OT Security für Industriebetriebe

Umfassende OT-IT Infrastruktur Security für effektiven Schutz gegen Cybergefahren

T Systems

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 für Industriebetriebe zählen unter anderem:

- **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:** OT-Infrastrukturen werden immer öfter Ziel von Ransomware-Attacken. So verzeichneten im Jahr 2023 beispielsweise 56 % der produzierenden Betriebe einen solchen Cyberangriff.
- **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.

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 Eintrittspforten für Hacker oder Risiken, sind sich die Organisationen noch gar nicht bewusst.

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

**The State of Ransomware in Manufacturing and Production Report, 2023*

Cybergefahren besser identifizieren und abwehren

T-Systems bietet eine 360° Security Lösung, die die komplette IT-Landschaft eines Industriebetriebs abdeckt: Netzwerke, Endpoints, Datensicherheit, Cloud Computing und Produktionstechnologie. Das KI-basierte Managed Detection and Response (MDR) Tool ermöglicht die Echtzeiterkennung von Cyberbedrohungen und reduziert die Anzahl von Fehlalarme, 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.

Eine mehrstufige Vorgehensweise unseres SOC ermöglicht:

- Alle sicherheitsrelevanten Prozesse in IT-Netzwerken und OT-Systemen überwachen zu können
- Sicherheitsvorfälle in Echtzeit zu entdecken und Bedrohungen sofort melden zu können
- Die Resilienz Ihrer Systeme zu stärken, um den kontinuierlichen Betrieb Ihrer IT-Systeme und Produktion zu gewährleisten
- Ein End-to-End Konzept statt isolierter „Security Silos“ umzusetzen und damit die Sichtbarkeit und den Schutz weiter zu steigern

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 MDR Services unterstützen wir Sie mit weiteren Tools wie OT Security Assessment, Mikrosegmentierung und Infrastruktursicherheit bei der weiteren Verbesserung Ihrer OT Security.

OT-Security Assessment

Ein OT-Security Assessment verbessert die Sichtbarkeit innerhalb des Netzwerks, liefert Informationen zu Assets und hilft, Schwachstellen zu identifizieren. Ein Assessment umfasst unter anderem die Installation von Netzwerksensoren, Visualisierung, Risikoüberwachung und Aufspüren von Abweichungen.

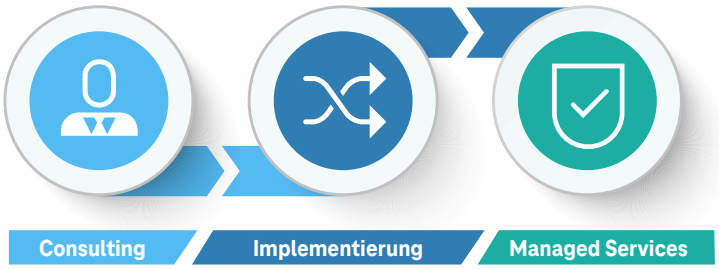
Mikrosegmentierung

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 für diese Segmente besser geschützt werden.

Infrastruktursicherheit

Die Absicherung der Infrastruktur ist von zentraler Bedeutung für den Schutz vor Cyberbedrohungen. Das umfasst den Schutz physischer und virtueller Netzwerkkomponenten, um IT und OT-Landschaften widerstandsfähig gegen Cyberangriffe zu machen. Moderne Security Lösungen unterstützen Sie dabei, den Betrieb dieser Systeme stabil aufrechtzuerhalten.

Eine umfassende Herangehensweise für OT Security



Consulting

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-Systems verfügt weltweit über SOCs mit den Möglichkeiten für SIEM1, SOAR2 und XDR3. Unsere Sicherheitsexperten verstehen sich als Ergänzung zu Ihren Inhouse-Security-Teams.

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

- **Verlustreduktion:** Verhindern Sie finanzielle Verluste durch Cyberangriffe und Datenlecks.
- **Minderung von Risiken:** Minimieren Sie operative Risiken und schützen Sie Ihre kritische Infrastruktur.
- **Geschäftskontinuität:** Stellen Sie sicher, dass der operative Betrieb nicht unterbrochen wird und Ihr Unternehmen sich von Angriffen schnell erholt.
- **Verbesserte Resilienz:** Aufbau einer stabilen und resilienten OT-Umgebung, die auch massiven Angriffen standhalten kann.
- **Gesteigerte Produktivität:** Die Absicherung der operativen Prozesse sorgt für anhaltend hohes Produktivitätsniveau.
- **Compliance:** Garantieren Sie die Einhaltung der europäischen Rahmenvorgaben für industrielle und kritische Infrastruktur wie KRITIS, NIS2 und weiteren Regularien.
- **Wettbewerbsvorteile:** Sichern Sie sich Wettbewerbsvorteile, indem Sie Kunden und Stakeholdern mit umfassenden Sicherheitsmaßnahmen überzeugen.

Warum T-Systems?

T-Systems 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.

Starten Sie Ihr OT Security Assessment und kontaktieren Sie uns noch heute!

Expert Contact

Andreas Pecka
Head of International Sales and
Pre-Sales Cyber Security
a.pecka@t-systems.com

Herausgeber

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany
E-Mail: cyber.security@t-systems.com
Internet: www.t-systems.com

T Systems