txOne networks

Customer Story

Abgesicherte Herstellung von Sensoren :

Sensorikhersteller erhöht seine OT-Security mit TXOne Networks

Ausfälle und Stillstände verhindern: Das gehört zu den Kernaufgaben der Fachleute für Operational Technology (OT). Bislang war dies zwar eine schwierige, aber mit genügend Personal, welches über entsprechende Erfahrung verfügt, stemmbare Aufgabe innerhalb eines modernen Maschinenparks. Die Vernetzung von IT und OT, wodurch Maschinen aller Art nun vernetzt und oft sogar an das Internet angeschlossen wurden, hat diese Aufgabe zu einer gewaltigen Herausforderung entwickelt. Die Komplexität der Verbindungsströme zu überblicken – in jedem OT-System – ist aufgrund zunehmender Angriffe – von innen und außen kommend – ohne technische und organisatorische Hilfsmittel unmöglich geworden.

Bei einem weltweit führenden Hersteller von Sensoren und angeschlossenen Komponenten sollte eine OT-Security Lösung eingeführt werden. Produkte werden unter anderem in der industriellen Kommunikation, bei der Anzeigenbeleuchtung und Spannungsversorgung eingesetzt. Die Anwendungsfälle ziehen sich durch große Branchen, wie die Automobilindustrie, Erneuerbare Energien, Logistik, oder Schiffsautomation.

Der Maschinenpark aus Sicht der OT ist durch die unterschiedlichen Herstellungsprozesse und Anwendungsfelder hoch diversifiziert ausgestattet worden, denn teilweise handelt es sich um Anlagen von Marktführern, teilweise handelt es sich um selbstgefertigte Maschinen für spezielle Sensoren. Letztere werden in einer eigenen Abteilung für den Sondermaschinenbau hergestellt. Dies umfasst sowohl einfache Maschinen als auch eigene Roboter oder eine Produktionsstraße.

Die Ausgangssituation

Die zentrale Sicherheitsrichtlinie verlangte vom Unternehmen bei der Nutzung von Netzwerken und Cloud-Umgebungen, dass auf allen Geräten mit Prozessoren ein Anti-Viren-Scanner laufen muss. In der IT-Sicherheit setzte das Unternehmen bereits einen Hersteller flächendeckend für die Endpoint Security ein. Auch in der Produktion gab es bereits mehrere AV-Lösungen, welche jedoch vom Softwarehersteller nicht mehr unterstützt wurden und daher die Compliance Anforderungen nicht erfüllen konnten. Die aktuellen Lösungen der Anbieter waren außerdem klassische SaaS-Lösungen und konnten daher nicht zur Erfüllung der Richtlinie genutzt werden. Infolgedessen wurde der Entschluss gefasst, nach einer neuen konsolidierten Lösung zu suchen, welche flächendeckend eingesetzt werden kann. Eine der größten Herausforderungen hierbei und der Hauptgrund, weshalb sich für eine OT-native Lösung entschieden wurde ist die Heterogenität von Produktions-Infrastrukturen. Veraltete Betriebssysteme, Latenzempfindlichkeit und der Fokus

auf Verfügbarkeit und damit Ausfallsicherheit spielen in OT-Umgebungen eine große Rolle.

Ein erster Kontakt zwischen dem Unternehmen und TXOne Networks kam im April 2022 zu Stande, damals wurde die OT-Security Abteilung gerade aufgebaut und sollte die IT-Sicherheitsabteilung, welche ein zentrales SOC betreibt, ergänzen.

Um die OT spezifischen Herausforderungen zu erfüllen, war es für die Beteiligten selbstverständlich, dass die Abteilung ein Produkt benötigte, das genau auf die OT-Umgebung und ihre Anforderungen ausgerichtet ist und entschied sich für einen Test der von TXOne Networks bereitgestellten Endpoint Security Lösung.

Lösungsansatz: OT-Endpoint-Sicherheit

Zunächst wurde die Lösung ausgiebig getestet und auf einigen Labor Systemen, später aber auch auf produktiver Infrastruktur installiert. Die wichtigsten Kriterien im Test waren unter anderem eine Unterstützung von Windows 2000/Windows XP (mit und ohne Service Packs) sowie neueren Betriebssystemen, ein geringer Ressourcenverbrauch (CPU/RAM) und die einfache Verwaltung der Agenten über eine zentrale Konsole (Agenten und Signatur Updates, Policy Handling etc.). Die Unterstützung der Betriebssysteme war bereits im Vorfeld bekannt, bei dem Ressourcenverbrauch sowie der Administration überraschte die Lösung von TXOne jedoch positiv. Auf Systemen, welche extrem wenig Ressourcen zur Verfügung hatten, lief die Endpoint Security ohne das Systemverhalten zu ändern und durch die sowohl zentrale als auch dezentrale Verwaltbarkeit der Agenten an den Maschinen war ein sehr komfortables arbeiten möglich.

Nachdem das Endpoint-Produkt von TXOne erfolgreich getestet wurde, entschied sich die OT-Security Abteilung ab Oktober 2022 für die Ablösung der bestehenden Sicherheitsprodukte.

Der Umstieg war bis Ende des Jahres erledigt und inzwischen läuft der Scanner auf einer Vielzahl von OT-Geräten.

Die Sensoren-Herstellung wird über eine Produktions-Cloud von Microsoft Azure organisiert. Hier werden die Daten unter anderem mit SAP verarbeitet. Darauf greifen alle Maschinen und Anlagen zu und legen wiederum ihre Produktionsdaten ab. Bereits nach wenigen Monaten machte sich der Umstieg durch eine bessere Verwaltung bemerkbar. Die Warnmeldungen der OT werden über Syslog Forwarding verschickt, laufen im SOC auf und, falls sie eine gewisse Kritikalität erreichen, an das OT-Security Team weitergeleitet. Die meisten Events werden also zunächst von den IT-Security-Experten analysiert, geprüft und erst nach der Filterung an die OT-Kollegen verschickt. Die OT-Security Spezialisten schauen sich diese dann genauer an und entscheiden über die weiteren Schritte. Teilweise erfolgt dies über das Management-Interface, teilweise gehen sie aber auch direkt in die Produktionshallen und untersuchen die betroffenen Maschinen und Anlagen direkt vor Ort. Finden sie etwas Auffälliges oder aber sogar Verstöße gegen die Firmen-Compliance-Richtlinien, ziehen sie die nötigen Konsequenzen, um die Sicherheit der gesamten Produktionsumgebung zu gewährleisten.

Das Ergebnis

Bislang lautete die Herausforderung, dass die Vorgängerlösungen aufgrund des Alters der Software sowie dem nicht mehr vorhandenen Support der Softwarehersteller auf den Produktionsmaschinen keine Sicherheit brachte und die Compliance Richtlinien nicht erfüllen konnte. Dies konnte durch TXOne einfach und geschickt gelöst, die Systeme abgesichert und die Compliance erfüllt werden. Die Erwartungshaltung war, dass die OT-Security Spezialisten des Unternehmens auf allen Systemen (neu und alt) mehr Einsicht in ihre OT bekommen und genauer nachvollziehen können, was auf den einzelnen Geräten, neben den üblichen Produktionsprozessen, passiert, welche sich klar erfüllt hat. Die Meldungen, die aus dem SOC an die OT-Security herangetragen werden, lassen sich nun besser nachvollziehen. Darüber hinaus hat sich der Detailgrad erhöht, was die Bewertung der Kritikalität vereinfacht. Auf diese Weise war es für das OT-Security Team möglich, dass gesteckte Ziel zu erreichen und die Herausforderung, nämlich eine vernetzte Produktionsumgebung vollständig abzusichern, zu meistern.

Über TXOne Networks

TXOne Networks bietet Cybersicherheits-Lösungen, die mithilfe der OT Zero Trust-Methode die Zuverlässigkeit und Sicherheit von industriellen Steuerungssystemen und OT-basierten Produktionsumgebungen gewährleisten. TXOne Networks arbeitet sowohl mit führenden Produktionsunternehmen als auch mit Betreibern kritischer Infrastrukturen zusammen, um praktische, betriebsfreundliche Ansätze für die Cyberabwehr zu entwickeln. TXOne Networks bietet dank seiner Defense-in-Depth-Methode sowohl netzwerk- als auch endpunktbasierte Produkte zur Absicherung von OT-Netzwerken und betriebskritischen Endgeräten in Echtzeit. Mehr erfahren über www.txone.com.