T Security

OT Security

Umfassende OT-IT Infrastruktur Security für effektiven Schutz gegen Cybergefahren

Wachsende Herausforderungen für OT Security

Mit vermehrter Konnektivität und zunehmender IT-Integration ist die Zahl der Sicherheitsrisiken für Operational Technology (OT) und Industrial Control Systems (ICS) Umgebungen rapide angestiegen – was die Gefahr von Downtimes, Unterbrechungen in der Supply Chain, Produktionsausfällen, Rechtsstreitigkeiten und weiteren Problemen mit sich bringt.

Zu den häufig auftretenden OT-Sicherheitsrisiken zählen:

- **Advanced Persistent Threats (APT):** Cyberbedrohungen dieser Kategorie sind sorgfältig geplante Angriffe, die sich über längere Zeit im System verstecken können, bevor sie aktiv werden.
- **Ransomware:** Ransomware-Angriffe stellen weiterhin eine erhebliche Bedrohung für OT Betriebe dar. In 40 % der Fälle werden Daten erfolgreich verschlüsselt, wobei die durchschnittlichen Wiederherstellungskosten $ 1,3 Millionen erreichen.*
- **KI-basierte Cyberangriffe:** KI-basierte Phishing-Kampagnen und Attacken auf die gesamte Supply Chain sowie IoT (Internet der Dinge) Malware-Angriffe können von Cyberkriminellen immer präziser und in immer größerem Umfang durchgeführt werden.
- **Zero-Day Schwachstellen:** Angreifer nutzen Systemschwachstellen, die noch nicht behoben werden konnten – was die Früherkennung solcher Sicherheitslecks unmöglich macht.
- **Unsichere Remote-Verbindungen:** Die zunehmende Nutzung von Cloud-Technologien und steigende Vernetzung erhöht auch die Zahl der Risiken, die durch unautorisierte oder unsichere Remote-Verbindungen zu OT-Systemen entstehen.

*The State of Ransomware in Manufacturing and Production Report, 2025

Zu den oben genannten Cyberbedrohungen kommen auch vermehrt Risiken entlang der Supply Chain. Etwa durch die Integration von Drittanbietersystemen, Gefahren, die durch den direkten Zugriff von Lieferanten auf kritische Infrastruktur entstehen sowie veraltete Software. Der damit verbundenen möglichen Eintrittstore für Hacker und andere Gefahren sind sich Organisationen noch gar nicht bewusst.

Abgesehen von organisatorischen Risiken und Verlusten können Angriffe auf OT- Systeme nicht nur eine Bedrohung für die Sicherheit der Mitarbeitenden, sondern auch für die Umwelt und die Öffentlichkeit darstellen. Um diese Risiken zu minimieren, benötigen Unternehmen moderne Sicherheitslösungen.

Cybergefahren besser identifizieren und abwehren

T Security bietet eine 360° Security Lösung, die die komplette IT-Landschaft eines Industriebetriebs abdeckt: Netzwerke, Endpoints, Datensicherheit, Cloud Computing und Produktionstechnologie. KI-basierte Managed Cyber Defense ermöglicht die Echtzeiterkennung von Cyberbedrohungen und reduziert die Anzahl von Fehlalarmen, sodass sich das IT-Security Team auf echte Cyberattacken konzentrieren kann. Darüber hinaus überwacht das Security Operations Center (SOC) Ihre Systeme rund um die Uhr, um Sicherheitsrisiken möglichst früh erkennen und eindämmen zu können.

Wir bieten einen mehrstufigen SOC-Ansatz, um:

- alle sicherheitsrelevanten Prozesse vernetzter IT- und OT-Systeme kontinuierlich zu überwachen
- Sicherheitsvorfälle in Echtzeit zu erkennen und die aktuelle Bedrohungslage sofort melden zu können
- die Cyber-Resilienz Ihrer Systeme zu stärken, um den kontinuierlichen Betrieb Ihrer IT-Systeme und Produktion zu gewährleisten
- ein ganzheitliches End-to-End Sicherheitskonzept zu etablieren, das isolierte „Security Silos“ vermeidet und eine höhere Transparenz sowie einen besseren Schutz ermöglicht

Diese Ziele erreichen wir durch Reaktion auf Sicherheitsalarme rund um die Uhr, die Koordination von Abwehrmaßnahmen, umfassendes Reporting, Gefahrenbewusstsein und Administration der Plattformen. Zusätzlich zu unseren Managed Cyber Defense Services unterstützen wir Sie mit OT Security Assessment, Mikrosegmentierung und SASE bei der weiteren Verbesserung Ihrer OT Security.

OT Security Assessment

Der Service schafft Transparenz in industriellen Umgebungen, indem er Anlagen und Systeme (Assets), Schwachstellen, Netzwerkrisiken sowie ungewöhnliche Aktivitäten identifiziert. Durch die Bewertung des Sicherheitsreifegrads und das Aufzeigen kritischer Sicherheitslücken können Unternehmen Verbesserungsmaßnahmen gezielt priorisieren, Cyberrisiken reduzieren und ihre operative Widerstandsfähigkeit nachhaltig stärken.

Mikrosegmentierung

OT-IT Netzwerke können in Segmente unterteilt werden, um Angriffsflächen zu reduzieren und Sicherheitslecks einfacher unter Kontrolle zu halten. Netzwerke mit kritischer Infrastruktur können durch zusätzliche Sicherheitsmaßnahmen geschützt werden, die gezielt auf die entsprechenden Netzwerksegmente angewendet werden.

Secure Access Service Edge (SASE)

SASE ermöglicht eine starke OT-Sicherheit, indem Netzwerk- und Sicherheitsfunktionen in einer einheitlichen Cloud-nativen Plattform vereint werden. Durch zentrale Richtlinienverwaltung, Zero-Trust-Zugriffe und durchgängige Transparenz reduziert SASE die Komplexität, verbessert den Schutz vor sich ständig weiterentwickelnden Bedrohungen und gewährleistet eine sichere, skalierbare Konnektivität für verteilte Nutzer, Standorte und industrielle Umgebungen.

Ein ganzheitlicher Ansatz für Ihre OT Security

Beratung

Zu Beginn erfolgt eine gründliche Überprüfung der Integration und des Status der OT-IT Security Ihres Unternehmens, um mögliche Schwachstellen und Sicherheitsrisiken aufzudecken.

Das ermöglicht uns, ein vollständiges Verzeichnis der vorhandenen OT-IT Assets zu erstellen – und somit die ideale Sicherheitslösung zu finden. Zusätzlich zu einem Gap Assessment enthält unser OT-Security Paket auch ein Maturity-Mapping, das Erstellen einer Cyber Security Roadmap und die Risikoplanung.

Implementierung

Anhand der Ergebnisse des Assessments werden unsere OT-Security Services entsprechend den Bedürfnissen und Prioritäten Ihrer Organisation in die IT-Infrastruktur des Unternehmens integriert.

Managed Services

T Security verfügt weltweit über SOCs mit den Möglichkeiten für SIEM[1], SOAR[2] und XDR[3]. Unsere Sicherheitsexpert:innen verstehen sich als Ergänzung Ihres Inhouse-Security-Team.

Ihre OT-IT Netzwerke werden rund um die Uhr überwacht, um Auffälligkeiten und potenzielle Bedrohung in Echtzeit erkennen zu können. Unsere SOC-Teams sind daher nicht nur für die Identifizierung, sondern auch für die Abwehr von Cyberbedrohungen zuständig.

[1] *SIEM: Security Information and Event Management*
[2] *SOAR: Security Orchestration Automation Response*
[3] *XDR: Extended Detection & Response*

Vorteile für Industriebetriebe

- **Schutz vor finanziellen Schäden:** Reduzieren Sie die Auswirkungen von Cyberangriffen, Sicherheitsvorfälle und Datenverletzungen.
- **Höhere Betriebssicherheit:** Minimieren Sie operative Risiken und schützen Sie Ihre kritischen Produktions- und Infrastrukturanlagen.
- **Geschäftskontinuität:** Gewährleisten Sie einen störungsfreien Betrieb und eine schnelle Wiederaufnahme der Prozesse nach Sicherheitsvorfällen.
- **Stärkere Unternehmensresilienz:** Erhöhte Widerstandsfähigkeit Ihrer OT-Umgebung gegenüber komplexen und schwerwiegenden Cyberangriffen.
- **Steigerung der Produktivität:** Sichern Sie operative Prozesse und gewährleisten Sie ein hohes Produktivitätsniveau.
- **Compliance:** Garantieren Sie die Einhaltung der europäischen Rahmenvorgaben für industrielle und kritische Infrastruktur wie KRITIS, NIS2 und weiteren Regularien.
- **Nachhaltiger Wettbewerbsvorteile:** Stärken Sie das Vertrauen von Kunden, Partnern und Stakeholdern durch ein nachweislich hohes Sicherheitsniveau.

Warum T Security

T Security verfügt über eines der größten SOC weltweit, modernste Technologien und ein Netzwerk aus hochqualifizierten Partnern, wodurch wir dynamische OT-IT Security Bedürfnisse Ihres Unternehmens abdecken können. Wir kennen die aktuellen Cyberbedrohungen und aufgrund unserer Erfahrungen aus der Zusammenarbeit mit zahlreichen Großkunden weltweit können wir Ihnen Security Lösungen auf höchstem Niveau anbieten. Wir bieten maßgeschneiderte Dienstleistungen, die zu Ihren Anforderungen passen und Ihre OT-IT-Infrastruktur langfristig absichern.

Unsere Expert:innen beraten Sie gerne
cyber.security@t-systems.com

Herausgeber
Deutsche Telekom AG
Friedrich-Ebert-Allee 140 , 53113 Bonn, Germany
security.telekom.de
t-systems.com