txOne networks

Customer Story

Stabile OT-Sicherheit: Weshalb sich die August Storck KG für die Sicherheitslösungen von TXOne Networks entschieden hat.

Um Süßwaren höchster Güte herzustellen, ist heutzutage auch ein durchdachter und umfangreicher Schutz der Produktionsumgebung auf digitaler Ebene notwendig. Die vernetzten Maschinen müssen gegen Hacker und Malware geschützt werden. Aus diesem Grund legt die August Storck KG großen Wert auf ihre Sicherheit im Bereich Operational Technology (OT).

STORCK
Part of Your World

Es berichteten:
Alois Ahlrichs, CISO der August Storck KG und Stephan Jochmann, Leiter der Elektrotechnik der August Storck KG

Die Ausgangslage

Die August Storck KG stellt erfolgreich hochwertige Süßwaren her. Das Unternehmen ist bis heute in Familienbesitz und gehört mittlerweile zu den größten Süßwarenherstellern der Welt. Markenprodukte von Storck werden in über 100 Ländern weltweit geliefert. Die Produktion erfolgt bei aller Internationalität weiterhin in Deutschland. Vier Produktionsstandorte mit insgesamt über 8.000 Mitarbeitern führt das Unternehmen mit Sitz in Berlin. Das technische Herz schlägt am Heimatstandort Halle in Ostwestfalen: Dort werden neue Konzepte entwickelt und auf alle anderen Standorte ausgerollt.

Um Produktionsausfälle zu vermeiden, ist der reibungslose Betrieb der Maschinen in den Produktionshallen unerlässlich. Viele dieser Maschinen sind aus verschiedenen Gründen miteinander vernetzt, wodurch ihre OT-Sicherheit besonders wichtig wird.

Hinzu kommt die wachsende IT-OT-Konvergenz, also die Überschneidung von Büro-IT und Produktions-OT. Eine wirksame OT-Abwehrstrategie erfordert deshalb, diese Grenze abzusichern und die Netzwerke durch Segmentierung strikt voneinander zu trennen.

Die Priorität dafür lag vor allem bei einer für die OT geeigneten Lösung, welche hohe Sicherheit ohne zunehmende Komplexität und zusätzlichen Betriebsaufwand bietet. Zur Minimierung des Sicherheitsrisikos innerhalb der Produktion, war eine asset-zentrische OT-Sicherheitsstrategie unerlässlich. Dies beinhaltet unter anderem Anforderungen zum Asset und Vulnerability Management sowie Incident Response, um neben der Produktionsverfügbarkeit auch den gesetzlichen Regularien gerecht zu werden.

Der Umstieg

Bei Storck wechselte man von einem klassischen Anti-Viren-Anbieter zu dem OT-Spezialisten TXOne Networks, dem Marktführer von OT-nativen Sicherheitslösungen. Der Kontakt kam über das deutsche Systemhaus pco GmbH & Co. KG zustande. Nach einem Proof of Concept im August 2021, startete man im Januar 2022 mit Stellar zum Schutz der Industrie-Computer an allen Standorten durch. Relativ zeitnah konnten bereits hunderte Agenten ausgerollt werden, ohne laufende Produktionsanwendungen (ICS Applications) zu beeinträchtigen. Es wurden keine umfangreichen Ausnahmen benötigt, sodass man sich direkt zukünftigen Funktionen widmen konnte. Dadurch entstand neben der lokalen Betreuung auch ein intensiver Austausch mit der Entwicklung in Taipeh (Taiwan), um Weiterentwicklungen direkt in den laufenden Betrieb zu überführen sowie mithilfe des Supports die Lösung bestmöglich zu integrieren. Dies ist auch einer der Gründe, warum Storck auch stets weitere Lösungen des Portfolios evaluiert, um Synergie-Effekte durch die Korrelation von Informationen zu erzielen, welche eine gesamtheitliche Sicht auf die OT-Sicherheitslandschaft ermöglicht.

Das Ergebnis

Federführend ist bei Storck die Abteilung Industrial IT innerhalb der zentralen Technik für die Umsetzung des Projekts und den Schutz von mehr als tausend Endpunkten verantwortlich. Den Fachleuten fällt ihre Aufgabe seit der Einführung von TXOne wesentlich leichter als zuvor, da die Komplexität enorm reduziert und parallel neben der Sichtbarkeit auch die Sicherheit der Vorgänge auf den Endpunkten erhöht wurde. Die Unterstützung von Alt- (Legacy-) und Neu-Systemen ermöglicht eine optimale Absicherung der heterogenen OT-Umgebung, was eine generelle Herausforderung innerhalb der OT ist, insbesondere durch lange Lebenszyklen einzelner Anlagen. TXOne unterstützt beispielsweise von Windows 2000 aufwärts und liefert seinen Support noch weit über 5 Jahre hinaus. Zuletzt stellt Stellar als Cyber-Physical-System-Detection-and-Response (CPSDR) Lösung umfangreiche Funktionen zur Anomalie-Erkennung und -Prävention zur Verfügung, welche als Basisinformationen an ein Security Operations Center (SOC) weitergeleitet werden können.

Eine weitere, nicht nur bei Storck bestehende Herausforderung, liegt in der Absicherung von zugekauften Anlagen, wie z. B. Package Units. Für dieses Szenario werden Lösungen aus dem TXOne Edge Portfolio evaluiert, die eine einfache Segmentierung und das Abschirmen von Verwundbarkeiten (Vulnerabilities) auf einfache Weise ermöglicht. Tiefes Verständnis der OT-Protokolle gilt dabei als selbstverständlich.

Das gesamte Portfolio der TXOne liefert dabei wichtige Asset-Informationen zur Beurteilung von Verwundbarkeiten und Risiken, welche innerhalb der SageOne korreliert werden können.

Über TXOne Networks

TXOne Networks bietet Cybersicherheitslösungen, die mithilfe der Zero Trust OT-Methodik die Zuverlässigkeit und Sicherheit von industriellen Steuerungssystemen und betrieblichen Technologieumgebungen gewährleisten. TXOne Networks arbeitet mit führenden Herstellern und Betreibern kritischer Infrastrukturen zusammen, um praktische und leicht umsetzbare Ansätze für die Cyberverteidigung zu entwickeln. Das Unternehmen bietet sowohl netzwerk- als auch endpunktorientierte Produkte an, um das OT-Netzwerk und kritische Geräte in Echtzeit und in der Tiefe zu sichern. Mehr erfahren über www.txone.com.