Datensicherung in der digitalen Fabrik: So schützen sie eine vernetzte Fabrik vor Bedrohungen

verizon business

Wenn Fertigungsunternehmen modernste Konnektivität und Technologien nutzen, setzen sie ihre vertraulichen Daten und ihren Geschäftsbetrieb möglicherweise Cyberbedrohungen aus. Deshalb ist der Schutz vernetzter Fabriken vor Cyberangriffen für die Integrität, Vertraulichkeit und Verfügbarkeit geschäftskritischer Daten unverzichtbar.

Im Folgenden finden Sie Informationen über Strategien und Best Practices zur Datensicherung in der digitalen Fabrik.

Die wichtigsten Bedrohungen in der Fertigungsbranche

Sowohl die Häufigkeit als auch die Komplexität von Cyberbedrohungen steigen unaufhörlich. Dieser beunruhigende Trend stellt eine kontinuierliche Gefahr für vertrauliche Daten und eine nicht zu unterschätzende Herausforderung dar.

Zu den Risiken gehören:

- Ransomware-Angriffe: Daten werden verschlüsselt, bis ein Lösegeld gezahlt wird.
- Phishing: Benutzer werden mit einer betrügerischen E-Mail oder Website dazu verleitet, vertrauliche Daten preiszugeben oder Malware herunterzuladen.
- Man-in-the-Middle Angriffe: Hacker fangen Gespräche ab oder manipulieren sie, damit die Teilnehmer Informationen mit ihnen (statt mit ihrem beabsichtigten Gesprächspartner) teilen.

Taktiken wie diese werden zum Stehlen verschiedenster Arten von Daten genutzt, von vertraulichen Forschungs- und Entwicklungsdokumenten und geistigem Eigentum über Marktforschungsergebnisse bis hin zu vertraulichen Kunden- und Finanzdaten.

Die Fertigung ist nun die am stärksten von Cyberangriffen betroffene Branche

Fertigungsunternehmen werden inzwischen sogar häufiger angegriffen als Finanzdienstleister und Versicherungen.

Durch die Coronapandemie sind die mit Lieferketten und Remote-Arbeit verbundenen Cybersicherheitsrisiken – wie Versorgungsengpässe, Verzögerungen zeitkritischer Prozesse oder die professionelle Nutzung privater Geräte in ungesicherten Netzwerken – nur zu gut bekannt. Infolgedessen ist das Management des Gerätezugriffs auf Unternehmen nun eine komplexe Aufgabe.

Im Jahr 2022 stellte ein japanischer Autohersteller wegen eines mutmaßlichen Angriffs auf einen Zulieferer die Arbeit in all seinen Fabriken ein. Von dem eintägigen Stillstand waren 14 Fabriken und die Produktion von 13.000 Fahrzeugen betroffen.

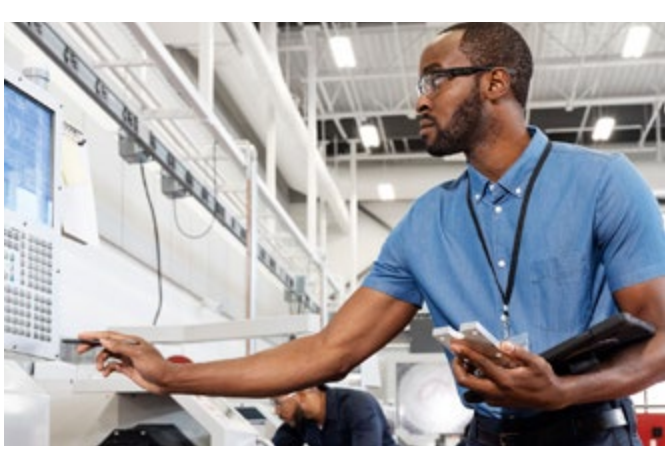
In einem anderen Angriff gelang es Hackern, sich über die Infrastruktur eines Anbieters cloudbasierter Sicherheitskameras Zugriff auf die Kameras in den Fabriken und Lagerhallen eines bekannten US-amerikanischen Autoherstellers zu verschaffen.

Cybersicherheit und Industrie 4.0: Warum intelligente Fabriken modernere Sicherheit benötigen

Wenn Fertigungsunternehmen im Rahmen des Übergangs zu Industrie 4.0 Maschinen, Produkte, Mitarbeiter und diverse Partnerunternehmen miteinander vernetzen, wirft dies neue Herausforderungen auf.

Zur Nutzung moderner Fertigungstechnologien müssen Gerätesensoren, HLK-Anlagen und andere OT-Komponenten (Operational Technology), die bislang streng von der IT getrennt waren, sowohl mit der IT-Infrastruktur des eigenen Unternehmens als auch mit der von Lieferkettenpartnern verbunden werden.

Diese OT-Komponenten sind jedoch in aller Regel nicht so gut geschützt wie Laptops, Smartphones und Tablets. In vielen Unternehmen werden sie auch weniger streng überwacht. Oft handelt es sich um ältere Systeme ohne moderne Bedrohungserkennungs- und -abwehrfunktionen. Das schränkt die Fähigkeit der Hersteller ein, ihr gesamtes Technologie-Ökosystem und alle potenziellen Gefahren zu bewerten.



Zudem gelten für die OT möglicherweise nicht dieselben Anforderungen bezüglich der Daten-Governance wie für die IT. Entscheidungen über die OT werden gewöhnlich im Geschäftsbereich Fertigung und ohne Einbeziehung des Unternehmens-IT- und Sicherheitspersonals getroffen.

All diese Herausforderungen und Einschränkungen einerseits und ihre kritische Rolle in der Fertigung andererseits machen die OT zu einem verlockenden Ziel für Hacker. Im vergangenen Jahr ist die Anzahl der erfolgreichen Angriffe auf OT-Technologie um alarmierende 50 Prozent gestiegen.

Doch in den sich rasch weiterentwickelnden Fertigungsumgebungen gibt es noch viele weitere potenzielle Einfallstore, die für Cyberangriffe ausgenutzt werden können. Daher benötigen fertigende Unternehmen mit brandneuen Technologieinfrastrukturen noch modernere und robustere Sicherheitsmaßnahmen.

Viele intelligente Fabriken sind nicht ausreichend geschützt

Im Jahr 2021 bewertete McKinsey den Reifegrad der Cybersicherheitsmaßnahmen von mehr als 100 Unternehmen und Institutionen in verschiedenen Branchen. Die Studie kam zu dem Ergebnis, dass die Mehrzahl der Unternehmen und Institutionen in allen Branchen (trotz erheblicher Fortschritte im Bankwesen und im Gesundheitswesen) noch weit von einem adäquaten Schutz wertvoller Daten vor neuen Bedrohungen und Angriffen entfernt war. Die unzureichende Datensicherung ist vielerorts auf ein mangelndes Verständnis der den eigenen Systemen drohenden Gefahren und auf unzureichende Investitionen in die IT/OT-Cybersicherheit zurückzuführen.

Unzureichend geschützten Unternehmen drohen:

- finanzielle Konsequenzen
- der Verlust geistigen Eigentums bzw. vertraulicher Daten
- Produktivitätseinbußen
- Lieferkettenprobleme
- Verlust des Kunden- und Partnervertrauens

Aufbau unerlässlicher Cybersicherheitsvorrichtunge

Als ersten Schritt empfehlen wir, sicherzustellen, dass die Mitarbeiter mit der Nutzung von Sicherheitssoftware vertraut sind und dass diese regelmäßig aktualisiert wird und alle verfügbaren Patches eingespielt werden.

Veraltete Geräte im Internet der Dinge (IoT) können Angreifer regelrecht anziehen. Doch Hersteller sollten bei proaktiven Firmware-Updates die Leistungsgrenzen dieser Geräte berücksichtigen. Viele IoT-Geräte haben beispielsweise eine so begrenzte Bandbreite und Konnektivität, dass ein Upgrade sie leicht überlasten und den Ausfall geschäftskritischer Funktionen verursachen könnte. Das richtige Gleichgewicht zwischen der Sicherung der Geräte und der Aufrechterhaltung ihrer Leistung ist nicht immer leicht zu finden, aber dennoch ausschlaggebend.

Bei 80 Prozent der Datendiebstähle werden gestohlene Anmeldedaten missbraucht. Deshalb sollten Hersteller das IoT Credentialing nutzen und nur „berechtigte" Geräte in ihr Netzwerk einbinden.

Sie sollten Datenspeicher in der Cloud und On-Premises nutzen – da es riskant wäre, alle wichtigen Daten an einem Ort zu speichern – und auf deren korrekte Konfiguration achten. Mithilfe von Cloud-Services, Managed Security Services und anderen Ressourcen können Hersteller sich proaktiv über neu aufkommende Bedrohungen auf dem Laufenden halten und sich vor ihnen schützen.

Vor der Implementierung jeder neuen Technologie sollten Unternehmen ihren Reifegrad bezüglich der Cybersicherheit, ihre Bereitschaft zur Abwehr eines Cyberangriffs und das Risikoprofil der neuen Technologie überprüfen. Mit Tests, die einen Cyberangriff simulieren, lassen sich Schwachpunkte im IoT-Netzwerk eines Unternehmens finden.

Bei einer aktuellen Umfrage des Manufacturing Leadership Council stuften 83 Prozent der Befragten die Cybersicherheit als sehr wichtige Geschäftsangelegenheit ein. 79 Prozent rechnen damit, dass die Anzahl der Angriffe im nächsten Jahr steigen wird, doch nur 40 Prozent sagten, dass sie ein großes Vertrauen in die unternehmensinterne Expertise zum Thema Cybersicherheit haben.

Aufbau eines robusten Cybersicherheitsframeworks für besseren Schutz

Eine kritische, aber oft vernachlässigte Komponente einer effektiven Cybersicherheit ist ein gutes Programm für die Cybersicherheits-Governance mit den folgenden Informationen:

- Risikokarten, die das Risikoprofil des Unternehmens zeigen
- einem Framework für die Risikoeskalation mit Schwellenwerten für die Meldung
- einem Plan für die rasche Reaktion auf und Eindämmung von Bedrohungen, der Aktionen in Abhängigkeit vom Risikoprofil priorisiert
- einem aktuellen Katalog aller OT- und IT-Ressourcen, den von ihnen erfassten Daten und allen Beziehungen zwischen den beiden
- Mitarbeiterschulungen unter besonderer Berücksichtigung von Fernarbeitern und Risikogruppen, die mit sensiblen Daten, industriellen Steuerungssystemen oder verbundenen Produkten arbeiten
- Backups geschäftskritischer Daten, die eine einfache Wiederherstellung unterstützen
- Sicherheitspatches und Updates für industrielle Steuerungssysteme und Sicherheitsfunktionen
- Verschlüsselung von Daten mit Schlüsseln, die sicher aufbewahrt und in Backups inbegriffen sind

Zudem sollten Hersteller Manager einsetzen, die Risiken effektiv einschränken und fundierte Investitionsentscheidungen treffen können und mit den komplexen Details industrieller Steuerungssysteme und der mit ihnen verbundenen Produkte vertraut sind. Chief Information Security Officers (CISOs) haben die wichtige Aufgabe, sicherzustellen, dass diese Schritte umgesetzt werden, und gegebenenfalls externe Partner zu finden, die das Unternehmen bei den notwendigen Änderungen und der Sicherung von Daten und Prozessen beraten und unterstützen können. Entscheidungsträger sollten ihrerseits bereit sein, in robuste Sicherheitsmaßnahmen zu investieren und die Effektivität dieser Lösungen sorgfältig zu prüfen.

Da OT- und IT-Systeme immer enger in Fabrikumgebungen integriert sind, benötigen Hersteller eine vollständige, unternehmensweite Übersicht über alle Bedrohungen.

Verizon hat eine effektive Strategie für die Bedrohungsprävention, -erkennung und -abwehr, moderne Technologien wie Edge Computing sowie private, 5G-fähige latenzarme Konnektivität mit großer Bandbreite, die auf Lösungen wie Verizon Private 5G, Mobile Edge Computing und cloudbasierten Services basiert.

Mit dem richtigen Aktionsplan, geeigneten Lösungen und Verizon an ihrer Seite können moderne Hersteller den Übergang zur Enterprise Intelligence meistern und ihre wertvollsten Ressourcen – ihre Daten – wirksam schützen.

Informieren Sie sich darüber, wie Verizon Ihre Cybersicherheitsprozesse modernisieren kann, damit Ihr Team sich auf das konzentrieren kann, was wirklich wichtig ist: die Weiterentwicklung Ihres Unternehmens.

verizon business