tenable.ot™

ANWENDUNGSFALL

ABSICHERUNG VON WASSERVERSORGUNGSANLAGEN

WICHTIGSTE TRENDS

- Die Pandemie hat die Umstellung auf digitales Wassermanagement beschleunigt und zu einer schnellen Einführung von IoT-Technologien geführt, um Echtzeitinformationen über den Status von Wasserbehandlungs- und/oder Wasseraufbereitungsvorgängen zu erhalten.
- Zentralisierte, autonom betriebene Trinkwasseraufbereitungsanlagen ersetzen auf Silos aufbauende Abläufe des Prozessmanagements.
- Entscheidungen in Kläranlagen sind zunehmend automatisiert und Vorgesetzte benötigen ein umfassendes Verständnis sowie Kenntnisse des Systembetriebs, um Vorfällen zuvorzukommen.
- Die Verbreitung von intelligenten Bewässerungs- und Leckerkennungstechnologien führt zu einer automatischen Neuplanung der Bewässerung, einer Optimierung des Wasserverbrauchs und zu Verbesserungen der Umweltverträglichkeit.

ZENTRALE HERAUSFORDERUNGEN

- Wasserbehandlungs- und Wasseraufbereitungsanlagen erfordern Transparenz und Kontext, um die Versorgung angemessen abzusichern.
- Durch IoT-Technologie und IT/OT-Konvergenz neu entstandene Angriffsvektoren zu versperren, ist unerlässlich. Hierzu sind erweiterte Verfahren der Bedrohungserkennung und Berichterstellung notwendig, um Wasserinfrastruktur bereits im Vorfeld etwaiger Schäden abzusichern.
- Schwachstellen müssen schnell identifiziert und basierend auf den geschäftlichen Auswirkungen bewertet werden, damit die schwerwiegendsten Schwachstellen während geplanter Wartungsarbeiten zuerst behoben werden.

HINTERGRUND

Wasseraufbereitungs- und Kläranlagen sind für die darüber versorgte Bevölkerung in Regionen und Gemeinden von kritischer Bedeutung. Für die öffentliche Gesundheit, den Schutz des Ökosystems und die Wirtschaftskraft ist sicheres und sauberes Wasser unverzichtbar. Die Behandlung von Schwarzwasser und Rückgewinnung von Grauwasser ist auch für die Sicherheit der Bevölkerung und für Maßnahmen zum Gewässerschutz wichtig. Parallel dazu tragen neue Entwicklungen dazu bei, dass die ohnehin schon lange Liste von Herausforderungen immer umfangreicher wird. Hierzu zählen Vereinbarungen zur gegenseitigen Hilfeleistung zwischen Behörden, sich verändernde Paradigmen im operativen Bereich und neue Standards zur Einhaltung gesetzlicher Vorschriften wie AWIA. Zur Unterstützung dieser wichtigen Aufgabenbereiche ist abgesicherte Informationstechnologie (IT) und operative Technologie (OT) notwendig.

Um diesen Anforderungen Rechnung zu tragen, werden Abläufe der Wasseraufbereitung und Abwasserbehandlung zunehmend intelligenter, verflochtener und digitalisierter. Folglich müssen Transparenz, Sicherheit und Kontrolle des Netzwerks gewährleistet sein – von der Wasserzufuhr über den Aufbereitungs-/Behandlungsprozess bis hin zum letzten Schritt der Verteilung von sauberem Wasser, der Rückgewinnung von Grauwasser und der endgültigen Ableitung von Schwarzwasser.

Bei der Verbesserung von Abläufen in Wasserwerken werden technologische Fortschritte genutzt, die sich auf erhöhte Interkonnektivität und Automatisierung stützen. Ein Verbundnetz bietet große Effizienzsteigerungen, weist aber auch eine deutlich breitere Angriffsoberfläche auf. Zudem besteht die Möglichkeit, dass sich ein Sicherheitsvorfall einfach von einem Anbieter auf den nächsten ausbreitet. Deshalb zählen industrielle Cyberbedrohungen in der Wasserindustrie zu den bedeutendsten Risiken für die Sicherheit, Zuverlässigkeit und Kontinuität kritischer Betriebsabläufe.

Gängige Protokolle der Wasserindustrie:

- BACnet
- Controlnet
- DNP3
- FINS
- HART
- Profinet
- CIP
- DeviceNet
- Ethernet/IP
- GE-SRTP
- Modbus

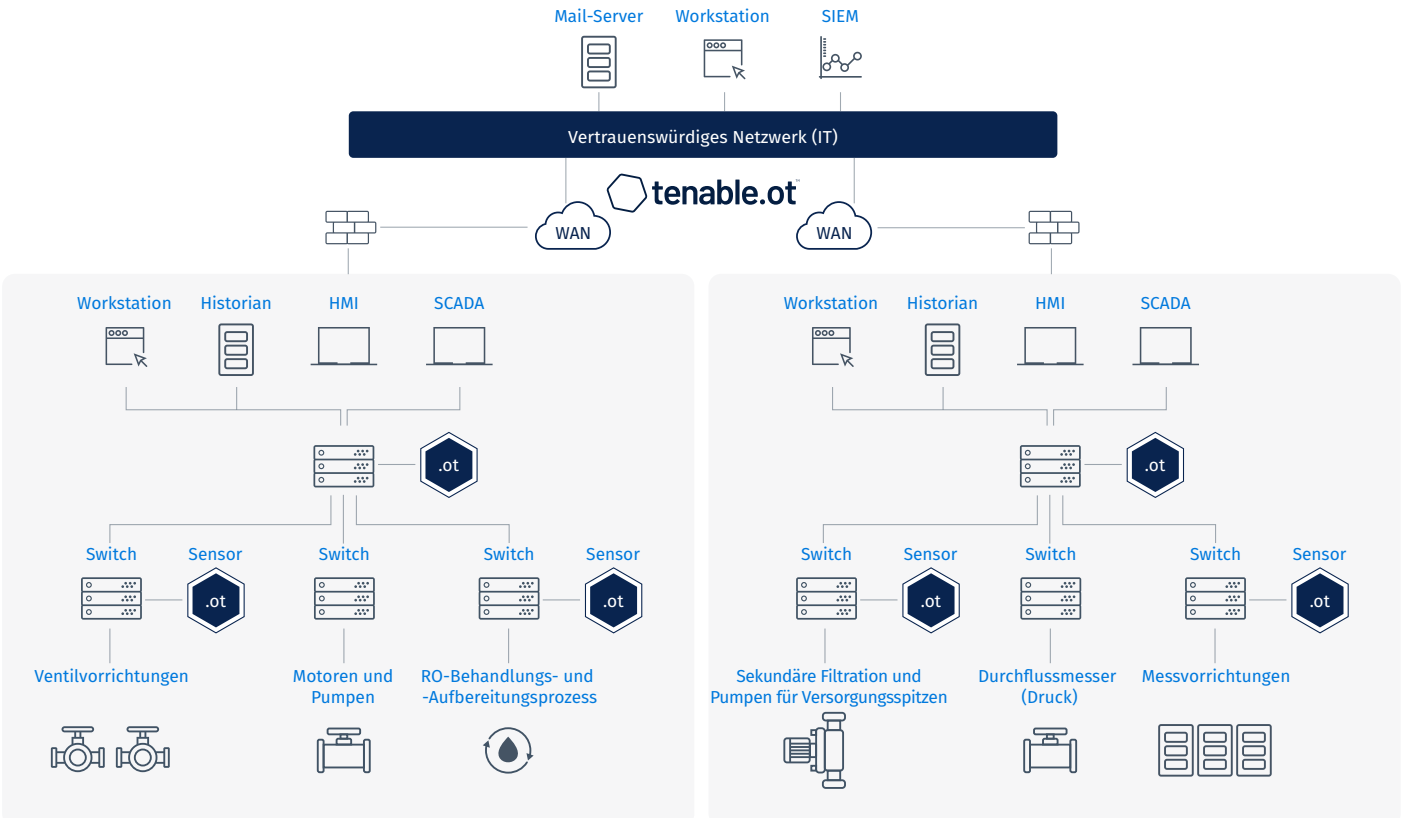
ANATOMIE EINES CYBERANGRIFFS IN DER WASSERVERSORGUNG

1. Anfängliche Infiltration eines Wassernetzes
2. Errichtung eines Brückenkopfes in einem oder mehreren Assets des Netzwerks
3. Beginn der Auskundschaftung zwecks Bestimmung von Zielen, anfälligen Geräten und Schwachpunkten
4. Ausbreitung auf weitere Assets, um in die gewünschten Bereiche zu gelangen
5. Die „letzte Meile" des Angriffs, in der Abläufe der Wasserbehandlung oder -aufbereitung gestört werden

Jüngste Vorfälle

- **2021 –** Angreifer verschafften sich Zugang zu einer Wasseraufbereitungsanlage in Florida. Dabei griffen sie extern über TeamViewer auf das nicht mehr unterstützte Betriebssystem Windows 7 zu. Der Hacker veränderte den Anteil von Natriumhydroxid – also Natronlauge – von 100 ppm auf 11.100 ppm. Glücklicherweise wurde der Vorfall bemerkt und die Einstellung rückgängig gemacht, bevor die Öffentlichkeit betroffen war.
- **2019 –** Im Post Rock Water District in Ellsworth, Kansas kam es zu einem Cybersecurity-Verstoß, als ein ehemaliger Mitarbeiter remote auf einen Computer des Post Rock Water District zugriff, um die Reinigungs- und Desinfektionsverfahren abzuschalten, mit denen das Wasser trinkbar gemacht wird.
- **2017 –** Angreifer nutzten – vermutlich im Auftrag eines Staates – die komplexe Malware namens Triton, um in ein Triconex-Sicherheitssystem von Schneider einzudringen. Diese Sicherheitssysteme werden eingesetzt, um den Betrieb in Nuklearanlagen, Öl- und Gasanlagen, Wasseraufbereitungsanlagen usw. herunterzufahren, wenn gefährliche Bedingungen festgestellt werden.

LOGIK EINES BEREITSTELLUNGS-BEISPIELS: WASSERINDUSTRIE



SYSTEMWEITE TRANSPARENZ

In Wasserversorgungsanlagen gibt es eine Vielzahl von unterschiedlichen industriellen Abläufen. In Trinkwasseraufbereitungsanlagen zählen hierzu die Überwachung der Wasserzufuhr und eine entsprechende erste Wasserförderung, die Filtration und Behandlung sowie die abschließende Verteilung. In Kläranlagen betreffen diese Abläufe die Erfassung, Filtration und Behandlung von Grauwasser zur Wiederverwendung. Bei Schwarzwasser hingegen betreffen sie Absetzbecken, eine hochentwickelte Filtration sowie die abschließende Behandlung, Ableitung und Entsorgung, wodurch es für die Umwelt unschädlich wird.

Jeder einzelne dieser Prozesse erfordert eine komplexe Orchestrierung – und ein Zusammenspiel von IT- und OT-Betrieb. Zahlreiche Unternehmen sind zu konvergenten IT/OT-Umgebungen übergegangen und haben zudem IoT-Technologie eingeführt, um die einzelnen operativen Elemente zu überwachen. Die Einführung von IP-basierten Geräten und der immer seltenere Einsatz von Air-Gaps hat de facto zu neuen Angriffsvektoren in Wasserbetrieben geführt. Hierzu zählt die „laterale Ausbreitung" von Sicherheitsvorfällen, die unter Umständen im IT-Bereich beginnen und sich dann auf den OT-Bereich – oder in umgekehrter Richtung – ausbreiten.

Aus diesem Grund benötigen Sie einen vollständigen und uneingeschränkten Überblick über Ihre konvergente Umgebung. Vollständige 360-Grad-Sichtbarkeit in Ihrer gesamten Infrastruktur stellt sicher, dass keine sicherheitsrelevanten blinden Flecken vorhanden sind, die den Betrieb möglicherweise stören oder gänzlich zum Stillstand bringen können. Sie benötigen Sichtbarkeit auf Netzwerkebene, um verdächtigen oder ungewöhnlichen Datenverkehr zu identifizieren, sowie auf Geräteebene, um infizierte IT- und OT-Geräte ausfindig zu machen.

INVENTARISIERUNG UND VERFOLGUNG VON ASSETS

Wasserwerke verfügen in der Regel über große Infrastrukturen. Zahlreiche unterschiedliche Geräte sind über ein großes Gebiet und mitunter auch über mehrere Netzwerke verteilt. Im Allgemeinen enthalten Netzwerke mehrere Gerätegenerationen sowie eine Vielzahl von Marken und Modellen. Ihre OT-Lösung sollte mehrere Erfassungsmethoden miteinander kombinieren können, um ein aktualisiertes Asset-Bestandsverzeichnis der gesamten verteilten Umgebung anzulegen.

Auch müssen Sie Assets verfolgen können, um Ihr Bestandsverzeichnis stets auf aktuellem Stand zu halten und bei sämtlichen nicht erfassten Änderungen per Warnmeldung benachrichtigt zu werden. Dazu gehört Einblick in alle Gerätetypen, die in Wassernetzen vorhanden sind, wie etwa Pump-, Filtrier-, Ventil-, Misch- und Messvorrichtungen. Zudem sollte Ihre OT-Lösung skalierbar sein, um große Netzwerke mit zahlreichen heterogenen Geräten abzudecken. Vor allem aber sollte sie auch inaktive Geräte berücksichtigen, die nicht regelmäßig über Ihr Netzwerk kommunizieren.

IDENTIFIZIERUNG UND BEWERTUNG VON SCHWACHSTELLEN

Trinkwasserbehandlungsanlagen und Kläranlagen müssen ständig in Betrieb sein. Wenn eine Schwachstelle entdeckt wird, kann der Betrieb nicht ohne Weiteres gestoppt werden, um routinemäßige Wartungsarbeiten durchzuführen oder Patches zu installieren. Dies führt dazu, dass Schwachstellen auf unbestimmte Zeit fortbestehen können und dabei sowohl von bekannten als auch von unbekannten Bedrohungen eine Gefahr ausgeht.

Aus diesem Grund ist es von entscheidender Bedeutung, dass der Zustand und sämtliche Merkmale all Ihrer Geräte genauestens bekannt sind. Dazu gehört auch, den spezifischen Zustand von Geräten exakt mit der verfügbaren Wissensdatenbank zu Schwachstellen abzugleichen, in der damit zusammenhängende Exploits aufgeführt sind. Aufgrund der dynamischen Beschaffenheit von Umgebungen in der Wasserversorgung sollte Ihre OT-Lösung diese Informationen regelmäßig aktualisieren und mit neu aufgedeckten Schwachstellen abgleichen. Eine VPR-Bewertung (Vulnerability Priority Rating) kann Ihnen beispielsweise eine geordnete Liste von Schwachstellen liefern, mit denen Sie sich – ausgehend vom höchsten bis zum niedrigsten Schweregrad – befassen sollten. Das VPR basiert auf zahlreichen Kriterien, wie etwa der CVSS-Bewertung, der Asset-Kritikalität, der Position in Ihrer Umgebung und vielen weiteren Aspekten. Dadurch steht Ihnen eine automatisierte, vollständig geprüfte und nach Priorität geordnete Liste der Schwachstellen zur Verfügung, die Sie beheben sollten, um die für Ihre spezifische Umgebung relevante Cyber Exposure zu senken.

ABSICHERUNG IHRER INFRASTRUKTUR

Um Ereignisse in jeder Phase eines Angriffs identifizieren zu können, sollten Sie Multi-Detection Engines einsetzen, die Folgendes beinhalten:

- Angriffsvektoren, anhand derer Schwachpunkte proaktiv identifiziert werden können, bevor Bedrohungsakteure einen Angriff durchführen; allgemeine Traffic-Zuordnung und Traffic-Visualisierung sowie Identifizierung von riskanten Protokollen, offenen Ports und Schwachstellen, um Risikofaktoren in Ihrer gesamten Infrastruktur zu beseitigen.
- DPI-Engines für dokumentierte und proprietäre Protokolle. Damit werden gegen festgelegte Regeln verstoßende Aktivitäten sowie Aufklärungsereignisse identifiziert – gestützt auf Richtlinien, die Schutz vor bekannten Angriffen bieten.
- Anomalie-Erkennung identifiziert Zero-Day- oder gezielte Angriffe, für die noch keine Signatur vorliegt. Dies kann zur Ermittlung von Traffic-Mustern und Verhaltensweisen genutzt werden, die vom normalen Tagesbetrieb abweichen.
- Bei signaturbasierter Erkennung kommt eine Datenbank wie Suricata zum Einsatz. Als Open-Source-Datenbank ist sie deshalb wertvoll, weil die breitere Security-Community neue Signaturen hinzufügen kann, wovon alle OT-Umgebungen profitieren.
- Die Konfigurationskontrolle verfolgt Änderungen, die von Malware und Benutzern über Ihr Netzwerk oder direkt auf einem Gerät vorgenommen wurden. So wird ein vollständiger Verlauf aller Änderungen bereitgestellt, die im Laufe der Zeit an Gerätekonfigurationen vorgenommen wurden, darunter detailgenaue Informationen zu Kontaktplansegmenten, Diagnosepuffern, Tag-Tabellen und mehr. Administratoren sind damit in der Lage, Backup-Snapshots mit dem „letzten als funktionierend bekannten Zustand" für eine schnellere Wiederherstellung und zur Gewährleistung der Einhaltung von Branchenbestimmungen zu erstellen.

ZUSAMMENFASSUNG

Inzwischen ist weithin bekannt, dass OT-Cybersecurity ein elementarer Bestandteil einer stets zuverlässigen, effizienten und sicheren Umgebung in der Wasserversorgung ist. Lückenlose Transparenz, Sicherheit und Kontrolle über alle Ihre operativen Assets sind zur Eindämmung von Risiken unverzichtbar.

Tenable.ot sorgt für die vollständige Sichtbarkeit von IT- und OT-Assets. Durch die Asset-Bestandsaufnahme wird jedes einzelne Asset in Ihrer Umgebung identifiziert – in Kombination mit einer umfassenden Situationsanalyse bis hin zur Firmware- und Backplane-Ebene. Bei der aktiven Suche nach Bedrohungen kommen proaktive Angriffsvektoren zum Einsatz, mit deren Hilfe Schwachpunkte bereits identifiziert werden, bevor Bedrohungsakteure einen Angriff durchführen. Eine hybride Erkennungs-Engine identifiziert bekannte wie auch unbekannte Bedrohungen, sobald diese auftreten. Im Rahmen des Schwachstellen-Managements werden Schwachstellen mit bekannten Exploits priorisiert, die für Ihre spezifische Umgebung relevant sind. Bei Bedarf identifiziert die Konfigurationskontrolle zu Audit- und Rollback-Zwecken sämtliche Änderungen an Ihrer OT-Infrastruktur und erstellt entsprechende Snapshots. Die flexiblen Bereitstellungsoptionen von Tenable.ot und die Integration mit führenden IT-Sicherheitsanbietern sorgen dafür, dass Infrastrukturen in der Wasserversorgung sicher und mit geringerem Risiko betrieben werden.

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Erfahren Sie mehr über uns auf de.tenable.com.