Sicher in die Zukunft:

Schutz von OT-Infrastrukturen während der digitalen Transformation

verizon business

Sicher in die Zukunft

Ein Gleichgewicht zwischen einem hohen Innovationstempo und zuverlässiger Sicherheit zu finden, ist oft nicht einfach.
Hier erfahren Sie, wie diese Gratwanderung gelingt.

Die größten Geschäftschancen bergen häufig auch die größten Risiken. Die Digitalisierung ist ein perfektes Beispiel dafür.

Einerseits kann die digitale Transformation die Effizienz steigern, die Produktqualität verbessern, das Kundenerlebnis optimieren und die betriebliche Resilienz erhöhen. Andererseits kann sie unbeabsichtigte Cybersicherheitsrisiken zur Folge haben – insbesondere bei der Betriebstechnologie (Operational Technology, OT), die für die Produktion unerlässlich ist.

Die OT-Sicherheit muss in zahlreichen Branchen berücksichtigt werden, unter anderem der Fertigung, der Öl- und Gasindustrie, dem Versorgungssektor und dem Transportwesen. Sie ist ein unverzichtbarer Bestandteil der kritischen Infrastrukturen, auf die wir alle angewiesen sind. Auch die Gewinne Ihres Unternehmens hängen von ihr ab.

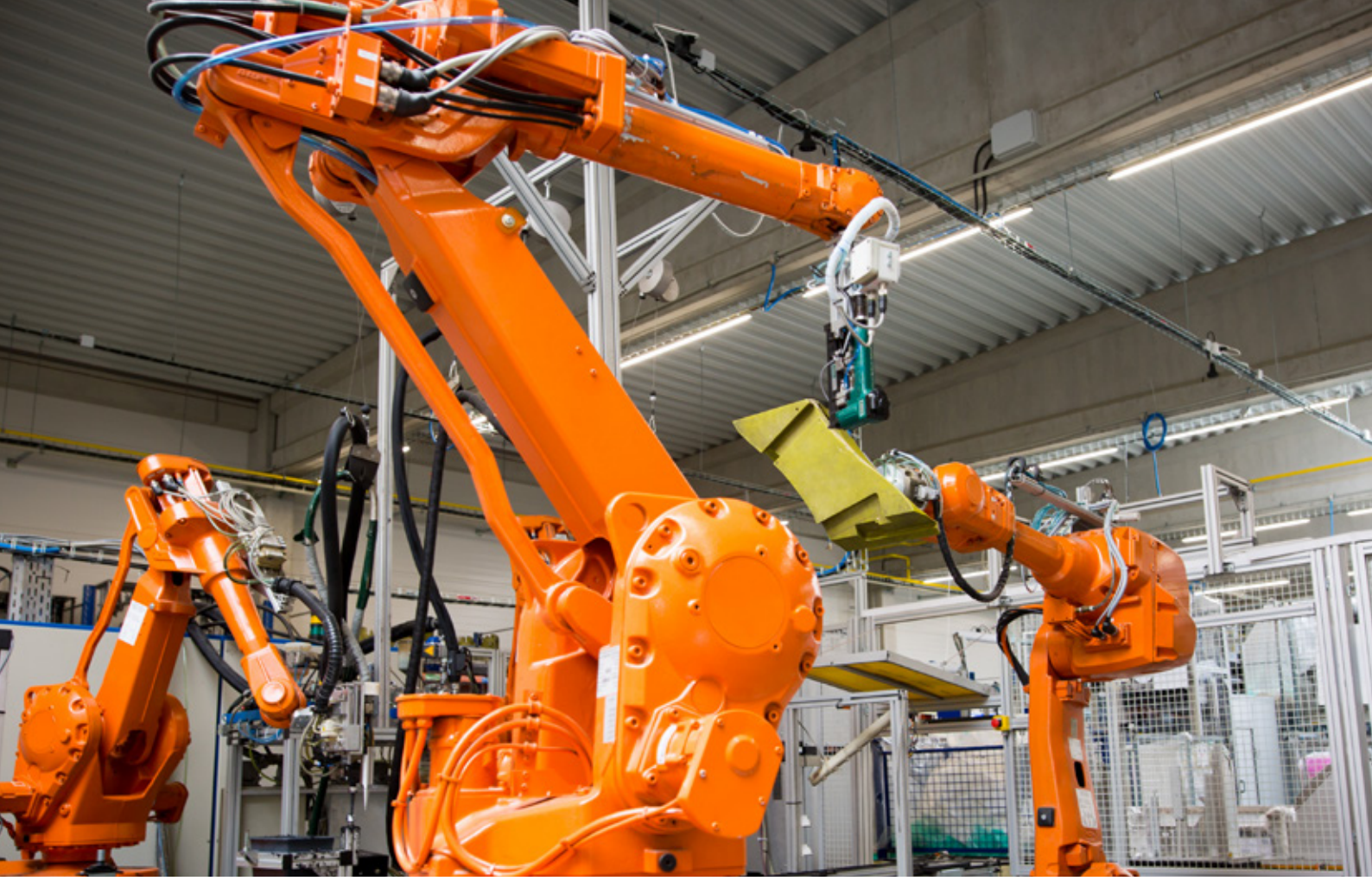
Glücklicherweise sind viele der Erkenntnisse, die bei der Digitalisierung einer Branche gewonnen werden, auch für andere relevant. So können Sie Innovationen vorantreiben, ohne Ihr Unternehmen unnötigen Risiken auszusetzen.

Wir möchten die Herausforderungen keinesfalls herunterspielen: Fertigungsunternehmen sind realen Cybersicherheitsbedrohungen ausgesetzt. Aber wir konzentrieren uns hier auf positive, praktische Schritte, mit denen Sie Ihre OT schützen und von den Vorteilen der Digitalisierung profitieren können.

Wenn Sie die Herausforderungen der OT-Sicherheit kennen, können Sie sie auch bewältigen. Verizon kann Ihnen dabei helfen, Ihr Unternehmen zu schützen und voranzubringen.

Setzen Sie auf den ganzheitlichen Cybersicherheitsansatz von Verizon

Die umfassenden Lösungen von Verizon für die IT- und OT-Sicherheit werden bereits von Tausenden Unternehmen weltweit genutzt. Unser ganzheitlicher Cybersicherheitsansatz passt sich an die Anforderungen, finanziellen Mittel und Ziele der digitalen Transformation Ihres Unternehmens an.



Die digitale Transformation ist unumgänglich

Wenn Sie dies lesen, gehört die digitale Transformation höchstwahrscheinlich zu Ihren Prioritäten. Das ist bei den meisten Fertigungsunternehmen inzwischen der Fall. Seit die „Fertigung 4.0“ in der Branche zum Diskussionsthema geworden ist, ist das Transformationstempo erheblich gestiegen.

> Durch die digitale Transformation lässt sich der Durchsatz deutlich erhöhen, potenziell um 10 bis 30 %.
>
> Quelle: McKinsey & Company, „Preparing for the next normal via digital manufacturing’s scaling potential“, 2020

Tatsächlich erfordert die starke Vernetzung der modernen Welt resiliente, agile und optimierte Lieferketten – und dazu müssen die Unternehmen möglichst schnell digitalisiert werden. Technologien wie das Industrielle Internet der Dinge (Industrial Internet of Things, IIoT) und künstliche Intelligenz (KI) sind inzwischen Branchenstandard. Damit lassen sich die notwendige Transparenz und Koordination für das proaktive Inventarmanagement, eine effizientere Produktion und ein besserer Schutz vor Systemausfällen erreichen. Die digitale Integration macht auch vor Kundeninteraktionen nicht halt – Unternehmen können sich wichtige Einblicke in Echtzeit verschaffen und Angebote personalisieren, um die Kundenzufriedenheit und -treue zu verbessern.

Die Digitalisierung verbessert jedoch nicht nur die betriebliche Effizienz, sondern kann auch bei der Bewältigung äußerer Einflüsse helfen. Aufgrund von geopolitischen Konflikten und Fachkräftemangel sind Unternehmen auf flexible, digitale Prozesse angewiesen, die schnell an Nachfrageschwankungen angepasst werden können. Außerdem kann die Digitalisierung die Umgebungsüberwachung, den Energieverbrauch und die Compliance mit gesetzlichen Vorgaben verbessern, damit sowohl die Kundenerwartungen als auch die Unternehmensziele erfüllt werden.

Die Transformation muss auch nicht kostspielig sein. Mit der Digitalisierung lassen sich sogar erhebliche Kosteneinsparungen erzielen, da durch Abfallreduzierung und vorausschauende Wartung die Effizienz verbessert wird. Wenn Sie die Workflows und Prozesse digitalisieren, erhalten Sie auch mehr Daten, die wichtige Einblicke ermöglichen. So können Sie fundierte Entscheidungen treffen und effektiver auf Marktschwankungen, Änderungen der gesetzlichen Vorgaben und unerwartete Störungen reagieren. In der heutigen unbeständigen Welt ist dies wichtiger als je zuvor.

In Unternehmen sollte jedoch stets darauf geachtet werden, dass durch die Änderungen nicht versehentlich Sicherheitslücken entstehen.

Die Bedrohungslandschaft wird immer komplexer

Digitale Technologien haben allerdings nicht nur neue Möglichkeiten für bahnbrechende Verbesserungen, sondern auch potenzielle Einfallstore für Cyberangriffe eröffnet.

Die Integration von Informationstechnologie (IT) mit bisher isolierten OT-Umgebungen und die zunehmende Verbreitung von vernetzten IIoT-Geräten und KI haben die Angriffsfläche von Unternehmen stark vergrößert.

OT-Systeme nutzen beispielsweise häufig noch veraltete Kommunikationsprotokolle, die von modernen Sicherheitstechnologien nicht immer unterstützt werden. Viele OT-Geräte weisen unter Umständen nicht gepatchte Sicherheitslücken auf und verfügen nicht über die zuverlässigen Sicherheitsfunktionen moderner IT-Systeme. Die längere Nutzungsdauer von OT-Geräten hat zudem zur Folge, dass veraltete Software und Firmware deutlich länger genutzt werden, was zu weiteren Schwachstellen führt.

> Die Integration von Informationstechnologie (IT) in bisher isolierte OT-Umgebungen ... hat die Angriffsfläche von Unternehmen stark vergrößert.

Durch die KI entstehen neue Angriffsvektoren, über die isolierte OT-Geräte und sensible Daten zugänglich werden könnten. Zudem steigt die Bedrohung durch nicht-menschliche Angreifer. Das erschwert wiederum das Identitätsmanagement.

Wenn Sie KI-Tools trainieren und verwenden, sollten Sie neue Sicherheitsfunktionen und -maßnahmen in Betracht ziehen, um Ihre Infrastruktur vor Angriffen und Ihre Daten vor Missbrauch zu schützen. Auch die Datenhoheit ist ein wichtiger Punkt, da Unternehmen wie Ihres Daten an verschiedenen Standorten generieren, anreichern, verarbeiten und speichern müssen. Der Schutz geistigen Eigentums und personenbezogener Daten vor datenhungrigen KI-Tools sollte zu Ihren Prioritäten gehören.

Eine unzureichende Vorbereitung kann Sie teuer zu stehen kommen

Cyberkriminelle wissen, dass sich Fertigungsunternehmen nahezu keine Ausfallzeiten leisten können. Sie wissen auch, dass diese Unternehmen über wertvolles geistiges Eigentum verfügen. Daher ist es kaum verwunderlich, dass System-Intrusion-Angriffe im Fertigungssektor 2025 stark zugenommen haben – die Zahl der gemeldeten Sicherheitsvorfälle ist fast doppelt so hoch wie 2024 (laut Data Breach Investigations Report 2025 von Verizon).

- **Phishing- und Social-Engineering-Angriffe** werden genutzt, um Mitarbeiter durch Täuschungsmanöver dazu zu bringen, sensible Informationen preiszugeben oder schädliche Aktivitäten auszuführen. Solche Angriffe richten sich häufig gegen Personen, die sowohl auf das IT- als auch das OT-Netzwerk zugreifen können.
- **Lieferkettenangriffe** nutzen Sicherheitslücken in dem komplexen Netzwerk aus Lieferanten und Partnern aus.
- **Angriffe auf industrielle Steuersysteme (ICS)** sind komplexe Bedrohungen, mit denen gezielt kritische Infrastrukturen und industrielle Prozesse gestört werden sollen.
- **Zero-Day-Angriffe** nutzen bislang unbekannte Sicherheitslücken in Technologien aus und sind eine ständige und wachsende Gefahr.
- **Nicht verwaltete und nicht geschützte IoT-Geräte** in Produktionsumgebungen können ebenfalls als Einfallstor für Cyberangriffe ausgenutzt werden.

> System-Intrusion-Angriffe haben 2025 im Fertigungssektor stark zugenommen – die Zahl der gemeldeten Sicherheitsvorfälle ist fast doppelt so hoch wie 2024.
>
> Quelle: Verizon, Data Breach Investigations Report 2025

Angriffe können jedoch nicht nur hohe Kosten, sondern auch erhebliche Störungen der Produktion, den Diebstahl wertvollen geistigen Eigentums und sensibler Daten, die Beschädigung physischer Assets und die Beeinträchtigung der Compliance zur Folge haben. Bei Angriffen auf kritische Infrastrukturen ist unter Umständen sogar die öffentliche Sicherheit in Gefahr.

Die Behebung dieser Cybersicherheitsprobleme wird häufig durch mehrere Faktoren erschwert. Dazu gehört zum Beispiel die Verwaltung akkurater und aktueller Inventarverzeichnisse für die rasant wachsende Anzahl an OT- und IIoT-Geräten. Es gibt auch viel weniger spezifische Threat Intelligence für OT- und IIoT-Infrastrukturen als für den IT-Bereich. Grundlegende Unterschiede in den Prioritäten und Ausrichtungen der IT- und Industrieumgebungen können die effektive Implementierung von Cybersicherheitsmaßnahmen für die OT ebenfalls erschweren.

Sollte Ihr Unternehmen im Rahmen der digitalen Transformation die Konvergenz von IT und OT anstreben, muss es unbedingt auch die Sicherheitsmaßnahmen anpassen.

Lösungen für die Herausforderungen globaler Fertigungsunternehmen

Fertigungsunternehmen nutzen häufig äußerst komplexe und geografisch verteilte IT- und OT-Umgebungen. Diese Systeme bestehen aus einer Kombination von modernen und älteren Technologien sowie zahlreichen vernetzten Geräten, was das Sicherheitsmanagement erheblich erschwert.

Aufgrund der enormen Ausmaße ist ein ausgereifter und einheitlicher Cybersicherheitsansatz notwendig.

Netzwerke und Unternehmenskulturen, die bisher getrennt waren, müssen jetzt integriert werden. Die Unterschiede in Bezug auf Prioritäten und Prozesse von IT- und OT-Teams müssen ausgeräumt werden, um einen kohärenten Sicherheitsansatz zu ermöglichen.

Fertigungsunternehmen nutzen zudem komplexe und oft sehr lange Lieferketten. Da diese globalen Lieferwege stark vernetzt sind, hat ein Sicherheitsvorfall an einem Punkt in der Kette oft Konsequenzen für alle Beteiligten. Fertigungsunternehmen müssen sicherstellen, dass alle Lieferanten strikte Sicherheitsrichtlinien einhalten, um die Angriffsanfälligkeit zu minimieren.

Werden Cyberangriffe nicht eingedämmt, drohen diesem Sektor gravierende Konsequenzen – nicht nur für den Geschäftsbetrieb, sondern auch für die Umwelt und die Menschen in ihrer Nähe. Ein Büro kann beispielsweise einfach die Systeme herunterfahren, um Cyberbedrohungen einzudämmen, aber OT wie Kühl- oder Stromsysteme müssen eventuell aus Sicherheitsgründen durchgehend betrieben werden. Die Vermeidung von Industrie- und Arbeitsunfällen hat immer höchste Priorität.

Die historisch entstandenen Diskrepanzen zwischen den Prioritäten und Prozessen von IT- und OT-Teams müssen überwunden werden, um einen kohärenten Sicherheitsansatz zu ermöglichen.

Auch die Notwendigkeit eines kontinuierlichen Betriebs kann dazu führen, dass Abstriche bei den Sicherheitsmaßnahmen gemacht werden. Eventuell zögert die Unternehmensleitung, notwendige Updates zu implementieren oder Systeme für Wartungsarbeiten offline zu nehmen, doch dadurch steigt das Risiko eines Cyberangriffs.

Vielleicht stehen Unternehmen auch nur knappe Budgets zur Verfügung, sodass die Mittel nicht für die neuesten Sicherheitstechnologien oder Unterstützung durch Experten reichen. Die effiziente Verteilung der Sicherheitsressourcen auf diverse globale Standorte und unterschiedliche Geschäftsbereiche kann ebenfalls zur Herausforderung werden. Besonders schwierig wird es, wenn das Cybersicherheitsbudget vom IT-Team und nicht vom gesamten Unternehmen getragen wird. OT- und IT-Budgets müssen kombiniert werden, wenn alle Unternehmensbereiche angemessen geschützt werden sollen.

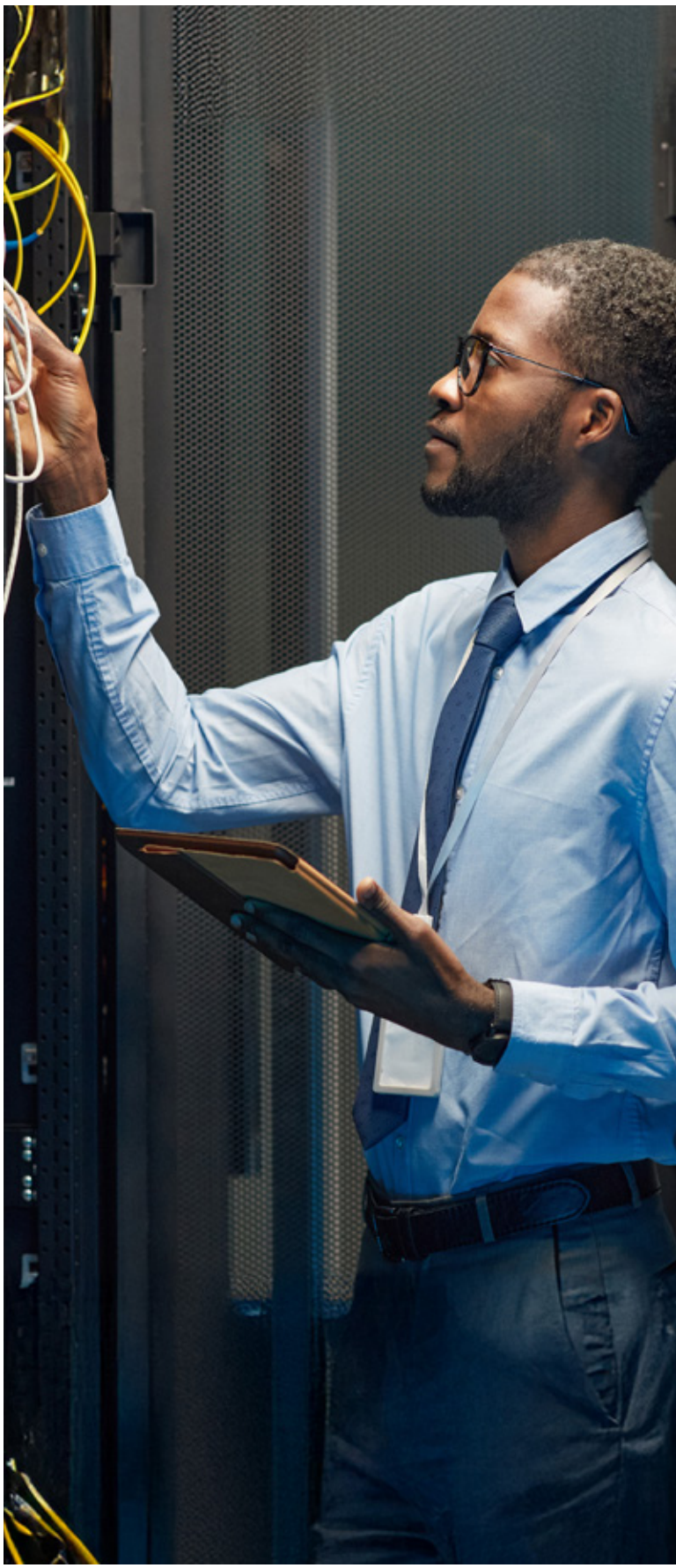
Ein weiteres Problem ist, dass ältere OT-Systeme oft eng mit den Produktionsprozessen verzahnt sind. Die Aktualisierung dieser Systeme ist oft schwierig und kostspielig, sodass riskante Sicherheitslücken entstehen. Die Aufarbeitung dieser technischen Altlasten in OT-Umgebungen und die Sicherstellung der unterbrechungsfreien Produktion sind nur mit sorgfältiger Planung, Unterstützung durch Experten und einer schrittweisen Modernisierung möglich.

Ein Überblick über die globalen Cyberbedrohungen

Der jährlich erscheinende Data Breach Investigations Report (DBIR) von Verizon zeigt zuverlässig die Entwicklungen in der Cybersicherheitslandschaft auf und spiegelt unser Engagement für einen datengestützten Sicherheitsansatz wider.

Der DBIR ist eine fundierte, vertrauenswürdige Informationsquelle zu Cybersicherheitsverletzungen. Er deckt die wichtigsten Risiken für die Fertigung und andere Branchen auf und enthält Empfehlungen von Experten zur Behebung dieser Probleme. Im Bericht für 2025 wurden über 22.000 reale Sicherheitsvorfälle analysiert und dabei wertvolle Erkenntnisse gewonnen, die Ihnen beim Schutz vor neuen Bedrohungen helfen können.

Laden Sie den Bericht gleich herunter.



Umfassende Cybersicherheit für eine sicherere OT

Durch die Zusammenarbeit mit einem auf diesen Bereich spezialisierten Partner lassen sich viele der komplexen Herausforderungen der OT-Cybersicherheit bewältigen.

Verizon hat bereits vielen Unternehmen geholfen, ihre Cybersicherheitsmaßnahmen zu verstärken. Wir bieten einen umfassenden Schutz, damit nicht nur die IT-Infrastruktur, sondern auch zunehmend vernetzte OT-Umgebungen abgesichert sind.

Dabei nutzen wir nicht nur unsere breite Palette an eigenen Lösungen, sondern arbeiten auch mit anderen Sicherheitsanbietern zusammen, um individuelle OT-Sicherheitskonzepte zu entwickeln. Auf diese Weise können wir maßgeschneiderte Lösungen für die spezifischen Anforderungen Ihres Unternehmens erstellen, darunter auch die digitale Transformation.

Wenn Sie branchenführende Sicherheit für die OT-Infrastruktur Ihres Unternehmens suchen, kann Verizon ein Assessment vor Ort durchführen, um die kosteneffektivsten und wichtigsten Bereiche mit Verbesserungspotenzial zu ermitteln.

Die OT ist das Herz Ihres Unternehmens – sie sollte unbedingt angemessen geschützt werden.

Kundenreferenz: Schutz eines modernen Fertigungsunternehmens

Ein globaler Getränkehersteller für Spirituosen, Wein und Softdrinks stellte fest, dass seine Sicherheitsinfrastruktur den neu eingeführten vernetzten Technologien nicht gewachsen war. Er arbeitete mit Verizon an der zügigen Aktualisierung seiner Sicherheitsmaßnahmen, um die neuen Anforderungen zu erfüllen und die Sicherheitsmechanismen in der Nähe der Daten zu installieren.

Die Lösung von Verizon:

- Installation neuer On-Premises-Firewalls und Konfiguration neuer Richtlinien/ Zonen
- Verantwortung für deren Management über die Verizon Managed Security Services
- Segmentierung von OT- und IT-LAN für über 20 globale Fertigungsstätten
- Sicherheitsrichtlinienbasierte Interaktionen mit minimaler Beeinträchtigung der Produktion

Das Ergebnis:

- Eine neue Sicherheitsumgebung für zukünftiges Wachstum
- Bessere Überwachung von Sicherheitsgeräten
- Reduzierung der Cyberrisiken durch die Trennung von IT- und OT-Netzwerken
- Besserer Überblick über die Geräte- und Unternehmensdatenströme

Sie möchten gern mehr über die digitale Transformation erfahren?

Lesen Sie die wichtigsten Erkenntnisse und Tipps von Branchenexperten rund um die neuesten Technologien für Ihren Weg zum vernetzten Unternehmen.

Hier erfahren Sie mehr über die Lösungen von Verizon für die Fertigungsbranche.

Entdecken Sie die neuesten zukunftsweisenden Tools, die Herstellern Wettbewerbsvorteile verschaffen.

Besuchen Sie ein Innovationszentrum

Weitere Informationen zum Schutz von OT-Umgebungen

Laden Sie unser detailliertes Whitepaper zum Schutz von OT herunter.

verizon business