Ein ganzheitlicher Ansatz zur OT-Sicherung

Neue Cybersicherheitsherausforderungen für Betriebstechnologie

verizon business

Die vierte industrielle Revolution hat die Branche grundlegend verändert. Um von diesem Fortschritt zu profitieren, benötigt die moderne Industrie schnelle, sichere und resiliente Services und Systeme. Unternehmen müssen die Sicherheit ihrer Betriebstechnologie (Operational Technology, OT) priorisieren und angemessene Überwachungs- und Abwehrmechanismen zum Schutz vor potenziellen Problemen implementieren.

Denn die Konnektivität von OT-Appliances und -Geräten bringt zwar viele Vorteile mit sich, kann aber auch von böswilligen Nutzern oder Cyberkriminellen ausgenutzt werden, um sich Zugriff zu verschaffen.

Bisher waren OT-Netzwerke für eine größere Sicherheit und Zuverlässigkeit von den IT-Netzwerken und dem Internet getrennt. Doch das ist nicht mehr der Fall.

In diesem Whitepaper wird erläutert, wie Unternehmen ihre integrierten OT-Netzwerke schützen können, damit sie als Vorteil und nicht als Risiko eingestuft werden können.

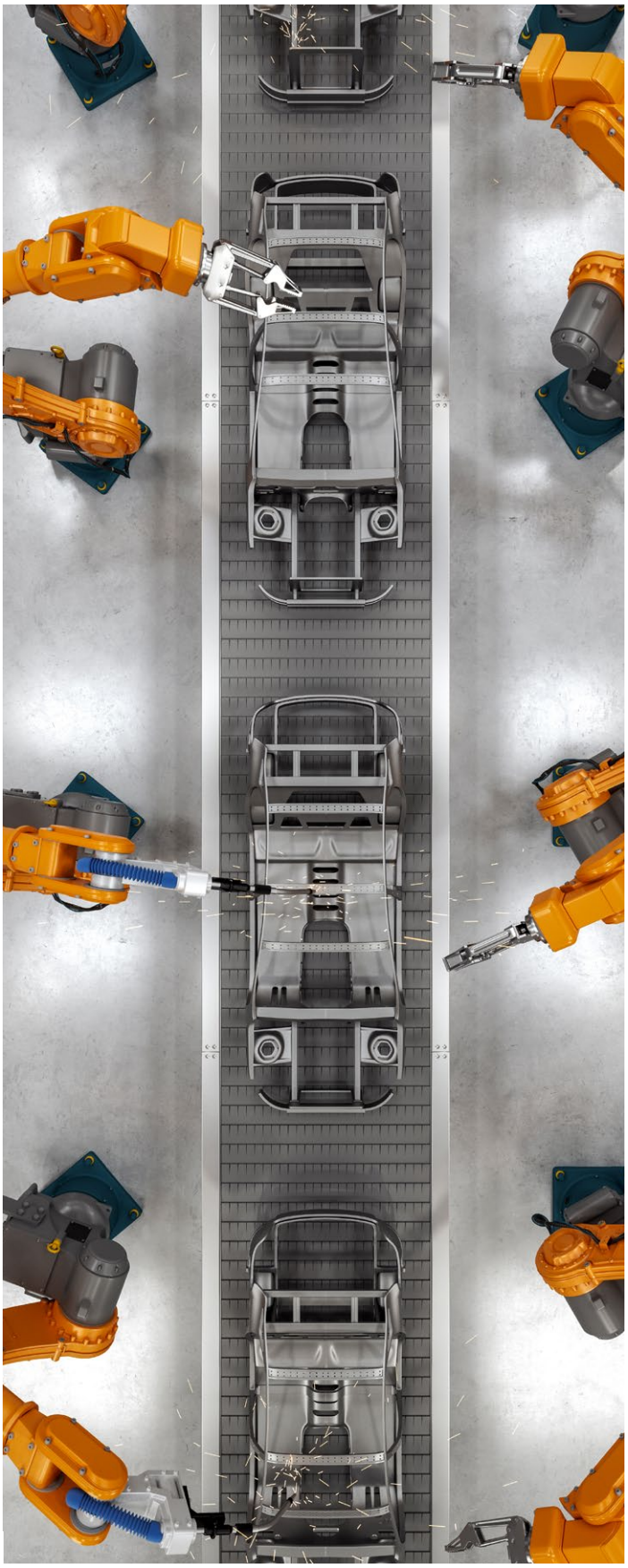
Auf dem OT-Sicherheitsmarkt stehen die Ressourcenidentifikation und die Erkennung von Bedrohungen und Schwachstellen im Mittelpunkt, doch dabei dürfen effektive Abwehrmaßnahmen nicht außer Acht gelassen werden.

Ein neuer Cybersicherheitsansatz für Industrie 4.0

Industrie 4.0, auch die vierte industrielle Revolution genannt, zeichnet sich durch die Kombination diverser Technologien aus, durch die die Grenzen zwischen physischen, digitalen und biologischen Bereichen verschwimmen.

Infolgedessen führen Unternehmen diverse Neuerungen ein – von autonomen Robotern und Fernsteuerungen nahezu in Echtzeit über Edge Computing bis hin zu modernen Konnektivitätstechnologien. Da diese Prozesse äußerst komplex und eng mit der Cloud verzahnt sind, müssen die Sicherheitsarchitekturen vollständig überarbeitet werden. Für eine strenge Zugriffskontrolle wird beispielsweise Zero Trust notwendig.

Quelle: [1] Forrester, „The Forrester Wave™: Operational Technology Security Solutions“, Q2 2024



Das sollte jedoch nicht als Problem betrachtet werden. Bei dieser Umgestaltung bietet sich auch die Möglichkeit, die Unternehmensarchitektur zu vereinfachen und zu optimieren. Ein Vorteil ist die Erfassung riesiger Datensätze für Analysen, die in ganz unterschiedlichen Bereichen einen wichtigen Beitrag leisten können – von der Behebung von Sicherheitsvorfällen bis zur Produktverbesserung.

Neue Trends bergen auch neue Risiken

OT-Evolution

Zur Effizienzsteigerung wird die OT – wie schon die IT – immer häufiger in die Cloud migriert. Unternehmen nutzen auch zunehmend KI für die vorausschauende Wartung und Automatisierung und finden neue Wege für die Zusammenarbeit mit Drittanbietern. Ausschlaggebend ist ihren Angaben zufolge meist das Ziel, die Sicherheitsmaßnahmen und die Kosteneffizienz zu verbessern.

> 80 % der CIOs werden bis 2028 KI und Automatisierung für eine größere Agilität und den Aufbau eines datengestützten Unternehmens einsetzen.“
>
> **CIO Predictions** der IDC für den asiatisch-pazifischen Raum* für 2024 und darüber hinaus

Risiken der IT-OT-Konvergenz

Die zunehmende Konnektivität zwischen IT- und OT-Netzwerken vergrößert eventuell die Angriffsfläche, da bei älteren OT-Systemen die Cybersicherheit in der Regel nicht berücksichtigt wurde.

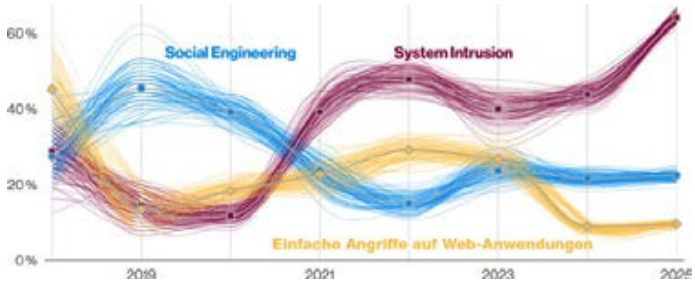
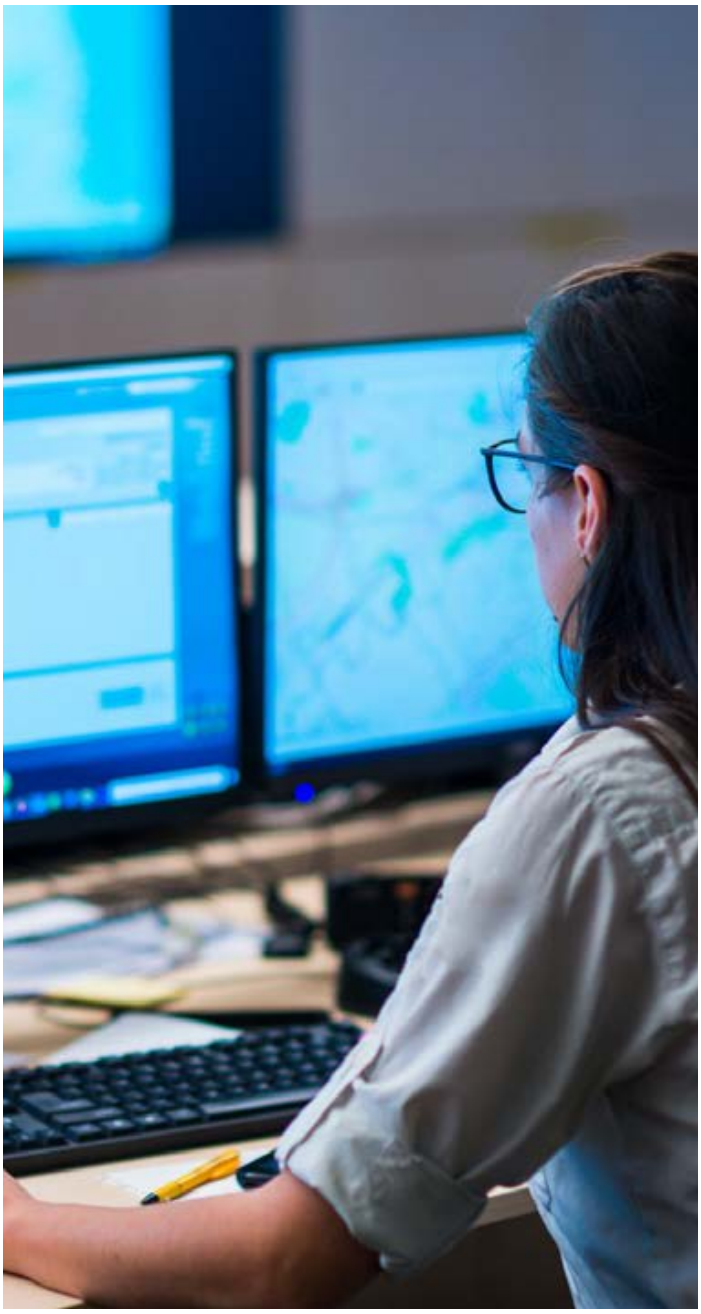


Abbildung 1: Häufigste Angriffskategorien in der Fertigungsbranche im Zeitverlauf

Quelle: Abbildung 1: Verizon DBIR 2025

Das hat bereits gravierende Auswirkungen. Laut dem Data Breach Investigations Report 2025 (DBIR) von Verizon haben die System-Intrusion-Angriffe seit 2020 stark zugenommen. Vor allem die Fertigungsbranche hat im letzten Jahr einen deutlichen Anstieg verzeichnet. In diesem Sektor haben auch die Datenschutzverletzungen stark zugenommen: Kleine und mittelständische Unternehmen (KMU) haben dieses Jahr 1.607 Angriffe gemeldet.

Zwar bleiben finanziell motivierte, externe Angreifer die größte Gefahr, aber es ist auffällig, dass bei etwa 20 % der Sicherheitsvorfälle in der Fertigungsbranche Spionage das Motiv war. Das ist ein deutlicher Anstieg von nur 3 % im Vorjahr.



Veraltete und nicht gepatchte Systeme

In vielen OT-Umgebungen werden noch veraltete Betriebssysteme und Software genutzt, für die es keinen Anbietersupport – oder Support im Allgemeinen – mehr gibt. Die Implementierung von Patches und Updates in OT-Systemen ist schwierig, da Ausfallzeiten und Produktionsverluste vermieden werden müssen.

Kein Überblick und ein unzureichendes Ressourcenmanagement

Viele Unternehmen haben kein umfassendes Inventarverzeichnis für ihre vernetzten OT-Ressourcen, was die Risikobewertungen erschwert. Schatten-OT-Geräte und nicht dokumentierte Endpunkte können unbekannte Sicherheitslücken aufweisen und damit zu weiteren Schwachstellen führen.

Ransomware und Cyberbedrohungen

Laut dem DBIR 2025 beeinträchtigen Ransomware-Angriffe die Fertigungsbranche stärker als andere Angriffsmethoden. Die Hacker nutzen häufig die unzureichende Segmentierung von IT- und OT-Systemen aus und breiten sich dann in der Umgebung aus, um die Betriebsabläufe zu stören.

Abbildung 2: Häufigste Angriffsmethoden in der Fertigungsbranche

Bei 44 % aller Angriffe, die im DBIR 2025 analysiert wurden, kam Ransomware zum Einsatz. Im Vorjahr waren es noch 32 %. Trotz dieses Anstiegs ist der Medianwert der gezahlten Lösegelder von 150.000 Dollar auf 115.000 Dollar gesunken. Das liegt eventuell auch daran, dass sich immer mehr betroffene Unternehmen weigern, die geforderten Summen zu zahlen.

KMU sind deutlich stärker von Ransomware-Angriffen betroffen – dort machen sie 88 % der Sicherheitsvorfälle aus. Bei größeren Unternehmen sind es nur 39 %.

Quelle: Abbildung 2: Verizon DBIR 2025 | Abbildung 3: Verizon

Komplexe gesetzliche Vorschriften und Compliance-Vorgaben

Unternehmen müssen diverse Cybersicherheitsstandards und Branchenvorschriften einhalten, zum Beispiel des National Institute of Standards and Technology (NIST), IEC 62443 und die Richtlinien der Cybersecurity & Infrastructure Security Agency (CISA). Die Compliance in globalen Lieferketten sicherzustellen, ist nicht einfach und sorgt vor allem in kleineren Unternehmen für zusätzliche Schwierigkeiten.

Risiken durch Drittanbieter und Lieferketten

Durch die Zusammenarbeit mit verschiedenen Anbietern, Auftragnehmern und Lieferanten entstehen mehrere Cyberschwachstellen in den vernetzten OT-Umgebungen. Effektive Identitätskontrollen und ein Zero-Trust-Zugriffsmanagement sind für alle Arten von Remote-Zugriff unverzichtbar.

Fehlende Kompetenzen und Fachkräftemangel

Es gibt nicht genügend Cybersicherheitsexperten, die auf OT-Sicherheit spezialisiert sind. Neue Mitarbeiter sind in puncto Cybersicherheit eventuell nicht ausreichend geschult, wodurch das Risiko von Insiderbedrohungen und menschlichen Fehlern steigt.

Entwicklung einer OT-Sicherheitsstrategie

Standards wie NIST CSF, NIST 800-53, ISO 27K, IEC 62443, NIST 800-82 und NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) ermöglichen die Entwicklung konsistenter Cybersicherheitsprogramme und maßgeschneiderter OT-Sicherheitsstrategien.

Abbildung 3: Komponenten einer umfassenden OT-Sicherheitsstrategie

Eine vereinfachte OT-Sicherheitsstrategie muss mindestens die folgenden Komponenten in einer Governance-Struktur enthalten:

- ein umfassendes Framework für das Ressourcenmanagement zur Erfassung der Systeme, des Alters, des End-of-Life-Status und der Software- oder Firmware-Versionen,
- regelmäßige Sicherheitsbewertungen des OT-Netzwerks zur Identifizierung von Schwachstellen oder Sicherheitslücken,
- eine mehrschichtige Netzwerkarchitektur mit einer sicheren DMZ (Demilitarized Zone) in der IT-Umgebung, die den Zugriff auf in der Cloud gehostete Anwendungen vereinfacht,
- kontinuierliche Bedrohungsüberwachung für eine bessere Erkennung in den OT-Netzwerken (Sie sollte sowohl die Netzwerk- als auch die Anwendungsebene umfassen und YARA-Regeln (Yet Another Recursive Acronym) zur Erkennung OT-spezifischer Malware nutzen.),
- OT-spezifische Threat Intelligence zur frühzeitigen Angriffserkennung und -abwehr (Es sollte sich um eine Kombination aus öffentlich verfügbarer und behördlicher Threat Intelligence, branchenspezifischen Bedrohungs-Feeds, Open-Source- und Community-Feeds sowie von Anbietern bereitgestellten und privaten Bedrohungs-Feeds handeln.),
- ein sorgfältig entwickelter und getesteter Incident Response Plan für eine frühzeitige Bedrohungserkennung.

Phasen der Transformation zu einem OT-Sicherheits-Framework

Die oben aufgeführten Phasen beschreiben den idealen Weg zur OT-Netzwerksicherheit. Wenn Sie sich für Verizon als Partner bei der Transformation entscheiden, werden wir höchstwahrscheinlich diese Schritte durchführen.

Ihr Unternehmen kann mit der Phase beginnen, die für Ihre Anforderungen und den Reifegrad Ihrer Betriebsprozesse am relevantesten ist. Parallel dazu sollten die folgenden OT-Governance- und Unternehmensbereiche in Angriff genommen werden:

- Unternehmensbereiche, die für Innovationen und zukünftige Entwicklungen zuständig sind,
- Strategieplanung und -umsetzung von Führungskräften auf Unternehmens- und Geschäftsbereichsebene,
- Ernennung eines Verantwortlichen (Champions) pro Fertigungsstätte oder Gruppe, um die Akzeptanz der OT-Planung und -Umsetzung zu optimieren.

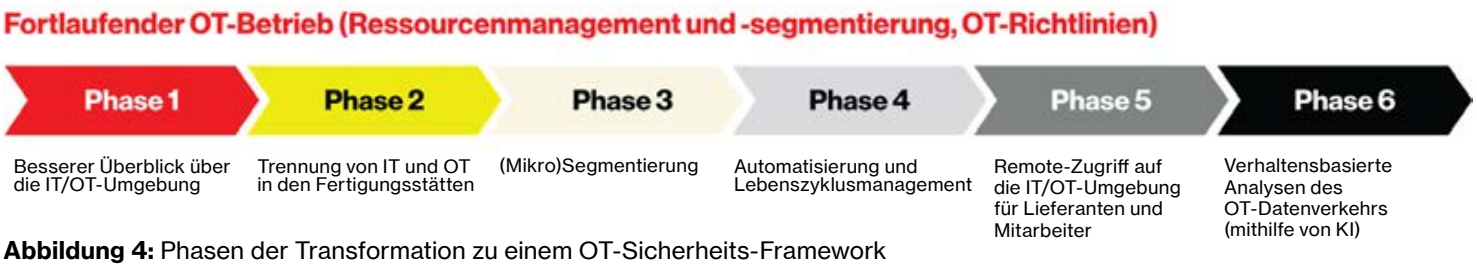


Abbildung 4: Phasen der Transformation zu einem OT-Sicherheits-Framework

PHASE 1: Besserer Überblick über die OT

Verizon Security Consulting Services helfen Ihnen, sich einen besseren Überblick über die vernetzten IT- und OT-Geräte in Fertigungsstätten, Warenlagern und ähnlichen Umgebungen zu verschaffen. Dazu werden alle vorhandenen Ressourcen erfasst und bewertet. Diese Bewertungen können entweder vor Ort oder per Remote-Zugriff durchgeführt werden, damit Sie einen umfassenden Überblick über die OT-Geräte und die Risikofaktoren erhalten.

PHASE 2: Trennung von IT und OT

Verizon arbeitet mit Ihnen zusammen an der Trennung des OT-Netzwerks von dem IT-Netzwerk. Dazu werden grundlegende Sicherheitsmaßnahmen eingeführt.

Zu diesem Zweck können physische oder virtuelle Firewalls implementiert oder umfunktioniert werden. Es müssen mindestens die folgenden Sicherheitsfunktionen aktiviert werden:

- Bedrohungsprävention,
- Malware-Schutz,
- DNS-Schutz (Domain Name System).

Unsere zertifizierten Experten unterstützen die Implementierung und Konfiguration der Sicherheitsmaßnahmen und die Managed Services-Teams von Verizon können die Umsetzung von unseren SOCs (Security Operations Centres) aus verfolgen.

PHASE 3: Mikrosegmentierung

In dieser Phase wird die OT-Umgebung segmentiert. Dazu werden spezifische Vorlagen entwickelt, die im gesamten Unternehmen eingesetzt werden können, um Prozesse zu standardisieren und zu vereinfachen. In dieser Phase werden die verschiedenen Sicherheitszonen und -richtlinien eindeutig festgelegt. Verizon Security Consulting Services können diese Vorlagen entwickeln und auf vorhandenen Sicherheitsvorkehrungen implementieren (Phase 2).

PHASE 4: Erste Automatisierungsschritte und Lebenszyklusmanagement

In dieser Phase werden die ersten spezifischen OT-Playbooks für die nahtlose Erstellung und Aktualisierung der OT-Segmentregeln entwickelt. Dazu werden vorhandene Tools und Ticketsysteme genutzt oder neue Skripte erstellt.

Mithilfe des Lebenszyklusmanagements wird sichergestellt, dass die Geräte stets mit den erforderlichen Sicherheitsmaßnahmen konform sind. Geräte, für die keine angemessene Wartung möglich ist, werden in eine separate Sicherheitszone verschoben.

Quelle: Abbildung 4: Verizon

PHASE 5: Remote-Zugriff auf die OT-Umgebung für Lieferanten und Mitarbeiter

In dieser Phase aktivieren wir moderne Services für den Remote-Zugriff nach dem Zero-Trust- und dem Least-Privilege- Prinzip (Nutzer erhalten nur unbedingt erforderliche Rechte). Anschließend implementieren wir Zugriffskontrollen für die Mitarbeiter und verschiedenen Lieferanten sowie kundensupport- und browserbasierte Lösungen.

PHASE 6: Aktivierung moderner – vorrangig KI-gestützter – Sicherheitsmaßnahmen und Automatisierungsprozesse

KI-gestützte Sicherheitsmaßnahmen, wie Funktionen zum Schutz vor Datenverlust (Data Loss Prevention, DLP), Intrusion Prevention Systems (IPS) und Sicherheitsanalysen mit UEBA-Services (User and Entity Behaviour Analytics), können zusätzliche Einblicke in den IT- und OT-Datenverkehr bieten. Diese Informationen können dann genutzt werden, um neue OT-Playbooks zu entwickeln oder vorhandene zu aktualisieren. Sie dienen auch der Verbesserung der OT-Incident-Response-Services und der Entwicklung von auf Deception-Technologie basierten Services für die OT.

Empfehlungen für das Betriebsmodell in OT-Umgebungen

Verizon hat bereits verschiedene Transformationsprogramme in Fertigungsumgebungen betreut und kann daher eine Betriebsstruktur für moderne Industrien empfehlen.

In diesem Diagramm ist die Struktur zu sehen, die Verizon bereits erfolgreich in IT/OT-Programmen genutzt hat.

Dies ist natürlich keine Patentlösung. Bei bestimmten kurzfristigen Zielen müssen Sie eventuell eine Struktur wählen, die sich besser für die angestrebten Ergebnisse eignet. Zur Unterstützung langfristiger Ziele sollten Sie unter Umständen das gesamte Unternehmen umgestalten und sämtliche Prozesse überarbeiten.

In der vorgeschlagenen Unternehmensstruktur werden alle bereichsübergreifenden, horizontalen Technologien und relevanten Ressourcen vom Gruppen-CIO (Chief Information Officer) verwaltet. Der CIO ist für die allgemeinen Services zuständig, die den Geschäftsbereichen bereitgestellt werden. Jeder Geschäftsbereich verfügt über einen Chief Technology Officer (CTO) oder einen CIO, der für die jeweils spezifische OT zuständig ist.

Die CIOs der einzelnen Bereiche unterstehen gemäß einer Matrixorganisation sowohl ihren Geschäftsbereichsleitern als auch dem Gruppen-CIO, gehören aber gleichzeitig dem CIO-Vorstand an. Der CIO-Vorstand ist für die allgemeine Ausrichtung und Governance der Technologien zuständig. Ein Chief Information Security Officer (CISO) wäre für die Sicherheitsbereiche zuständig und würde ebenfalls dem CIO-Vorstand angehören.

Verizon kann als Sicherheitsanbieter Managed Services für die Transformation und Integration sowie weitere Managed Security Services anbieten. Mit dieser Unterstützung können Sie sich dann ganz auf Ihre Wettbewerbsvorteile konzentrieren.

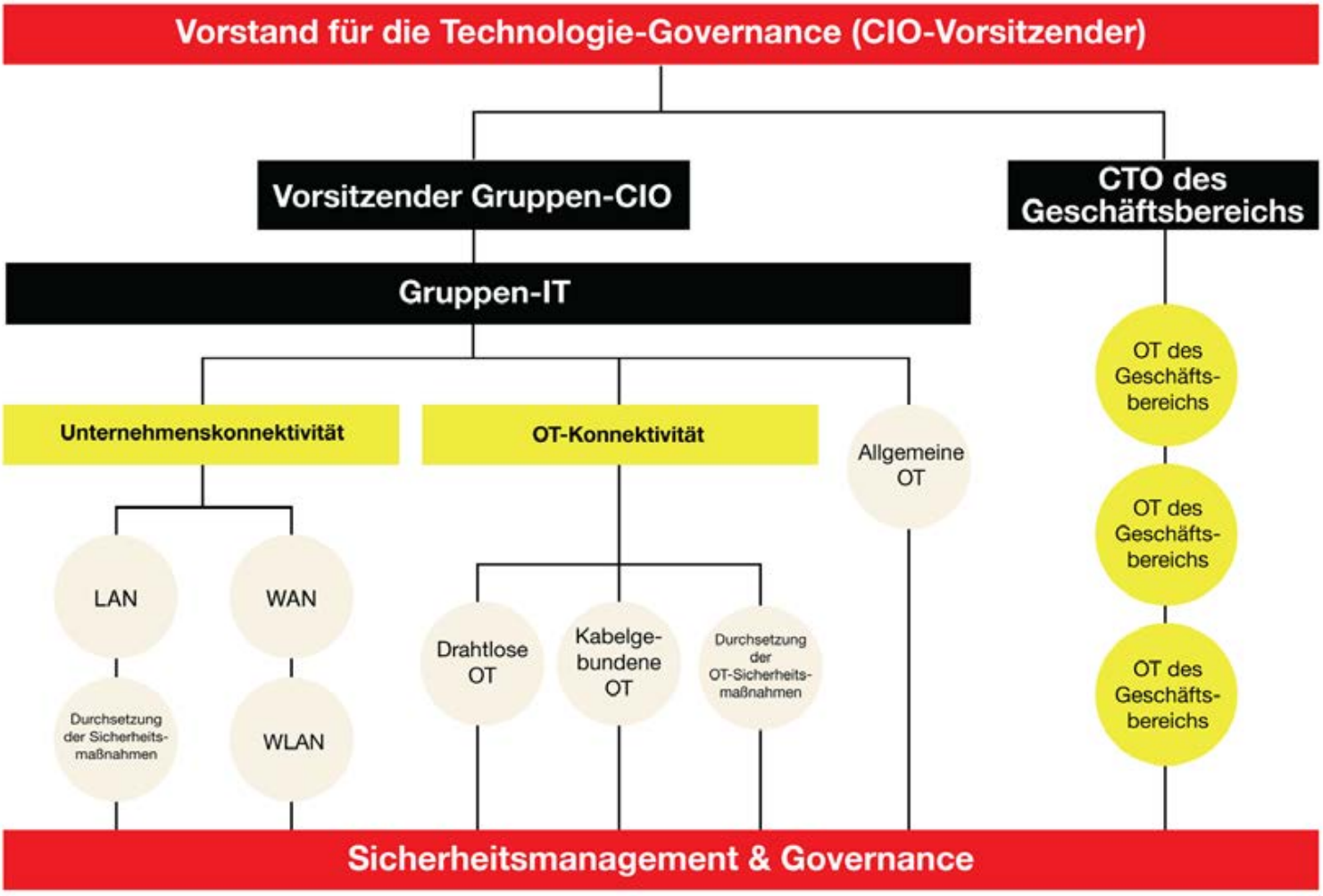


Abbildung 5: Ein Betriebsmodell für allgemeine/gruppenspezifische Technologie

Quelle: Abbildung 5: Verizon

Fazit

Mit einem solchen ganzheitlichen Ansatz für die OT-Sicherheit können Unternehmen die richtigen Sicherheitslösungen für ihre Anforderungen und ihr Budget implementieren. Verizon kann Ihnen helfen, sich optimal vorzubereiten, damit Sie Cyberangriffe effektiv abwehren können.

Weitere Informationen

Wenn Sie mehr darüber erfahren möchten, wie Verizon Ihnen helfen kann, Cyberbedrohungen abzuwehren und Ihr Unternehmen zu schützen, wenden Sie sich an Ihren Verizon Account Manager oder besuchen Sie unsere Website unter verizon.com/business/de-de/solutions/secure-your-business.

Autor und Mitwirkende

Autor

Marc Borking, OT SME und Principal Security Consultant, Consulting Services, Verizon Business

Mitwirkende

Ashish Khanna, Senior Director und Head of EMEA Security Consulting Services

Stephen Young, Director, Security Consulting Services

Beat Kueng, Associate Director, EMEA Security Solutions Architecture

Chris Zijderveld, Associate Director, Security Consulting Services

Ali Akl, Head of Risk and Resilience, EMEA Security Consulting Services

David Samreth, Principal Consultant, Consulting Services

Kundenreferenz: Globales Fertigungsunternehmen

Dieses globale Fertigungsunternehmen stellte fest, dass durch die zunehmende Automatisierung das Datenverkehrsaufkommen zwischen den IT- und OT-Systemen deutlich anstieg. Damit verbunden waren eine Zunahme der Sicherheitsrisiken und die Vergrößerung der Angriffsfläche. Um weiteres Wachstum zu fördern und gleichzeitig Mitarbeiter, Daten und Infrastruktur zu schützen, ergriff das Unternehmen proaktive Maßnahmen: Es führte eine umfassende Sicherheitsbewertung der vorhandenen OT-Umgebung durch und ermittelte seine Anforderungen.

Unternehmensanforderungen:

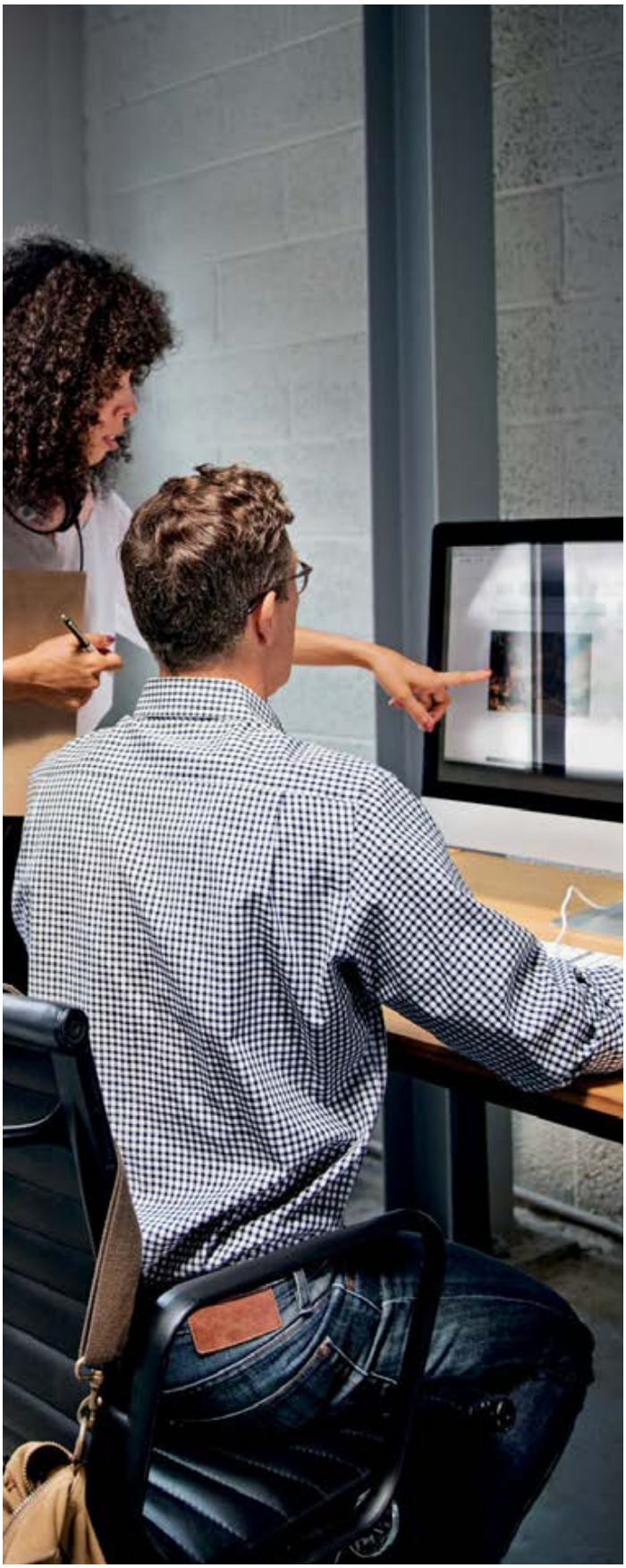
- Aktualisierung der vorhandenen Sicherheitsinfrastruktur, die nicht mehr den Anforderungen entsprach
- Umfassender Überblick über die aktuelle Architektur, Sicherheitsanforderungen, Segmentierungsrichtlinien, Datenströme im Unternehmen, Geräte und Prozesse
- Identifizierung der durch die fehlende Segmentierung entstandenen Sicherheitsrisiken
- Implementierung von Sicherheitsmaßnahmen zum Schutz der Unternehmensressourcen
- Abstimmung der Sicherheitsmaßnahmen und -richtlinien
- Schutz vor neuen globalen Sicherheitsrisiken
- Aktualisierung der Umgebung zur Unterstützung zukünftigen Wachstums und Sicherstellung der Compliance

Lösung:

- Erfassung und Bewertung der OT vor Ort in den Fertigungsstätten
- Aufbau einer Datenbank für die Konfigurationsverwaltung und einer passenden Architektur
- Erstellung von Vorlagen für Sicherheitsrichtlinien und die OT- und IT-Segmentierung
- Nutzung vorhandener oder neuer On-Premises-Firewalls und Konfiguration neuer Richtlinien, Segmente und Zonen vor der Übergabe an Verizon Managed Security Services
- LAN-Segmentierung in allen (über 25) Fertigungsstätten weltweit zur Erfassung von IoT-Geräten
- Schrittweise Verbesserung der Sicherheitsrichtlinien
- Automatisierte Playbooks zur Durchführung und Vereinfachung der OT-Segmentierung

Vorteile und Ergebnisse:

- Minimierung von Cyberrisiken durch die Trennung der IT- und OT-Netzwerke sowie der IT- und OT-Segmente
- Bessere Überwachung von Sicherheitsgeräten mit Verizon MSS
- Besserer Überblick über die Geräte- und Unternehmensdatenströme
- Bessere Compliance in Bezug auf die neuen Anforderungen und globalen Bedrohungen
- Aufbau einer neuen, auf zukünftiges Wachstum vorbereiteten Sicherheitsumgebung



Gewonnene Erkenntnisse

Die Umsetzung der Theorie in die Praxis dauert immer länger als veranschlagt. Das gilt für die meisten Projekte. In diesem Fall musste der Kunde vor dem Start den Projektumfang anpassen. Anschließend dauerte die Erfassung der erforderlichen Daten, die Kontaktaufnahme mit den zuständigen Personen, die Ermittlung der relevanten Switches und die Implementierung der korrekten Konfiguration länger als erwartet. Außerdem gab es längere Vorlaufzeiten aufgrund konkurrierender Prioritäten.

Gezielte Unterstützung von Kundenseite

Erst als ein Team gezielt mit der Unterstützung des Projekts beauftragt wurde, ging es zügiger voran. Sobald ein Standort abgeschlossen war, konnten die dort gesammelten Erfahrungen zu Prozessen, Designs und potenziellen Problemen auf die nächsten Standorte angewendet werden, sodass diese schneller fertiggestellt wurden. Die Erfassung von Netzwerkverkehr und Daten (über SPAN-Ports) war eine Herausforderung. Die Mikrosegmentierung dauerte aufgrund der potenziellen Beeinträchtigung des Geschäftsbetriebs länger. Die Datenströme der Ressourcen waren nicht immer bekannt, daher mussten erst die Protokolle verschiedener Firewalls analysiert werden, bevor eine „Deny“-Regel eingerichtet werden konnte. Zudem war auch die Ressourcenerkennung oft schwierig, da ältere Switches die Konfiguration oder zusätzliche Last nicht verarbeiten konnten. Dieses Problem wurde behoben, als der Datenverkehr über die Firewall geleitet wurde.

Abstimmen, informieren, einbeziehen und motivieren

Eine gute Koordination erwies sich als entscheidend. Für die Automatisierung mussten sich verschiedene Teams abstimmen, damit die Playbooks ordnungsgemäß funktionierten.

Es stellte sich heraus, dass Geräteanbieter relativ umfassenden Zugriff auf die Geräte hatten. Der Zugriff konnte beschränkt werden, aber nur auf SSH- (Secure Shell), RDP- (Remote Desktop Protocol) oder browserbasierten Zugriff.

Es empfiehlt sich, eindeutige und direkte Anfragen an Anbieter zu senden, um zeitnahe Architekturänderungen zu ermöglichen. Die Erfassung und Analyse des Datenverkehrs kann ressourcenintensiv sein, daher muss dieser Schritt sorgfältig geplant und im Budget berücksichtigt werden.

Die Transformation im Detail

Phase 1

- Durch die Ernennung eines zentralen Ansprechpartners konnten wir die Kommunikation optimieren und sicherstellen, dass alle Projektaktivitäten aufeinander abgestimmt waren.
- Die erste Analyse und Konfiguration wurden sorgfältig und präzise durchgeführt.
- Die Probleme bei der Erfassung des Netzwerkverkehrs konnten erfolgreich behoben werden, indem die Daten über die Firewall geleitet wurden.
- Das Startdatum des Projekts musste verschoben werden, doch dadurch konnten wir einen umfassenderen und besser abgestimmten Plan entwickeln, der letztendlich eine erfolgreiche Implementierung ermöglichte.

Phase 2

- Die Berücksichtigung der lokalen und gesetzlichen Vorschriften gehörte bei der ersten Implementierung der Firewalls zu den größten Herausforderungen.
- Wir konnten alle gesetzlichen Vorgaben erfüllen und eine konforme Einführung in jeder Region sicherstellen.
- Die erste Segmentierung war recht zeitaufwendig, aber unverzichtbar, um für einen reibungslosen, schnelleren und wiederholbaren Prozess an den anderen Standorten zu sorgen.

Phase 3

- Der zweite Teil der Mikrosegmentierung musste äußerst sorgfältig und schrittweise vorgenommen werden, um Störungen zu vermeiden.
- Entscheidend dabei waren die Informationen von den lokalen Ansprechpartnern.
- Für präzise Ergebnisse wurden die Firewall-Protokolle umfassend analysiert, um die Datenströme der Ressourcen im Detail nachzuvollziehen.

Phase 4

- Die Abstimmung der verschiedenen Teams war eine wichtige Voraussetzung für die Entwicklung effektiver und effizienter Automatisierungs-Playbooks.
- Dank der gut koordinierten Teams konnten wir eine nahtlose Lösung erstellen.

Phase 5

- Verizon unterstützte das Unternehmen bei dem Wechsel zu einem stärker kontrollierten Zugriffsmodell für Anbieter und Lieferanten.
- Dazu gehörte die Einführung eines neuen Standards, der den Zugriff auf SSH-, RDP- oder browserbasierte Methoden beschränkt.
- Es wurden direkte Anfragen gesendet und auf eine enge Zusammenarbeit mit den Anbietern geachtet, um sicherzustellen, dass sie den notwendigen Zugriff erhalten, aber auch mit der neuen Architektur konform sind.

Phase 6

- Verhaltensanalysen lieferten wichtige Informationen und ermöglichten einen besseren Einblick in die Netzwerkaktivitäten.