



MINERALÖLVERBUNDELEITUNG GMBH SCHWEDT

Resiliente Sicherheitsarchitekturen für kritische Infrastrukturen

↳ Zentrale Transparenz und Angriffserkennung über IT und OT hinweg

AUF EINEN BLICK

Aufgabe

Aufbau einer zentralen Plattform zur Angriffserkennung gemäß den Anforderungen des IT-Sicherheitsgesetzes 2.0 einschließlich Implementierung eines Security Information and Event Management Systems, Integration heterogener IT- und OT-Datenquellen sowie Entwicklung individueller Erkennungsmechanismen für kritische Infrastrukturen ...

ÜBER MVL MINERALÖLVERBUNDELEITUNG GMBH SCHWEDT

Die Mineralölverbundleitung GmbH Schwedt betreibt eine der zentralen Rohöltransportleitungen Deutschlands und übernimmt eine wichtige Aufgabe für die Versorgung bedeutender Raffineriestandorte. Als Betreiber kritischer Infrastruktur stehen höchste Anforderungen an Verfügbarkeit, Betriebssicherheit und Informationssicherheit im Mittelpunkt. Der sichere und zuverlässige Betrieb der technischen Infrastruktur bildet die Grundlage für eine stabile Energieversorgung und macht moderne Cyber Security zu einem wesentlichen Bestandteil der Unternehmensstrategie.

HERAUSFORDERUNG

Mit den steigenden regulatorischen Anforderungen des IT-Sicherheitsgesetzes 2.0 musste die bestehende Sicherheitsarchitektur umfassend erweitert werden. Ziel war der Aufbau eines leistungsfähigen Systems zur Angriffserkennung, das sowohl klassische IT-Systeme als auch industrielle OT-Komponenten zentral überwacht und sicherheitsrelevante Ereignisse automatisiert analysiert.

Die Herausforderung bestand dabei nicht nur in der Vielzahl unterschiedlichster Datenquellen, sondern insbesondere in der komplexen Infrastruktur eines KRITIS-Betreibers. Active Directory, Netzwerkkomponenten, Firewalls, Endpoint Security Lösungen und industrielle Steuerungssysteme mussten über verschiedene Netzwerksegmente hinweg sicher integriert werden.

...

Systeme & Software

- Splunk Enterprise
- Splunk Enterprise Security
- HPE ProLiant DL360 Gen11
- Active Directory
- Netzwerk- und Firewall-Systeme
- Endpoint Detection and Response
- OT-Systeme und -Steuerungstechnik

Vorteile

- Erfüllung regulatorischer Anforderungen nach IT-SiG 2.0
- zentrale Transparenz über IT- und OT-Sicherheitsereignisse
- Frühzeitige Erkennung komplexer Cyberangriffe
- individuell entwickelte Detektionsmechanismen

Besonders anspruchsvoll war die Integration der OT-Systeme. Für zahlreiche industrielle Datenquellen existierten keine standardisierten Schnittstellen oder fertigen Parser, sodass individuelle Lösungen entwickelt werden mussten. Darüber hinaus sollten sämtliche Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik nachhaltig erfüllt und zukünftige Audits optimal vorbereitet werden.

LÖSUNG

Gemeinsam mit SVA wurde eine moderne Plattform zur Angriffserkennung auf Basis von Splunk Enterprise und Splunk Enterprise Security aufgebaut. Nach der Installation der Infrastruktur erfolgte zunächst die Identifikation sämtlicher sicherheitsrelevanter Datenquellen innerhalb der IT- und OT-Landschaft.

Über speziell entwickelte Forwarding-Konzepte konnten auch Systeme aus streng voneinander getrennten Netzwerksegmenten sicher angebunden werden. Die eingehenden Logdaten werden zentral gesammelt, normalisiert, korreliert und nahezu in Echtzeit ausgewertet.

Für OT-spezifische Systeme entwickelte SVA individuelle Parser und Normalisierungsmechanismen, da hierfür keine Standardlösungen verfügbar waren. Auf dieser Grundlage entstand eine einheitliche Datenbasis für die Sicherheitsanalyse sämtlicher Unternehmensbereiche.

Gemeinsam mit dem SOC by SVA wurden darüber hinaus maßgeschneiderte Detection Use Cases entwickelt, die speziell auf die Anforderungen der industriellen Infrastruktur zugeschnitten sind. Dadurch lassen sich komplexe Angriffsmuster, Anomalien sowie potenzielle Insider-Bedrohungen deutlich früher erkennen und bewerten.

Ein weiterer Schwerpunkt lag auf dem Wissenstransfer. Durch intensive Workshops und praxisnahe Schulungen wurden die Mitarbeitenden in die Lage versetzt, Splunk Enterprise Security eigenständig zu bedienen und auch regulatorische Fragestellungen während BSI-Audits sicher beantworten zu können.

SVA begleitete das Projekt dabei ganzheitlich von der ersten Beratung über die Architektur und Implementierung bis hin zur Schulung und kontinuierlichen Weiterentwicklung der Sicherheitsplattform.

ERFOLGREICHES FAZIT

Mit der Einführung einer modernen Splunk Plattform verfügt der Betreiber heute über ein zentrales Security Monitoring für seine gesamte IT- und OT-Infrastruktur. Sicherheitsereignisse können wesentlich schneller erkannt, bewertet und analysiert werden. Gleichzeitig wurde eine belastbare Grundlage geschaffen, um regulatorische Anforderungen nachhaltig zu erfüllen und zukünftige Erweiterungen flexibel umzusetzen.

Durch die Kombination aus technischer Expertise im Bereich Splunk, langjähriger Erfahrung im KRITIS-Umfeld sowie umfassendem Know-how im Bereich Operational Technology entstand eine Lösung, die weit über die reine Einführung eines SIEM-Systems hinausgeht. Sie bildet heute die Grundlage für ein modernes, kontinuierlich weiterentwickeltes Security Monitoring und stärkt nachhaltig die Cyber Resilience des Unternehmens.

KONTAKT

SVA System Vertrieb
Alexander GmbH
Borsigstraße 26
65205 Wiesbaden
Tel. +49 6122 536-0
mail@sva.de