FUJITSU

Cyber Security for Operational Technology (OT)

Schutz für
geschäftskritische
Produktionsnetzwerke
und Ressourcen

Wir kennen Ihre Herausforderungen

Produktions- und Versorgungsunternehmen stehen vor der Herausforderung, ihre Betriebstechnologie (Operational Technology, OT) – also die Hardware und Software zur Steuerung von Industrieanlagen – digital zu sichern. Denn mit der zunehmenden IT-Konnektivität steigt auch die Gefahr von Cyber-Attacken. Nur mit effektiven und sicheren digitalen Betriebsprozessen lassen sich Ausfallzeiten minimieren, die Sicherheit der Mitarbeitenden optimieren, Kunden- und Geschäftsdaten schützen und Unterbrechungen der Lieferkette vermeiden. Dies ist keine einmalige Aufgabe, sondern ein stetiger Prozess.

Die proaktive Risikominimierung für OT-Netzwerke ist eine Grundvoraussetzung, um mit dem rasanten digitalen Wandel Schritt zu halten. Unsere Expert*innen verhelfen Ihnen zu einem sicheren Netzwerk, das Ihre Industrieprozesse und geschäftskritischen Ressourcen rund um die Uhr schützt. Wir unterstützen Sie und Ihre Mitarbeitenden dabei, Ihre geschäftskritischen Infrastrukturen zu analysieren, zu schützen und zu verwalten – nahtlos, sicher und zuverlässig.

Wir arbeiten anhand von drei einander ergänzenden Services mit unseren Kunden zusammen:

OT Assessment and Asset Discovery
Analyse Ihrer bestehenden Netzwerke, Ermittlung von Compliance-Lücken, Erstellung Ihres Risikoprofils und Definition von Basiswerten zu Ihren vernetzten digitalen Ressourcen

OT Network Transformation
Anwendung vorrangiger Maßnahmen zum Schutz Ihrer OT-Netzwerke

OT Managed Monitoring Service
Rund-um-die-Uhr-Service zur Erkennung ungewöhnlicher Aktivitäten in OT-Umgebungen

Unterschiede zwischen IT und OT

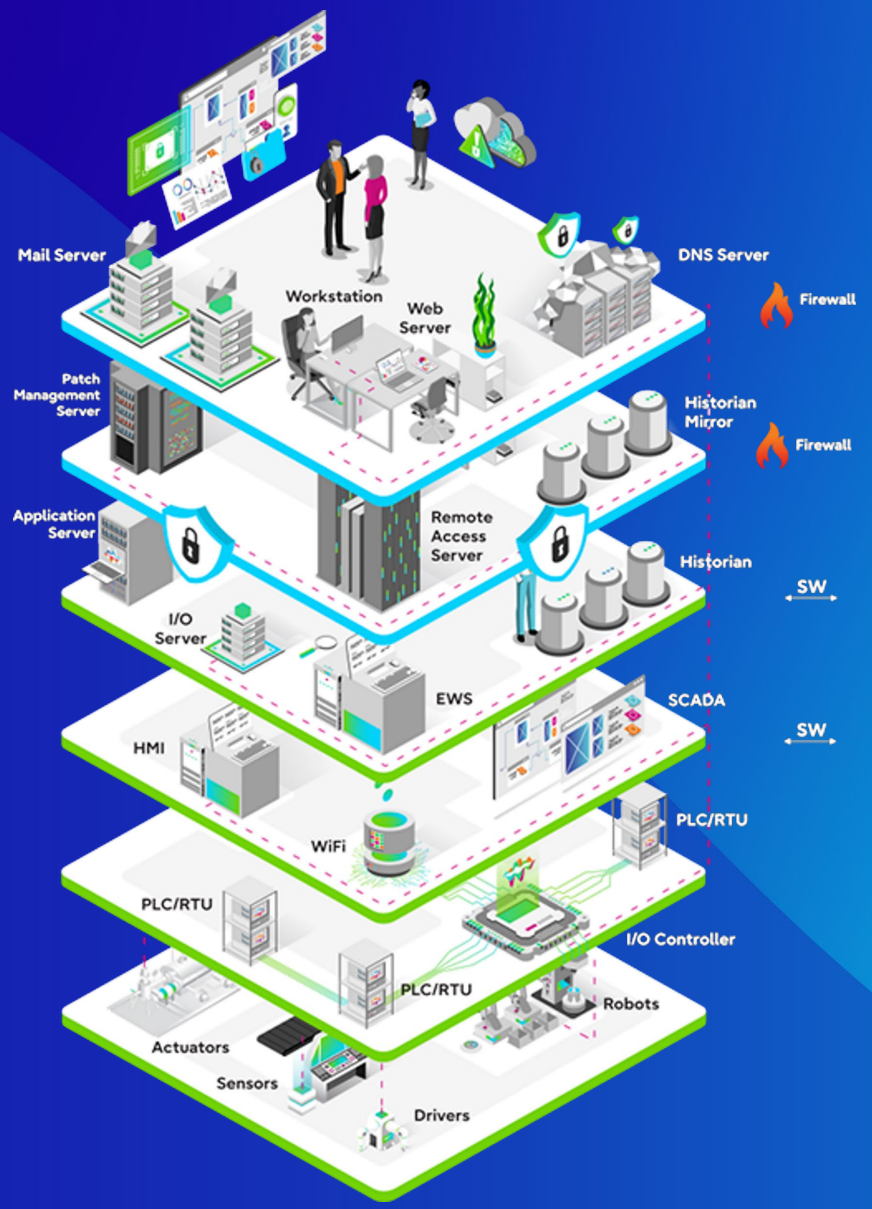
IT-Mindset

- Die Welt ist virtuell
- Schutz, Verfügbarkeit und Integrität von Daten haben Priorität
- Zentrale Verwaltung vernetzter Ressourcen
- Agilität

OT-Mindset

- Die Welt ist physisch
- Sicherheit, Verfügbarkeit und Resilienz von Produktionsprozessen als Priorität
- Verwaltung vernetzter Ressourcen auf Standortebene
- Messung der Gesamtanlageneffektivität
- Kultur des „Don't touch, don't break“

IT und OT unterscheiden sich nicht nur in technischer Hinsicht, sondern auch in Sachen Mitarbeitende, Ausbildung, Organisation und Kultur.



Produktions- und Versorgungsunternehmen müssen...

- ... die Kontinuität ihrer Produktionsprozesse sowie physische Sicherheit gewährleisten
- ... die Nachhaltigkeit & Compliance der Produktion sicherstellen
- ... die Gesamtanlageneffektivität (Overall Equipment Effectiveness, OEE) stetig verbessern
- ... Wettbewerbsvorteile in neuen Wertschöpfungsketten erlangen
- ... datengetrieben handeln, um das Geschäftsergebnis zu verbessern

Die Lücke zwischen IT und OT schließt sich

OT- und IT-Teams haben seit jeher getrennt voneinander gearbeitet. Dies kann allerdings die Sicherheit, Zuverlässigkeit und Belastbarkeit Ihrer Unternehmens-IT gefährden.

Mit der zunehmenden Digitalisierung haben Cyber-Attacken ein Rekordhoch erreicht. Wenn nahtlose Netzwerke für die unternehmensweite Konnektivität installiert werden, muss auch der Schutz der Betriebstechnologie vor Cyber-Bedrohungen sichergestellt sein.

OT und IT sind entscheidend für Ihren Geschäftserfolg und sollten sowohl zu Sicherheits- als auch Management-Zwecken integriert werden.

Intelligente Produktion braucht intelligente Cyber-Sicherheit

Der mangelnde Schutz vor Cyber-Bedrohungen kann sich negativ auf die Produktionsziele auswirken, Maschinen, Mitarbeitende und selbst ganze Gemeinden beeinträchtigen sowie zum Verlust von geistigem Eigentum führen. Die Bedrohungen können von externen Faktoren, böswilligen Insidern oder Lieferanten ausgehen. Unser Ziel besteht darin, diese Bedrohungen deutlich zu reduzieren und den Stress rund um das Thema Cyber-Sicherheit zu verringern. Gemeinsam können wir die Herausforderungen der Cyber-Sicherheit meistern und gleichzeitig die Zuverlässigkeit und Compliance der Betriebsprozesse im Blick behalten. Umfassende Richtlinien definieren die Anforderungen an die Betreiber, Integratoren und Komponentenlieferanten für die physikalischen Prozesse. Wir wissen, dass es kompliziert werden kann.

Deshalb unterstützen wir Sie dabei, diese Theorie in die Praxis umzusetzen. Neue, verbundene Netzwerke und stetig wachsende Anforderungen machen ein verstärktes Sicherheits-Monitoring wichtiger interner Ressourcen und Prozesse erforderlich. Zudem bieten zahlreiche Produktionsumgebungen keinen Einblick in digitale Ressourcen. Wir helfen Ihnen, Ihre Daten zu ermitteln und effektiv zu nutzen, um Ihren Geschäftsbetrieb zu optimieren. Was sind also die nächsten Schritte?

2021 waren Produktions- und Versorgungsunternehmen das häufigste Ziel von Cyber-Attacken* – und damit bei Angreifern beliebter als die Finanzdienstleistungs-Branche

Ungeplante Ausfallzeiten kosten Unternehmen durchschnittlich **532.000** US-Dollar pro Stunde.**

*Quelle: IBM Security X-Force Threat Intelligence Index 2022
**Quelle: Bericht „The True Cost of Downtime“

Unser Ansatz

Unser Ansatz ist einfach: Wir analysieren und schützen Ihre geschäftskritische Infrastruktur und helfen Ihnen, sie sicher zu verwalten. Gemeinsam mit Ihnen schaffen wir ein solides Fundament, das den Belastungen einer sich ständig weiterentwickelnden Technologielandschaft standhält. Die drei Services können unabhängig voneinander bestellt und bereitgestellt werden.

Die Fujitsu OT Cyber Security Services umfassen drei Komponenten:

OT Assessment and Asset Discovery
Analyse Ihrer bestehenden Netzwerke, Ermittlung von Compliance-Lücken, Erstellung Ihres Risikoprofils und Definition der Basiswerte Ihrer vernetzten digitalen Ressourcen.

OT Network Transformation
Anwendung vorrangiger Maßnahmen zum Schutz Ihrer OT-Netzwerke.

OT Managed Monitoring Service
Rund-um-die-Uhr-Service zur Erkennung ungewöhnlicher Aktivitäten in OT-Umgebungen

OT Assessment and Asset Discovery

„Was man nicht sieht, kann man nicht kontrollieren."
Zunächst erfolgt eine Bestands-aufnahme Ihrer bestehenden Netzwerk-Infrastruktur unter dem Gesichtspunkt der Cyber-Sicherheit für Mitarbeitende, Prozesse und Technik. Anhand dieser Analyse schlagen wir eine Entwicklungs-Roadmap vor, die den individuellen technischen, organisatorischen und Compliance-Anforderungen Ihres Unternehmens gerecht wird.
Die Bestandsaufnahme umfasst auch die automatische Erkennung vernetzter OT-Ressourcen wie speicher-programmierbare Steuerungen (SPS), Fernbedienungsterminals (RTUs), SCADA-Systeme, Arbeitsplatzrechner, HMIs und Historians. In Kombination mit dem Wissen der Mitarbeitenden zu ihrer Nutzung ermöglicht dies eine auf den Produktionsprozess abgestimmte qualitative Risikobewertung. Die während der Sicherheitsbewertung erfassten Ressourcendaten lassen sich zum Beispiel für eine Configuration Management Database (CMDB) weiterverwenden.

OT Network Transformation

Zur Optimierung Ihrer Netzwerk-Infrastruktur prüfen wir zunächst die bestehenden Verbindungspunkte innerhalb von und ggf. auch zwischen Standorten. Unter Verwendung vorheriger Investitionen wie Firewalls implementieren wir eine segmentierte Netzwerkarchitektur nach dem Purdue Model. So werden die funktionalen Anforderungen und Risikoprofile Ihrer gesamten Produktionslinie aufgezeigt. Während der Implementierung und Umstellung arbeiten wir eng mit Ihnen, Ihrem OT-Team und Ihren spezialisierten OT-Partnern zusammen, um das Risiko einer Unterbrechung geschäftskritischer Prozesse zu minimieren.

Wir nutzen erprobte und kosteneffektive Techniken wie SD-WAN, um die Wireless-Konnektivität zwischen Standorten und dem Unternehmensnetzwerk zu verbessern. Unsere sichere Netzwerkarchitektur basiert auf dem in Norm IEC 62443-3-2 definierten Zonen-und-Conduits-Modell.

OT Managed Monitoring Service

Unser OT Managed Monitoring Service wird remote von unseren Security Operating Centers (SOCs) bereitgestellt. Dabei werden laufend Informationen über Ihre OT-Ressourcen erfasst und an Ihre eigene Steuerzentrale weitergeleitet. Verwertbare Erkenntnisse werden sofort an Ihr Betriebsmanagement-Team berichtet, damit Sie Cyber-Vorfälle verhindern, erkennen, entschärfen und beheben können.
Die Erstellung eines umfassenden Profils Ihres Arbeitsmodells und Datenaustauschs ermöglicht es uns, den Rahmen Ihrer normalen Cyber-OT-Aktivitäten abzustecken. Eine abgestimmte Kommunikation zwischen unserem und Ihrem Team stellt sicher, dass Sie im Falle einer Bedrohung schnell reagieren können.
Es ist uns wichtig, dass Sie Vertrauen in Ihre OT-Cyber-Sicherheit haben. Deshalb führen wir regelmäßig Leistungsbeurteilungen durch und analysieren die Effektivität und Kundenzufriedenheit.

Geschäftsvorteile

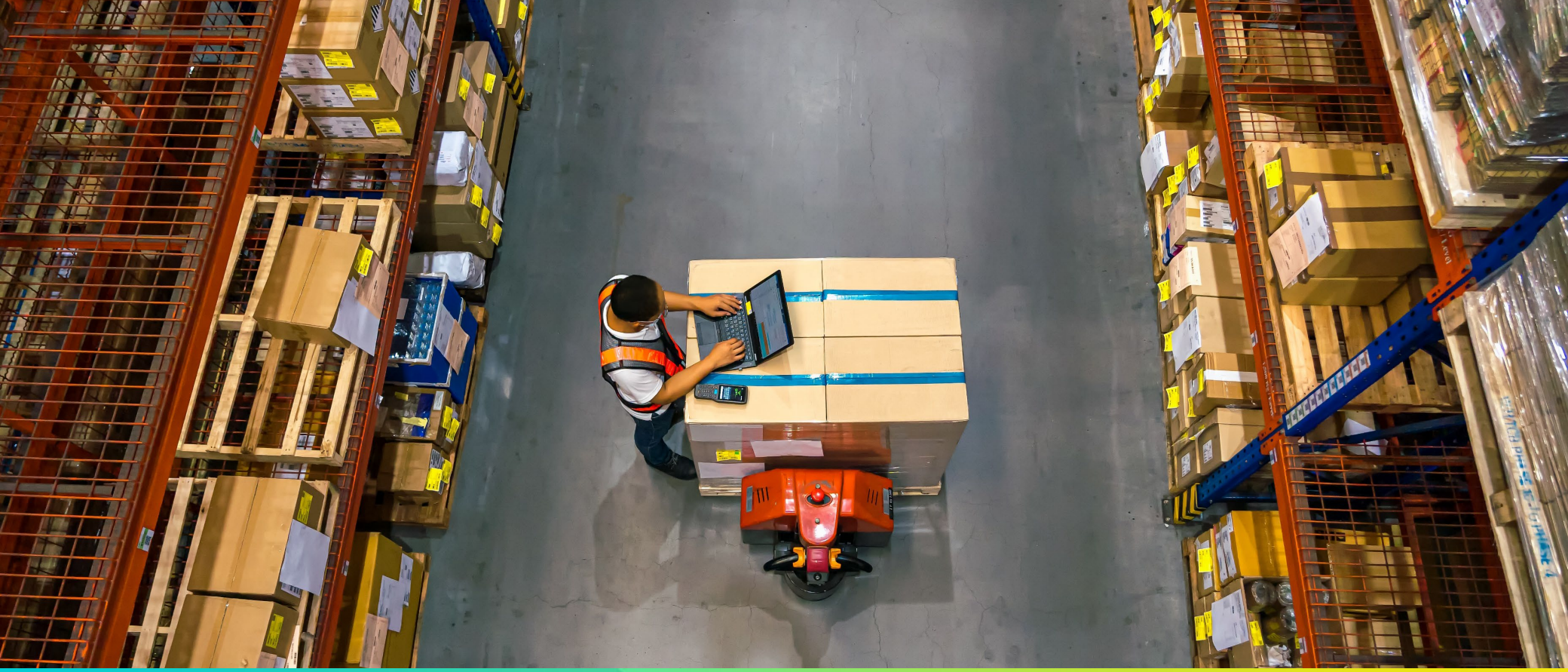
Wir bieten fünf wichtige Geschäftsvorteile für Unternehmen aus der Fertigungs- und Versorgungsindustrie:

- Maximale Kontinuität des Produktionsprozesses
- Einhaltung von Standards für das Wohlbefinden und die Sicherheit von Mitarbeiter*innen
- Minimierung des Cyber-Sicherheitsrisikos – Schutz geistigen Eigentums vor Cyber-Attacken
- Sicherer Zugriff auf Produktionsdaten für alle Arten von unternehmensweiten Verbesserungs-prozessen
- Compliance in regulierten Branchen – CNI, Industrienormen und -richtlinien sowie Daten

Warum Fujitsu for OT Security?

- **OT-Cyber-Sicherheitsschutz als Service**
- **Nachgewiesene Qualifikation für ISO27001 und ISO22301**
- **Partnerschaftlicher Ansatz mit unseren Kunden und einem größeren Ökosystem**
- **40 Jahre Erfahrung im Bereich Cyber-Sicherheit mit globalen und lokalen Kompetenzen**
- **Erfahrung mit Normen der Fertigungs- und Versorgungsbranche, darunter NIS-D, NIST und IEC 62443**

Wir sind nicht nur ein Anbieter erstklassiger Cyber-Lösungen, wir stellen diese auch her. Damit sind wir der ideale strategische Partner, um die Cyber-Herausforderungen auf dem Weg zu digitalem und nachhaltigem Wandel zu meistern. Wir sind Ihr zentraler Ansprechpartner für Ihre vollständige digitale End-to-End-OT-Transformation.



Sie denken, Ihre OT-Umgebung ist sicher?

Lassen Sie uns darüber sprechen, wie wir Ihre OT-Sicherheit auf das nächste Level heben können.

Hier erfahren Sie mehr über Fujitsu OT Security.

FUJITSU

OT Security Technology Partner:

Radiflow | FORTINET | servicenow