STORMSHIELD

MEINUNGEN

WASSERINFRAS-TRUKTUR: WENN SICH STAATEN UND CYBE-RANGREIFER EIN-MISCHEN

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

Versuche von Cyberangriffen auf Staudämme, Bewässerungssysteme oder sogar Wasseraufbereitungsanlagen sind in den Medien nicht sehr präsent. Dennoch existieren diese Angriffe – und sie nehmen sogar einen beispiellosen strategischen Charakter an. Wie ist der aktuelle Stand der Cybersicherheit von Wassernetzen auf der ganzen Welt?

Im Allgemeinen ist der Cyberschutz für den Menschen ein wichtiges Thema, bei dem es von der Frage der Versorgung mit Nahrungsmitteln bis zur Gesundheit, einschließlich des Wassermanagements geht. Neben den kritischen Problemen, die diesem Sektor und der entscheidenden Bedeutung dieser Ressource inhärent sind, muss sich die Wasserindustrie auch mit dem Umfang von Cyber-Angriffen, deren Ziel sie ist, befassen. In der Tat **sind Cyber-Angriffe auf Wasser, so wie die Industrie selbst: Komplex und raffiniert**. Und sie werden oft von staatlichen Organen orchestriert, die darauf abzielen, eine Wirtschaft oder ein Land aus dem Gleichgewicht zu bringen. Die Wasserindustrie muss sich daher Produktionsproblemen von großer Bedeutung und gleichzeitig dazu auch Sicherheitsanforderungen stellen. Alle

kritischen Infrastrukturen und Geräte müssen wirksam geschützt werden, indem eine Verteidigungshaltung eingenommen wird, um den Schaden, der durch groß angelegte Cyberangriffe verursacht werden könnte, so weit wie möglich zu begrenzen.

CYBERSICHERHEIT VON WASSERNETZEN – WAS WURDE BEREITS ERREICHT?

Die wichtigsten digitalen Nachrichten über Wasserinfrastrukturen sind der Austausch von RTC-Verbindungen (einem alten Kommunikationsmodus), die für die Migration in das Ethernet-Netzwerk oder in 4G- und 5G-Netzwerke, die eine effizientere Konnektivität bieten, veraltet sind. Alle Standorte der Wasserindustrie betreiben diese Migration nach und nach und sind daher mit der Außenwelt verbunden, was vorher nicht der Fall war. In den (gesegneten) Tagen der RTC-Verbindungen waren die meisten Geräte (wie z. B. SPS) vom Internet isoliert. Mit dem Ende dieser Art der Kommunikation werden dieselben Geräte jedoch verbunden und müssen sich neuen Cyber-Bedrohungen stellen.

„Die Wasserindustrie ist nun gezwungen, über die Sicherung ihrer Systeme nachzudenken, da sie sich in einer IoT-Logik befinden, oder sogar einer IIoT-Logik und das mit den Sicherheitsproblemen, die damit verbunden sind"

Raphaël Granger, Named Account Manager Stormshield

Dieser Paradigmenwechsel zwingt die Wasserindustrie dazu, auf eine doppelte Herausforderung zu reagieren: Alternde industrielle Systeme und Geräte (Windows XP und weitere) auf effizientere – und besser vernetzte – Technologien umzustellen und den **Begriff der Cybersicherheit als wesentlichen Bestandteil der industriellen Tätigkeit** zu integrieren. *„Die Wasserindustrie ist nun gezwungen, über die Sicherung ihrer Systeme nachzudenken, da sie sich in einer IoT-Logik (Internet of Things) oder sogar einer IIoT-Logik (Industrial Internet of Things) mit den Sicherheitsproblemen, die dem inhärent sind, befinden*", erklärt **Raphaël Granger**, Named Account Manager bei Stormshield.

Die Wasserindustrie ist aber auch Bedrohungen ausgesetzt, die ihrer Natur nach inhärent sind. Aufgrund der Existenz mehrerer physischer Standorte (z. B. Aufbereitungsbecken, Verteilungszentren und andere Wassertürme) muss sich die Wasserindustrie auf verteilte Architekturen verlassen, in denen Nachrichten und Befehle übertragen werden. Die Herausforderungen der Integrität und Vertraulichkeit dieses Austauschs sind daher unerlässlich, um am Ende der Kette die Qualität einer lebensnotwendigen Ressource in einer Zeit sicherzustellen, in der die Verwaltung aus der Ferne weit verbreitet ist. Diese Herausforderungen implizieren aber auch eine echte Cyber-Sensibilität aller Beteiligten – ebenso wie der Anbieter von Fernwartungen.

REGULATORISCHE AUFMERKSAMKEIT IN MEHREREN GESCHWINDIGKEITEN

In Frankreich werden sensible Infrastrukturen, die mit der Wasserindustrie verbunden sind, im Rahmen des Militärplanungsgesetzes seit vielen Jahren als **Betreiber von entscheidender Bedeutung** identifiziert. Und werden daher von der Nationalen Agentur für die Sicherheit von Informationssystemen (Agence nationale de la sécurité des systèmes d'information: ANSSI) genau überwacht. Diese besondere Wachsamkeit des Staates zwingt den Wassersektor aufgrund der Umstände dazu, sich der mit seiner Tätigkeit verbundenen Cyberprobleme immer mehr bewusst zu werden.

Auf internationaler Ebene beginnen die meisten Wasserakteure in Industrieländern ebenfalls damit, die Cybersicherheit als Voraussetzung zu integrieren. *„Das Maß an Cybersicherheit in Wassernetzen entspricht noch nicht dem Grad der Bedrohung, dem die Wasserindustrie ausgesetzt ist"*, gibt **Nebras Alqurashi**, Manager für Geschäfts- und technische Entwicklung im Mittleren Osten bei Stormshield, an. Aber immer mehr Behörden schlagen Alarm und wollen, dass sich alles schnell weiterentwickelt. *„In Entwicklungsländern hingegen gehört die Cybersicherheit keineswegs zu den Prioritäten der Wasserindustrie. Für diese Länder sind die Herausforderungen andere: Wasserknappheit, Wasseraufbereitung, Effizienz der Verteilungsnetze, Abwasserentsorgung usw. In Bezug auf Verwaltung und Zugang zu Wasser sind nicht alle Länder gleich weit"*, betont **Tarik Zeroual**, Global Account Manager bei Stormshield. Wenn man von Ungleichheit und Knappheit spricht – zum Beispiel ist Wasser im Nahen Osten ein sehr seltenes Gut – spricht man auch von Gier und Konflikten um Wasser und die Kontrolle über die Wasserindustrie. Dieser wirtschaftliche und politische Zustand schafft einen besonders günstigen Nährboden für Cyber-Angriffe, die dann zu einem Druck- und Destabilisierungsmittel von Staat zu Staat werden.

GEOPOLITIK, ÖFFENTLICHE GESUNDHEIT USW., DIE HERAUSFORDERUNGEN HINTER DEN CYBERANGRIFFEN, DIE GEGEN DIE WASSERINFRASTRUKTUR STATTFINDEN

Man könnte beinahe sagen, dass die Wasserindustrie die Probleme zwischen Geräten, die besonders anfällig sind (da sie von alten Betriebssystemen gesteuert werden), den Übergang zum IIoT oder auch die damit verbundenen geopolitischen und strategischen Probleme in Bezug auf die Wasserressource, vervielfacht. Es ist daher unmöglich, dass Wasser und seine kritische Infrastruktur den Cyberangreifern entgehen.

Die heutige Wasserinfrastruktur steht daher unter Cyber-Beschuss, und dies sind *Ransomware-Angriffe*, die scheinbar von den Angreifern bevorzugt werden. Laut der amerikanischen Firma Gray Matter wurden 2019 allein in den USA mehr als 22 Cyberangriffe dieser Art registriert. Bereits im Jahr 2018 war ein Wasserversorger in North Carolina das Ziel eines Cyberangriffs durch Ransomware, während sich der Staat

mitten im Krisenmanagement befand, nachdem er einige Wochen zuvor die verheerenden Folgen des Hurrikans Florence erlitten hatte. Die Angreifer wurden verdächtigt, diesen chaotischen Kontext ausgenutzt zu haben, um Wassersysteme anzugreifen und der Bevölkerung Schaden zuzufügen. Um in das Wassernetz einzudringen, hätten sie zuerst die Emotet-Malware verwendet und dann, sobald sie in den Systemen installiert waren, die Ryuk-Ransomware injiziert – die dafür bekannt ist, dass so insbesondere öffentliche Strukturen angreift – und einen Teil der Daten des Wasserdiensts verschlüsselt.

Im Jahr 2017 hatten Cybersicherheitsforscher der Georgia State University eine neue Form von Malware entwickelt, die Wasser durch Veränderung des Chlorgehalts in den Wasseraufbereitungsanlagen vergiften kann. Um diesen Angriff zu simulieren, übernahmen die Forscher die Kontrolle über die PLC (*Programmable Logic Controllers*) der Anlage. In ihrem Bericht, der diese Simulation nachzeichnet, beschreiben die Forscher die Vorgehensweise, mit der Angreifer die Kontrolle über diese anfälligen PLC übernehmen können. Es gibt zunächst eine erste Erkennungsphase, in der mit dem Internet verbundene PLC (insbesondere über die spezialisierte Suchmaschine Shodan) erkannt und als Einstiegspunkte verwendet werden. Sobald Angreifer sich im System befinden, können sie sich über das Fabriknetzwerk ausbreiten und wichtige Fabrikdaten wie den Zugriff auf SPS-Steuerungen und deren Befehle erfassen. Der letzte Schritt besteht schließlich darin, die dem Wasser zugesetzte Chlormenge zu erhöhen und falsche Messwerte anzuzeigen.

Denn das ist auch eines der Ziele von Cyber-Angriffen auf die Wasserinfrastruktur: strategische Angriffe, die vorangetrieben werden und deren Auswirkungen einen Teil der Bevölkerung eines Landes gefährden können. Und zur Destabilisierung eines ganzen Staates führen. Das Problem der öffentlichen Gesundheit im Zusammenhang mit Wasser ist ein kritisches Thema, mit dem sich Hersteller im Kampf gegen Cyber-Angriffe auseinandersetzen müssen. „*Wenn man Zugriff auf eine Wasserverteilungsstelle bekommt, hat man auch Zugriff auf die Bevölkerung mit dem Risiko erheblicher physischer Schäden. Ein erfolgreicher Cyberangriff auf die Wasserindustrie ist ein Angriff, der ein unmittelbares Risiko darstellen kann*“, warnt Tarik Zeroual.

> *“Ein erfolgreicher Cyberangriff auf die Wasserindustrie ist ein Angriff, der ein unmittelbares Risiko darstellen kann”*
>
> **Tarik Zeroual,** Global Account Manager Stormshield

Über die Arbeit dieser Universität hinaus ist die Änderung der chemischen Behandlung von Wasser mit einem sehr realen Risiko verbunden. Im April letzten Jahres versuchte der Iran angeblich durch Cyberangriffe, diese Operation durchzuführen und damit die Qualität des Wassers zu beeinträchtigen, das dazu gedacht war, einen Teil der israelischen Bevölkerung zu versorgen. Die Angreifer hätten zuerst die Kontrolle über amerikanische Server übernommen, um ihre Spuren zu verwischen, und dann die gezielten Wasserverteilungsnetze angegriffen. Der Angriff war letztendlich erfolglos, aber wenn er im Gegenteil erfolgreich gewesen wäre, wäre der Schaden für die öffentliche Gesundheit erheblich gewesen, mit der wahrscheinlichen Vergiftung eines Teils der Einwohner.

Im Juli letzten Jahres bedauerte Israel zwei neue Angriffe auf seine empfindliche Wasserinfrastruktur. Diesmal wurden nicht städtische Netzwerke ins Visier genommen, sondern Geräte, die für den Agrarsektor verwendet werden. Wenn auch in kleinerem Maßstab bleibt der Iran jedoch im Verdacht, der Ursprung dieser Angriffe zu sein, mit dem Ziel, den Staat Israel zu destabilisieren und politisch zu schwächen. Für diese beiden Versuche hätten die Angreifer erneut amerikanische Server verwendet, um dann die Pumpensteuerungsprogramme zu infizieren.

Im Allgemeinen scheinen diese Cyberangriffe gegen die Wasserinfrastruktur reibungslos durchgeführt zu werden: Sie werden vorweggenommen, vorbereitet und äußerst gut dokumentiert. Die Angreifer wissen also, wie die Systeme funktionieren, auf die sie abzielen; nichts wird dem Zufall überlassen und es wird nichts aus Opportunismus heraus getan. Dies deutet darauf hin, dass die Cyber-Angriffe gegen die Wasserindustrie offenbar von oder für Staaten durchgeführt werden und dass die Gruppen von Angreifern, die sie ausführen, alles andere als Amateure sind. „*Die Angreifer, die Aktionen gegen die Wasserindustrie durchführen, sind organisierte Gruppen – im Allgemeinen ATPs von russischer, chinesischer oder iranischer Herkunft – und sie werden von staatlichen Stellen finanziert oder geleitet*“, gibt Tarik Zeroual an.

Wasser bietet daher die Möglichkeit, groß angelegte Cyber-Angriffe mit einer echten strategischen Dimension durchzuführen. Die Wasserindustriellen müssen sich entsprechend bewaffnen, um die Übernahme ihrer Infrastrukturen zum Zwecke der Cyberkriegsführung vor dem Hintergrund der Geopolitik so weit wie möglich zu begrenzen.

SEGMENTIEREN, UM SICH BESSER ZU SCHÜTZEN: DIE ANTWORT DER WASSERINDUSTRIE

Bei schweren Krankheiten werden starke Heilmittel eingesetzt. Um sich vor Cyberangriffen zu schützen, muss die Wasserindustrie filtern, was von der Außenwelt in ihre Fabriken kommt. Zu diesem Zweck hat der Sektor eine Politik der Segmentierung seiner Standorte eingeführt. Ein wesentlicher Ansatz zum Schutz der Wasserinfrastruktur, zumal er viele Formen annehmen kann. „*Die Wasserindustrie segmentiert jeden ihrer Standorte und kontrolliert die Kommunikation, die diese durchlaufen*“, legt Raphaël Granger aus. Über die Segmentierung der Betriebsstätten hinaus trennt die Wasserindustrie auch die IT-Welt (PCs, Server, Benutzer) von der OT-Welt (Betriebswelt) in diesen Standorten. Diese Segmentierung zielt darauf ab, den operativen Teil im Falle von Angriffen zu isolieren. Schließlich ist es innerhalb des OT-Teils selbst wieder möglich, eine Form der Segmentierung mit einer Trennung zwischen dem Überwachungsteil und dem Ausführungsteil (SPS) zu finden.

Die Hauptakteure im Bereich Cyber, insbesondere Entwickler, unterstützen die Wasserindustrie bei diesem Segmentierungsprozess und durch eine Reihe von Sicherheitsmaßnahmen, die darauf abzielen, die Kapazitäten zur Verhinderung von Cyberangriffen zu stärken. *„Um die Cybersicherheit von Wassernetzen zu gewährleisten, helfen Entwickler den Industriellen in der Branche, die Zuverlässigkeit und Konformität von Netzprotokollen zu überprüfen. Die Idee dahinter ist, durch die Einrichtung insbesondere von industriellen Firewalls sicherzustellen, dass diese Protokolle nicht von einem Angreifer geändert oder angegriffen werden* ", erklärt Raphaël Granger. Für diese Branche ist es daher unerlässlich, über Lösungen zu verfügen, mit denen die Rechtmäßigkeit der von den SPS ausgeführten Befehle überprüft und Systeme eingerichtet werden können, mit denen Fernzugriffe (für Fernwartung, Alarmverwaltung usw.) verwaltet und gesichert werden können.

Die Wasserindustrie organisiert ihre Reaktion auf Cyberangriffe, aber dies ist erst der Anfang. Ab morgen muss der Sektor auf eine neue Herausforderung reagieren: die Ausweitung seiner Sicherheitspolitik auf die gesamte Kette über Fabriken hinaus; und hin zu einem noch fortschrittlicheren IIoT-Ansatz mit von Anfang bis Ende garantierter Sicherheit von Kommunikation und Systemen von der Fabrik bis zum Verbraucher.

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.

Version 1.1 - Copyright Stormshield 2020