INDUSTRIE

ÖFFENTLICHE WASSERVERSORGUNG IN EINER METROPOLE

OPTIMIERUNG DER CYBERSICHERHEIT UNTER BERÜCKSICHTIGUNG BETRIEBSBEDINGTER EINSCHRÄNKUNGEN

1.3 millionen
EINWOHNER

60
GEMEINDEN

100
WASSERTÜRME

Immer enger verflochtene Netze

Der Schutz von Trinkwasseranlagen stellt Ballungsräume vor große Herausforderungen. Der Informationsaustausch zwischen Computer- und Betriebsnetzen entwickelt sich zu einem kontinuierlichen Prozess, aber diese Optimierung der Infrastrukturverwaltung bietet auch eine größere Angriffsfläche. Beispielsweise wurde eine US-amerikanische Trinkwasseranlage im März 2016 Opfer eines Hackerangriffs, bei dem böswillige Personen die Menge der chemischen Stoffe im Wasser veränderten. Im April 2020 machte die israelische Regierung eine Reihe von Computerangriffen auf ihre Wasserversorgungs- und Wasseraufbereitungsanlagen öffentlich. Die israelische Behörde für Cybersicherheit forderte alle Mitarbeiter von Unternehmen, die im Energie- und Wassersektor tätig sind, dazu auf, ihre Passwörter für alle mit dem Internet verbundenen Systeme zu ändern.

Kontext

Die Hauptstadt einer großen französischen Region mit rund 60 Gemeinden und mehr als einer Million Einwohner führte eine Ausschreibung zur Rationalisierung der Verwaltung ihres Trinkwassernetzes durch. In den Jahren zuvor oblag die Wasserversorgung drei privaten Versorgungsunternehmen, sodass das Ziel der Ausschreibung nun darin bestand, die Verwaltung nur noch in die Hände eines einzelnen einheitlichen Betreibers zu legen. Über die betriebliche Rationalisierung hinaus wollte die Metropole auch ihre IT-Architektur modernisieren und das Sicherheitsniveau erhöhen.

Die drei bestehenden Betreiber konkurrierten um die Verwaltung der öffentlichen Trinkwasserversorgung im größten Teil der Region, einschließlich der Gewinnung, des Transports, der Speicherung und der Verteilung von Trinkwasser.

Um die Sicherheit ihrer Betriebsnetze zu erhöhen, wünschte die Metropole sich zudem eine Architektur, die mittels der Einrichtung von Firewalls einen unabhängigen Schutz der folgenden Bereiche ermöglichte:

- IT-Büronetzwerke
- Zentrale VPN-Konzentratoren
- Industrielle und sicherheitsrelevante IT
- Remote-Standorte

Gewählte Lösung

Die Ausschreibung wurde durch den führenden Betreiber auf dem französischen Markt gewonnen, der sich an Stormshield wandte, um Unterstützung bei der Sicherung dieser Betriebsumgebung zu erhalten.

Die wichtigsten Funktionen und Prozesse, welche die Stadt von dieser globalen Systemarchitektur erwartete, waren die Steuerung und Filterung der gesamten DPI- Kommunikation (hauptsächlich mittels des Modbus-Protokolls) sowie die Einrichtung einer IPsec-VPN-Lösung zum Schutz der Kommunikation.

Verwaltung von strikten betriebsbedingten Einschränkungen über eine einzige Lösung

In der Folge wurde die Sicherheit des zentralen Standorts durch die Einrichtung von Firewalls zwischen dem Büronetzwerk und den branchenspezifischen Anlagen erhöht. Diese Anlagen verteilen sich auf zwei verschiedene Netzwerke (Sicherheits- und Betriebsnetz), die jeweils durch einen Firewall-Cluster geschützt werden, der die Funktion eines VPN-Konzentrators übernehmen soll. Mittels dieser Architektur können dieselben Anwendungen mit verschiedenen Wassertürmen verbunden werden.

Im Einzelnen wurde ein Cluster aus SN3100-Firewalls ausgewählt, um das Betriebs- und das Sicherheitsnetz zu schützen und mittels einer doppelten Stromversorgung und RAID-Laufwerken einen unterbrechungsfreien Betrieb zu gewährleisten.

Darüber hinaus wurden drei SN710-Firewall-Cluster für die VPN-Konzentratoren (IT-/OT-Kommunikation) implementiert. Durch anpassbare interaktive Berichte erhält der Kunde sofort die wichtigsten Informationen über Aktivitäten und sicherheitsrelevante Ereignisse im Netzwerk. Auf der Grundlage mehrerer verhaltensbasierter Erkennungsmethoden bietet die direkt in den Produktkern integrierte „*Intrusion Prevention Engine*“ (IPS) einen effektiven Schutz vor Zero-Day-Bedrohungen, ohne die Netzleistung zu beeinträchtigen.

Schließlich wurden 100 Wassertürme einzeln in zwei Clustern (einem für das Sicherheits- und einem für das Betriebsnetz) mit robusten SNi40-Firewalls ausgestattet, um den Datenfluss zwischen den verschiedenen Standorten und Anwendungen zu schützen. Diese Firewalls wurden speziell für den Schutz von SPS (speicherprogrammierbarer Steuerung) entwickelt und ermöglichen auch den Aufbau von IPsec-VPN-Tunneln zu zentralen Standorten.

Das von Stormshield vorgeschlagene Branchenangebot entsprach perfekt den verschiedenen Bedürfnissen des Betreibers. Darüber hinaus ermöglichte die Anpassungsfähigkeit der vorgeschlagenen Lösung sowohl die Verwaltung von Standardstandorten als auch von Umgebungen mit strikten betriebsbedingten Einschränkungen (Temperatur, Luftfeuchtigkeit, Tragschienen, industrielle Stromversorgung). Dies geschieht mit einer einzigen Firmware, die in der gesamten Stormshield-Network-Security-Familie eingesetzt wird, und einer einzigen Verwaltungskonsole für alle Firewalls, dem „*Stormshield Management Center*“. Nicht zuletzt war der Kunde über das Preis-Leistungs-Verhältnis hinaus und unabhängig von den Standardfunktionen (VPN, Segmentierung etc.) sehr überzeugt von der IPS-Funktionalität der Industrieprotokolle. Sie verfügen über die beste Granularität auf dem Markt und ermöglichen eine Weiterentwicklung der Sicherheit dieser sensiblen Systeme parallel zur Modernisierung der Infrastruktur.

Ein auf komplexe Industrieumgebungen zugeschnittenes Serviceangebot

Im Hinblick auf die Wartung und den Betrieb sah der Kunde sich mit Problemen hinsichtlich der Zugänglichkeit und der Sensibilität bestimmter Standorte konfrontiert, um die Verfügbarkeit des Services für die Benutzer zu gewährleisten. Um diesen Einschränkungen entgegenzuwirken, haben Stormshield und der ausgewählte Betreiber ein angepasstes Begleitsystem implementiert, das Folgendes ermöglicht:

- Die Umsetzung eines Verfahrens, mit dem technische Mitarbeiter ausgefallene Firewalls auch ohne Netzwerk- oder Sicherheitskenntnisse austauschen und Standorte wieder in den Betriebsmodus mit dem richtigen Sicherheitsniveau versetzen können
- Eine Aktivierung des Sicherheitsmodus (Bypass) für 5 % der Standorte, die nicht mit einem Cluster, sondern mit einer einzelnen Standalone-Firewall ausgestattet sind. Dies geschieht, um die Verfügbarkeit und Betriebssicherheit von Industriesystemen anstelle von IT-Sicherheit zu priorisieren.
- Ein Portfolio aus Professional Services, um die Metropole bei der Rationalisierung der Konfiguration an den ersten Pilotstandorten zu begleiten.

Das gesamte Projekt und seine Implementierung wurden völlig reibungslos und in kürzester Zeit durchgeführt, was auf das starke Engagement und die Zusammenarbeit zwischen dem Betreiber und dem Editor zurückzuführen ist. Der Endkunde schätzte auch die Umsetzung dedizierter Verfahren zur Erfüllung der fachlichen Anforderungen in diesem Branchenkontext.

Die Geschäftsbeziehung besteht fort, denn Stormshield hat noch weitere Projekte und Ausschreibungen an der Seite dieses Betreibers durchgeführt. So zieht er Stormshield auch intern im Rahmen der Modernisierung seines Geschäfts und der Anpassung seiner Angebote bezüglich IT-/OT-Sicherheit zurate. Dieses Thema gewinnt in Bezug auf kritische und sensible Infrastrukturen, in denen Cyberrisiken schwerwiegende wirtschaftliche, ökologische und menschliche Folgen haben können, immer mehr an Bedeutung.