OT-SECURITY

Strategien zur Sicherung von Betriebstechnologie

WHITEPAPER

sure[secure] X securance

Einführung

Im Wilden Westen der 90er Jahre war Cybersicherheit nicht einmal ein Schlagwort, geschweige denn eine Priorität. Damals war das Internet noch neu und die Unternehmen begannen gerade erst, ihre Zehen in den riesigen digitalen Ozean zu stecken. Heute leben wir in einer Welt, in der die Sicherheit der Betriebstechnologie von entscheidender Bedeutung geworden ist.

Warum also die Aufregung um die OT-Security?

Wie unterscheidet sie sich von den Cybersicherheitsbedenken der Vergangenheit?

Also sattelt eure Pferde – wir reiten los.

Die Entwicklung der OT-Security

In den 90er Jahren war das Konzept der Sicherung von Betriebstechnologien nahezu inexistent. Computer steuerten zwar industrielle Prozesse, waren aber oft isoliert, und die Vorstellung, dass sie mit der Außenwelt verbunden waren, war eine Seltenheit. Heute sind OT-Systeme mehr denn je miteinander vernetzt. Von Kraftwerken bis hin zu Produktionsanlagen ist alles auf vernetzte digitale Systeme angewiesen, was sie zu attraktiven Zielen für Cyberangriffe macht. Die 90er Jahre waren wie die Ära des Wilden Westens mit minimalen Regeln und einer „anything goes“-Haltung. Heutzutage müssen wir unsere digitalen Grenzen sichern, um kritische Infrastrukturen zu schützen.

Definition der Grenzen

Nachdem wir nun geklärt haben, warum OT-Security ein Thema ist, wollen wir nun klären, was OT umfasst. Operationelle Technologie (OT) bezieht sich auf die Hard- und Software, die zur Überwachung und Steuerung physischer Prozesse eingesetzt werden, z. B. in der Fertigung, Energieerzeugung und im Transportwesen, aber auch in Krankenhäusern, Kliniken, Smart Cities/Buildings oder der Verkehrssicherheit. Die OT-Security konzentriert sich daher auf den Schutz dieser Prozesse vor Cyber-Bedrohungen. Sie ist der digitale Schutzschild, der vor Cyberangriffen schützt, die Stromnetze stören, Wasseraufbereitungsanlagen manipulieren oder Produktionslinien sabotieren wollen.

Verständnis von OT-Security

OT-Security kann definiert werden als die Praxis des Schutzes kritischer Infrastrukturen und industrieller Systeme vor Cyber-Bedrohungen und unbefugtem Zugriff. Diese Systeme sind das Herz unserer modernen Welt und steuern alles von Ölraffinerien bis hin zu Wasseraufbereitungsanlagen. Das Ziel der OT-Security besteht darin, den kontinuierlichen Betrieb dieser Systeme zu gewährleisten und sie vor Cyberangriffen zu schützen, die katastrophale Folgen haben könnten. Dazu gehört eine Kombination aus Richtlinien, Verfahren und Technologien, die darauf ausgelegt sind, Cyber-Bedrohungen in der OT-Umgebung zu erkennen, zu verhindern und darauf zu reagieren.

Unternehmen, die im OT-Sektor tätig sind, stehen vor einer Reihe von Herausforderungen.

Verantwortlichkeiten

OT-Leiter? IT-Leiter?

Legacy-Systeme, die Altlasten der OT-Umgebungen.

An erster Stelle steht das Problem der Altsysteme. Viele der heute verwendeten OT-Systeme wurden vor Jahrzehnten entwickelt und implementiert, als die Cybersicherheit noch keine große Bedeutung hatte. Diese Systeme zu aktualisieren, ohne kritische Abläufe zu unterbrechen, ist eine gewaltige Aufgabe.

Fachpersonal.

Und dann ist da noch das Problem des qualifizierten Personals. Personen zu finden, die über das nötige Fachwissen verfügen, um sich in den Feinheiten der OT-Security zurechtzufinden, gleicht der Suche nach der Nadel im Heuhaufen. Darüber hinaus hat die Konvergenz von IT (Informationstechnologie) und OT neue Schwachstellen geschaffen und einen Kulturwandel in den Unternehmen erforderlich gemacht, bei dem die Sicherheit Vorrang hat.

OT-Landschaften sind häufig „unmanaged“ und sehr heterogen.

Die IT-Abteilung grenzt sich davon meist ab und in vielen Unternehmen gibt es keine dedizierte OT-Abteilung. In der Regel bedeutet das: keine Entscheiderstrukturen und keine genehmigten Budgets. Das bedeutet auch, dass es niemanden gibt, der sich z. B. beim Bau einer neuen Produktionshalle mit Fertigungsstraße Gedanken darüber macht, wie die Systeme betrieben und gepatched werden. Das ist fahrlässig, da eine Produktionshalle samt Inventar oft einen Lifecycle von mehreren Jahrzehnten hat und somit weitere Legacy-Systeme bewusst in Kauf genommen werden.

Prozesse ja, aber nicht für die OT?

Die gesamten Risikoanalyse-/Schwachstellenmanagement-Prozesse in Unternehmen sind oftmals für die IT etabliert. Dadurch fehlt gänzlich die Visibilität im OT-Bereich. OT nutzt eigene Protokolle für den Datenaustausch im Netzwerk. Dadurch sind bestehende Sicherheitskomponenten wie z.B. Firewalls oder Virenscanner in diesem Bereich gar nicht anwendbar, da sie diese Daten entweder nicht analysieren können oder keine Erkennungen dafür besitzen.

Wartung - never touch a running system.

Dies gilt insbesondere für die OT. Warum? Weil in der OT häufig die Wertschöpfung stattfindet und ein Fehler hier schwerwiegende Folgen haben kann. Der potenzielle Schaden ist wesentlich höher als in der IT, weshalb Änderungen nur sehr bedacht durchgeführt werden. Die Folgen von Eingriffen sind aufgrund der Heterogenität oft nicht zu antizipieren.

In Produktionsstätten ist es üblich, dass Maschinen regelmäßig gewartet werden müssen. In diesen oft manuellen Prozessen werden dann neue Firmware oder Updates eingespielt. Dieser Prozess unterliegt in den meisten Fällen keinen Sicherheitsrichtlinien. Das heißt, es gibt keinerlei Vorschriften wie (remote oder vor Ort) und mit welchen Medien diese Wartungen durchgeführt werden.

Lösungsansatz:

Wir haben verstanden: Ein umfassendes, flexibles und modernes OT-Sicherheitskonzept ist entscheidend oder von entscheidender Bedeutung, um kritische Infrastrukturen und industrielle Prozesse vor potenziellen Bedrohungen zu schützen. In diesem Kontext spielen verschiedene Aspekte eine wichtige Rolle:

Visibilität schaffen:

OT-Asset Visibility and Discovery

1

Risiken verstehen:

Risiko- und Schwachstellenmanagement

2

Architektur implementieren:

OT-Netzwerksegmentierung & Zero Trust Access Management

3

Kontinuierliche Überwachung:

Überwachung und Einhaltung gesetzlicher Vorschriften und Compliance-Regeln

4

1. Visibilität schaffen: OT-Asset Visibility and Discovery

Das Vorgehen verfolgt einen ganzheitlichen Ansatz, um die Sicherheit und Resilienz operativer Technologie zu gewährleisten. Die kontinuierliche Sichtbarkeit und Kommunikation über alle OT-Netzwerke und -Systeme hinweg ist dabei von zentraler Bedeutung. Durch die Implementierung von fortschrittlichen Überwachungslösungen und Netzwerkanalysen gewährleisten wir eine Echtzeitüberwachung des gesamten OT-Umfelds, um potenzielle Anomalien oder verdächtige Aktivitäten frühzeitig zu erkennen und zu mitigieren.

Zur Steigerung der Visibilität ist die Implementierung eines Monitoring-Tools zur Echtzeitüberwachung der OT-Systeme erforderlich. Dazu braucht es den Einsatz von Sensoren und Protokollierungstechnologien, um Aktivitäten in OT-Umgebungen zu erfassen und Kommunikationswege aufzuzeigen. Über eine Schnittstelle zu einer SIEM-Lösung können diese Daten zentral erfasst, korreliert und analysiert werden.

2. Risiken verstehen: Risiko- und Schwachstellenmanagement

Ein weiterer wesentlicher Bestandteil ist das Schwachstellenmanagement. Dabei werden kontinuierlich Schwachstellenanalysen und -bewertungen durchgeführt, um potenzielle Sicherheitslücken zu identifizieren und zeitnah zu beheben. Bei der Behebung von Schwachstellen helfen vordefinierte und erprobte Playbooks, da ein Patchmanagement in OT-Umgebungen nicht immer anwendbar ist.

Durch die gleichzeitige Implementierung eines robusten Risikomanagementprozesses können wir Risiken quantifizieren, priorisieren und entsprechende Gegenmaßnahmen zielgerichtet ergreifen, um potenzielle Bedrohungen frühzeitig zu beseitigen.

- Durchführung einer Risikobewertung (am Impact für das Business des Kunden ausgerichtet), um kritische Assets und potenzielle Bedrohungen zu identifizieren.
- Implementierung von Sicherheitskontrollen und Maßnahmen zur Risikominderung.
- Regelmäßige Durchführung von Schwachstellen-Scans in OT-Systemen und Umgebungen.
- Priorisierung und Behebung der identifizierten Schwachstellen unter Berücksichtigung ihres Risikopotenzials und der damit verbundenen Auswirkungen auf den Betrieb.
- Festlegung von Notfallplänen und Wiederherstellungsstrategien für den Fall von Sicherheitsvorfällen (siehe auch Incident Response).

3. Architektur implementieren: OT-Netzwerksegmentierung & Zero Trust Access Management

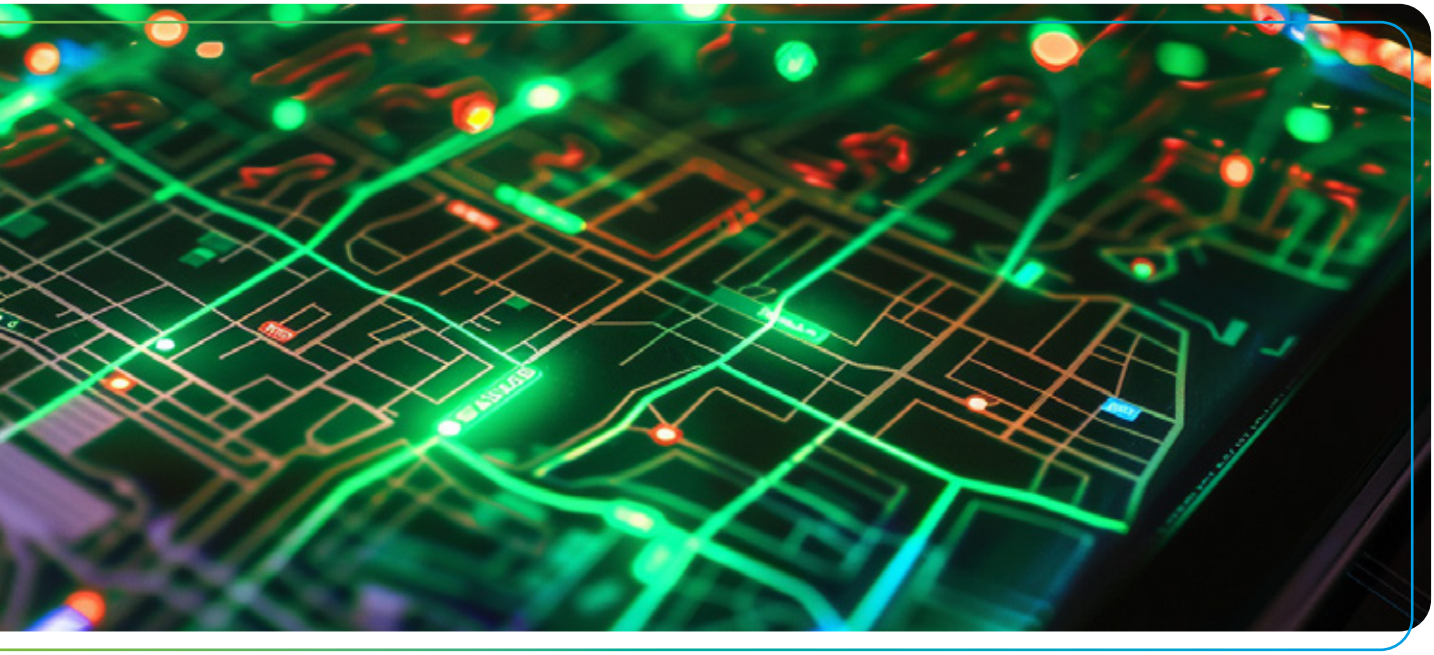
Um die Sicherheit und Integrität eines OT-Netzwerks zu erhöhen, setzen wir zudem auf eine strikte Netzwerksegmentierung. Durch die Aufteilung des OT-Umfelds in isolierte Zonen können wir das Risiko von lateralen Bewegungen und die Auswirkungen von Cyberangriffen begrenzen. Dabei orientieren wir uns an den Prinzipien des Zero Trust Access Managements, bei dem der gesamte Netzwerkverkehr unabhängig von Quelle und Ziel streng authentifiziert und autorisiert wird.

- Segmentierung des OT-Netzwerks in logische Zonen gemäß den funktionalen Anforderungen und Sicherheitsrichtlinien.
- Implementierung von Authentifizierungs- und Autorisierungsmechanismen für den Zugriff auf OT-Ressourcen und Assets (vor allem für Remote User und 3rd Party Unternehmen).
- Einsatz von Multi-Faktor-Authentifizierung und kontextabhängiger Zugriffssteuerung.
- Überwachung und Protokollierung aller Zugriffsaktivitäten für Audit- und Compliance-Zwecke.

Für den Fall eines Sicherheitsvorfalls ist ein detaillierter Incident Response Plan (IRP) unerlässlich. Dieser definiert klare Rollen und Verantwortlichkeiten, um eine effiziente Reaktion auf Vorfälle zu gewährleisten. Wichtig ist hierbei vor allem die Einbindung des IT-Teams, um die Kommunikation, Übergabepunkte und Schnittstellen klar zu definieren und zu dokumentieren. Wir führen regelmäßig Krisenübungen durch, um die Effektivität des Sicherheitskonzeptes zu testen, kontinuierlich zu verbessern und das Incident Response Team zu schulen. Idealerweise werden sowohl die IT als auch die OT-Sicherheit zentral in einem SOC (Security Operation Center) gemanagt, um in einem Incident schnell mit den notwendigen Experten bestehend aus Forensikern, Analysten etc. reagieren zu können.

Incident Response Plan

- Entwicklung eines umfassenden Incident Response Plans zur schnellen Erkennung, Reaktion und Wiederherstellung bei Sicherheitsvorfällen.
- Integration der OT-Sicherheit in ein SOC-Team, entweder intern oder durch einen externen Dienstleister im Rahmen eines Managed Service.
- Schulung des Personals im Umgang mit Sicherheitsvorfällen und Durchführung regelmäßiger Incident Response Übungen unter Einbindung der OT- und IT-Teams.



4. Kontinuierliche Überwachung: Überwachung und Einhaltung gesetzlicher Vorschriften und Compliance-Regeln

Neben der technischen Sicherheit legen wir großen Wert auf die Einhaltung gesetzlicher Vorgaben und Compliance-Regeln. Unsere Sicherheitsmaßnahmen orientieren sich eng an den relevanten Regelwerken, wie unter anderem dem Industriestandard IEC 62443. Durch regelmäßige Audits und automatisierte Überprüfungen stellen wir sicher, dass die vorhandenen OT-Systeme den geltenden Standards entsprechen und jederzeit compliant sind.

- Identifikation und Verständnis der relevanten gesetzlichen Vorschriften und branchenspezifischen Compliance-Anforderungen.
- Implementierung von Kontrollen und Prozessen zur Einhaltung dieser Vorschriften, einschließlich regelmäßiger Audits und Berichterstattung.

Zusammenfassung

Insgesamt verfolgt unser OT-Sicherheitskonzept somit einen ganzheitlichen Ansatz, der auf Sichtbarkeit, proaktivem Risikomanagement, robusten Sicherheitsmaßnahmen und der Einhaltung von Compliance-Vorschriften basiert. Durch diese Maßnahmen können wir die bestmögliche Sicherheit der OT-Infrastrukturen gewährleisten und potenzielle Risiken und Bedrohungen effektiv minimieren.

Dies bildet die Grundlage für ein umfassendes OT-Security Framework, das darauf abzielt, die Sicherheit und Integrität von Betriebsanlagen und -prozessen zu gewährleisten. Dabei ist es wichtig, dass dieses Konzept an die spezifischen Anforderungen und Risiken der jeweiligen Organisation angepasst wird und in ein unternehmensweites Cyberdefense Konzept eingebunden ist.

In der heutigen vernetzten Welt hat der Schutz der Betriebstechnologie oberste Priorität, und ein Verständnis der besonderen Herausforderungen und Lösungen im Bereich der OT-Security ist für die Sicherheit und Widerstandsfähigkeit unserer kritischen Infrastrukturen unerlässlich. All das kann nicht an einem Tag gelöst werden, aber es ist wichtig, die eigenen Herausforderungen im OT-Sektor zu verstehen.

Ein OT-Assessment bietet die Möglichkeit, das Risiko der OT-Umgebung zu bestimmen. Daraus kann dann eine zielgerichtete Roadmap abgeleitet werden, um die OT-Risiken sukzessive zu mindern.

Wenn du mehr über OT-Security erfahren möchtest, dann hör dir unseren Podcast an. Und wenn du eine persönliche Beratung wünschst, vereinbare einen Termin mit unserem OT-Security Experten Uwe Grunwitz.

Hier kannst du einen Termin mit Uwe vereinbaren.

Fragen zur OT-Security? Schreib uns.

Hör dir unseren Podcast an:
Never touch a running system? Zeit für einen Realitätscheck in der OT-Security!

“Die Bedeutung von OT und IOT-Security im Kontext der Digitalisierung kann nicht überbetont werden, da sie die grundlegende Integrität, Verfügbarkeit und Verlässlichkeit operativer Technologien gewährleistet, die sowohl in kritischen Infrastrukturen, bei industriellen Prozessen sowie in Smart Cities und in der Gebäudedigitalisierung eingesetzt werden.“

- Uwe Grunwitz – OT-Security Advisor

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de