu stärken*".

> ***„Automatisierungsintegratoren befassen sich zunehmend mit den Herausforderungen der industriellen Systeme. Zu begrüßen ist auch die Zahl der Ausschreibungen für den Entwurf oder die Renovierung von Systemen, die jetzt eine Cyberkomponente enthalten"***
>
> **Vincent Nicaise,**
> Industrial Partnership and
> Ecosystem Manager bei Stormshield

Es ist daher eine gute Idee, einen Schritt voraus zu sein, indem man den Rat von Tarik Zeroual, Global Account Manager bei Stormshield, befolgt, der darauf drängt, „*über die Mindestanforderungen hinauszugehen*".

Bewährte technische Lösungen

Die Zukunft der Wasserwirtschaft wird unweigerlich von Cyberbedrohungen geprägt sein, aber Anbieter und Forscher im Bereich Cybersicherheit arbeiten hart daran, Lösungen für wiederkehrende und neue Probleme zu finden.

• Schutz der Netze durch Segmentierung

Die Segmentierung der Netze ist wichtig, um die Ausbreitung eines Cyberangriffs zu verhindern, indem Teilsysteme isoliert werden. Zu diesem Zweck können Firewalls wie die Produktreihe Stormshield Network Security (SNS) verwendet werden.

• Datenverkehr validieren

Wichtig sind auch Lösungen, mit denen die Rechtmäßigkeit der von den Automaten ausgeführten Befehle überprüft werden kann. „*Es geht um den Schutz vor Man-in-the-Middle-Angriffen, aber auch um die Überprüfung der Integrität der Daten durch Inspektion*", sagt Stéphane Prévost, Produkt-Marketing-Manager bei Stormshield.

• Fernzugriffe authentifizieren

In einem Sektor mit teilweise weit voneinander entfernten Infrastrukturen müssen unbedingt Systeme zur Verwaltung und Sicherung des Fernzugriffs (Fernwartung, Alarmverwaltung usw.) eingerichtet werden. Um eine sichere Kommunikation zwischen verschiedenen Standorten und Maschinen zu gewährleisten, bietet die SNS-Lösung eine Datenverschlüsselung durch den Aufbau von VPN-Tunneln.

• Sich einen Überblick verschaffen

Um die Verwaltung mehrerer verteilter SNS-Lösungen zu erleichtern, hat Stormshield eine zentralisierte Verwaltungsplattform namens Stormshield Management Center (SMC) entwickelt. Stormshield bietet auch eine Lösung zur Protokollverwaltung: Stormshield Log Supervisor (SLS) bietet einen besseren Einblick in den Status und die Protokolle von IT-Netzwerken. Diese Lösungen berücksichtigen obendrein die Zunahme des Datenverkehrs zwischen IT und OT – dank einer einheitlichen Sicherheitsrichtlinie zwischen den beiden Welten.

• Arbeitsplätze schützen

Der Schutz von Terminals ist von grundlegender Bedeutung – unabhängig davon, ob es sich um Engineering- oder Überwachungsstationen handelt, da sie die Parameter des Betriebsprozesses steuern und einen Echtzeitüberblick über den Zustand der Systeme liefern. Ein Cyberangriff auf die Überwachungsstationen beispielsweise würde die Betriebsteams völlig „blind" machen und den ordnungsgemäßen Ablauf der industriellen Prozesse verhindern. Deshalb kombiniert die Stormshield-Endpoint-Security-Lösung (SES) eine Verhaltensanalyse-Engine, eine Gerätesteuerungs-Engine und die Möglichkeit, Anwendungen auf eine Whitelist zu setzen, um nicht unbedingt benötigte Software zu deaktivieren und so einen besseren Schutz zu gewährleisten.

• Die Anlagen an die Bedürfnisse der Wasserwirtschaft anpassen

Die Wasserwirtschaft unterliegt einer Reihe spezifischer physischer Begebenheiten (hohe Luftfeuchtigkeit, große Temperaturschwankungen, Isolierung bestimmter Standorte usw.) sowie betrieblicher Bedürfnisse für die Geschäftskontinuität. Diese Branche

SNi40 und SNi20, die industriellen Firewall-Lösungen

In Zusammenarbeit mit Schneider Electric hat Stormshield robuste Gehäuse entwickelt, die den Anforderungen von stark beanspruchten Umgebungen wie der Wasserwirtschaft gerecht werden. Optimiert für niedrige Latenzzeiten und mit Bypass-Funktion, lassen sie sich leicht in der Nähe der zu schützenden Geräte installieren und halten den besonderen Bedingungen dieser Branche stand. Auf regulatorischer Ebene ist das SNi40 das einzige Produkt auf dem Markt, das die grundlegende Qualifikation der ANSSI erhalten hat, nachdem es die CSPN-Sicherheitszertifizierung der ersten Stufe bekommen hatte. Eine Garantie für Robustheit und Zuverlässigkeit.–

benötigt Geräte, die diesen Umgebungsauflagen entsprechen. Die Fähigkeiten der SNS-Firewalls und ihre Bypass-Funktion (Sicherheitsmodus) sind auch für die Wasserwirtschaft von großem Nutzen, da sie die Verfügbarkeit des Betriebsprozesses gewährleisten.

• ***Sicherheit durch Design*, auch bei der OT**

Der Ansatz von „*Security by Design*" besteht darin, die Cybersicherheit bereits in der Phase des Systementwurfs zu berücksichtigen – ein für die Wasserwirtschaft relevanterer und besserer Ansatz als die *nachträgliche* Integration von Cybermaßnahmen. Dies liegt daran, dass die Entwicklungszeiten relativ lang sind, die Probleme der installierten Basis noch größer sind als bei der Büroautomation und es zahlreiche technische Herausforderungen bei der Kompatibilität mit bestehenden Systemen gibt. Integratoren und Experten sind sich daher bewusst, dass „*Security by Design*" der Schlüssel zu einer besser geschützten Industrie der Zukunft ist.

Neue Profile für Cybersicherheit in Wasserindustrie

Wie wir gesehen haben, erfordert die Gewährleistung der Cybersicherheit im Wassersektor heute den Einsatz von immer mehr Instrumenten. Daher sind viele verschiedene Fähigkeiten erforderlich, um sie zu erfassen, sie zu verstehen und optimal zu nutzen. Um sicherzustellen, dass die Überwachungs- und Interventionsteams (CSIRT, SOC usw.) über die besten Profile verfügen, ist es daher wichtig, dass die Automatisierungsspezialisten in IT-Cybersicherheit geschult sind. Und umgekehrt, dass Cybersicherheitsspezialisten gute Kenntnisse der industriellen Welt erwerben.

> ***Um unsere Teams besser kennenzulernen und die Zusammenarbeit zu stärken, organisieren wir jedes Jahr eine Cyberübung, bei der unsere EO-Spezialisten an einem Szenario mit industriellen Systemen teilnehmen"***
>
> **David Giorgis**
> Leiter der IT- und OT-Sicherheit sowie der industriellen IT bei SUEZ Frankreich.



Hat nach der Konvergenz der IT- und OT-Systeme nun auch die Konvergenz der entsprechenden Teams begonnen? Die Zeit wird es zeigen, doch scheint die Cybersicherheit des Wassersektors in den kommenden Jahren von der Fähigkeit der Industrie und der Cybersicherheitsexperten abzuhängen, gemeinsam relevante Lösungen zu entwickeln.

Haben Sie ein komplexes Problem mit der Cybersicherheit? Ein Sicherheitsprojekt rund um eine Infrastruktur? Unsere internen Experten stehen Ihnen zur Verfügung, um Sie zu beraten und zu unterstützen.
Kontaktieren Sie uns.

Interview mit dem Kunden

Ein verteiltes Netzwerk sichern: Optimierung der Cybersicherheit eines städtischen Wasserversorgungsunternehmens

Die Metropole einer großen französischen Region hat sich dafür entschieden, die Verwaltung des öffentlichen Dienstes für die Gewinnung, den Transport, die Speicherung und die Verteilung von Trinkwasser auf dem größten Teil ihres Gebiets einem einzigen Unternehmen zu übertragen, nachdem sie mehrere Jahre lang mit drei verschiedenen Betreibern zusammengearbeitet hatte.

1,3 Millionen Einwohner

60 Gemeinden

100 Wassertürme

Die IT-Infrastruktur modernisieren und das Sicherheitsniveau erhöhen

Diese Rationalisierung des Dienstes war für die Stadt auch eine Gelegenheit, ihre IT-Architektur zu überprüfen, um sie moderner und sicherer zu machen.

Der vom Kunden ausgewählte Referenzbetreiber beauftragte Stormshield mit der Unterstützung bei der Sicherung dieser industriellen Umgebung und der Implementierung der wichtigsten erwarteten Funktionen, nämlich der Kontrolle und Filterung jeder Kommunikation (dank *„Deep Packet Inspection"* (DPI) und einer besonderen Aufmerksamkeit für das Modbus-Protokoll) und der Implementierung einer IPSec-VPN-Lösung zum Schutz der Kommunikation.

Firewalls wurden eingerichtet, um die verschiedenen Betriebsnetze (Büro-IT-Netz, zentrale VPN-Konzentratoren, Industrie- und

Sicherheits-IT sowie entfernte Standorte) zu segmentieren und besser zu schützen.

Eine an die Bedürfnisse des Wassersektors angepasste industrielle Antwort

Die Sicherheit des zentralen Standorts wurde daher durch die Installation von Firewalls zwischen dem Büronetz und den Geschäftsräumen verstärkt. Diese Einrichtungen sind in zwei getrennte Netze (Sicherheits- und Industrienetz) aufgeteilt, die jeweils durch eine Gruppe von Firewalls geschützt werden, die die Funktion eines VPN-Konzentrators bieten.

Diese Architektur ermöglicht es, die gleichen Anwendungen mit den verschiedenen Wassertürmen zu verbinden. Diese wurden individuell mit zwei Clustern von gehärteten SNi40-Firewalls ausgestattet, um die Datenströme zwischen den verschiedenen Standorten und Anwendungen zu sichern. Der Kunde war auch sehr angetan von der Stateful-DPI-Funktion der Industrieprotokolle, die eine Weiterentwicklung der Sicherheit dieser sensiblen Systeme parallel zur Modernisierung der Infrastruktur ermöglichen wird.

Für diese komplexen industriellen Umgebungen konzipierte Dienstleistungen

Um den Service für die Nutzer zu gewährleisten und auf die Zugänglichkeit und Sensibilität bestimmter Standorte zu reagieren, haben Stormshield und der ausgewählte Betreiber einen angepassten Support eingerichtet, der Folgendes umfasst:

- Die Implementierung eines Verfahrens, das es einem technischen Agenten ohne Netzwerk-/Sicherheitskenntnisse ermöglicht, eine fehlerhafte Firewall zu ersetzen und die Site mit dem richtigen Sicherheitsniveau wieder in den Betriebsmodus zu versetzen.

- Aktivierung des Sicherheitsmodus (Bypass) für die 5 % der Sites, die mit einer einzelnen Firewall und nicht mit einem Cluster ausgestattet sind.

- Eine Reihe professioneller Dienstleistungen, die die Stadt bei der Industrialisierung der Konfiguration an den ersten Pilotstandorten unterstützen.–

Drei Schlüsselfaktoren für eine effektive Reaktion

– Eine starke Einbindung des **Herstellers, die es ermöglicht,** das Projekt und seine durchgängige Umsetzung erfolgreich und in kürzester Zeit zu bewältigen.

– Das industrielle **Angebot von Stormshield eignet sich** sowohl für die Verwaltung von Standardstandorten als auch für Umgebungen mit starken industriellen Einschränkungen (Temperatur, Feuchtigkeit, DIN-Schiene, industrielle Stromversorgung, Bypass).

– Eine **einzige Firmware** für die gesamte Stormshield-Network-Security-Reihe und eine **einzige Konsole,** (Stormshield Management Center) zur Verwaltung der gesamten Firewall-Anlage.–

STORMSHIELD

Die europäische Wahl für Cybersicherheit



Weltweit benötigen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden zuverlässige Partner, die sie auf dem Weg des digitalen Wandels begleiten und die Cybersicherheit ihrer Einrichtungen, Nutzer und Daten sicherstellen. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien (EU Restricted, NATO Restricted, Common Criteria EAL3+/EAL4+, Qualifikationen und Gütesiegel der ANSSI) sind die richtige Antwort auf IT- und OT-Risiken und um Ihre Geschäftstätigkeit zu schützen. **Dank unserer Sicherheitslösungen können Sie sich voll und ganz auf Ihr Geschäft konzentrieren, ohne sich Sorgen machen zu müssen.**
www.stormshield.com/de

Jegliche Verbreitung, Reproduktion oder Darstellung, auch auszugsweise, dieses Whitepapers für andere Zwecke als den privaten Gebrauch auf irgendeinem Medium ist verboten und kann zivil- und strafrechtliche Verantwortlichkeiten von Personen nach sich ziehen, die sich nicht an dieses Verbot halten.