



eye.

eye security

Cybersicherheit für die industrielle Fertigung

Ein Lösungsleitfaden

Schutz vor Ransomware-Angriffen hat oberste Priorität

Die schnelle digitale Transformation im Fertigungssektor hat eine einzigartige Umgebung geschaffen, die ebenso einzigartige Herausforderungen für die Cybersicherheit mit sich bringt.



Die häufigste Cyberbedrohung, mit der die Fertigungsindustrie konfrontiert ist, unterscheidet sich dabei kaum von anderen Branchen: Ransomware.

26 %

aller Cyberangriffe der letzten
3 Jahre richteten sich gegen
Fertigungsunternehmen



71 %

aller Cyberangriffe auf
Hersteller waren Ransomware



1.

**Digitale
Transformation
schafft neue
Herausforderungen
für die IT-Sicherheit**



Unternehmen im Fertigungssektor setzen zunehmend auf digitale Transformation, um Innovation, Wachstum, Effizienz und Profitabilität voranzutreiben. Die Geschwindigkeit und das Ausmaß dieses Wandels haben eine einzigartige Umgebung geschaffen, in der sich Informations- und Betriebstechnologien (IT und OT) zunehmend vermischen. Hinzu kommen komplexe Lieferketten, Mitarbeitende mit unterschiedlichsten Kompetenzen und zahlreiche regulatorische Anforderungen. Diese Kombination aus wertvollen Daten und den potenziell gravierenden Auswirkungen von Betriebsunterbrechungen macht Fertigungsunternehmen zu einem attraktiven Ziel für Cyberkriminelle und andere Bedrohungsakteure.

Als Reaktion darauf bieten viele Cybersicherheitsunternehmen spezialisierte Lösungen an, die vor allem auf den Schutz von Betriebstechnologien (OT) ausgelegt sind. Doch obwohl es gezielte Angriffe auf OT gibt, liegt die Hauptbedrohung für Hersteller in Bereichen, die sich nicht wesentlich von denen anderer Unternehmen unterscheiden. Ein Bericht des Weltwirtschaftsforums aus dem Mai 2024 zeigte, dass der Fertigungssektor in den drei Jahren zuvor der am häufigsten von Cyberangriffen betroffene Bereich war – **71 % dieser Angriffe waren Ransomware-Attacken.**

Unternehmen der verarbeitenden Industrie sind ein bevorzugtes Ziel für Cyberkriminelle. Daher sollte der Schutz der Informationen, die Angreifer zu stehlen oder zu verschlüsseln versuchen, oberste Priorität haben. Im Folgenden finden Sie die zehn wichtigsten Sicherheitsmaßnahmen, die Sie in Betracht ziehen sollten. Zunächst lohnt es sich jedoch, zu analysieren, warum gerade Fertigungsorganisationen so stark ins Visier geraten.

2.

Einzigartige technologische Umgebung

Fertigungsumgebungen waren schon immer besonders, da sie sowohl IT- als auch OT-Komponenten umfassen. Durch die digitale Transformation haben sich die Komplexität und die Angriffsfläche jedoch weiter erhöht – und bieten Cyberkriminellen neue Möglichkeiten.



Schnell wachsende Angriffsfläche

Die Angriffsfläche ist die Summe all dessen, was ein Bedrohungsakteur ausnutzen kann, um seine Ziele zu erreichen, einschließlich Software, Hardware, Menschen und Prozesse. In Fertigungsunternehmen wird diese Angriffsfläche durch die Einführung neuer Technologien, die Verbreitung des Internet der Dinge (IoT), die Einführung der Telearbeit und die Zunahme von BYOD-Praktiken („Bring-your-own-device“) immer größer.



Steigende Vernetzung

Industrieanlagen, die früher durch Air-Gaps (physische Netztrennung) gesichert waren, sind heute häufig mit IT-Netzwerken und dem Internet verbunden. Zudem entstehen durch IoT-Geräte große, oft heterogene Netzwerke. Zwar können gut konzipierte, segmentierte und gesicherte Netzwerke Angreifer daran hindern, von OT- zu IT-Systemen zu wechseln, doch keine Sicherheitsmaßnahme bietet einen absolut zuverlässigen Schutz.



Veraltete, anfällige OT-Systeme

Viele OT-Systeme sind schon seit Jahren im Einsatz und wurden nicht nach modernen Sicherheitsstandards entwickelt. Da sie ursprünglich nicht als Ziel für Angriffe betrachtet wurden, nutzen sie oft eingebettete Betriebssysteme und Software, die vom Hersteller nicht mehr unterstützt werden. Diese Systeme werden weiterhin eingesetzt, weil sie ihre spezifische Aufgabe zuverlässig erfüllen. Ein Austausch wäre teuer und würde den Betriebsablauf stören. Obwohl sie selten direkt Ziel eines Angriffs sind, können vorhandene Schwachstellen von Angreifern genutzt werden, um sich lateral durch Ihr Netzwerk zu bewegen und ihre Ziele zu erreichen.

3.

Ein einzigartiges Geschäftsumfeld

Die Kombination dieser technologischen Herausforderungen mit typischen Geschäftsprozessen und -strukturen in der Fertigung hat ein Umfeld geschaffen, die Cyberkriminelle gezielt ausnutzen.

Komplexe Lieferketten

Angriffe auf die Lieferkette missbrauchen vertrauenswürdige Geschäftsbeziehungen, um Zugang zu den Systemen und Netzwerken eines Unternehmens zu erhalten. Solche Angriffe können einfach sein, etwa wenn das E-Mail-Konto eines Geschäftspartners kompromittiert wird und eine infizierte Nachricht verschickt wird. Da die Nachricht von einem vertrauenswürdigen Partner stammt, fällt es vielen schwer, den Betrug zu erkennen. Komplexere Angriffe umfassen beispielsweise die Kompromittierung eines Softwarelieferanten, bei der Hintertüren in Anwendungen eingebettet werden, um Angreifern den Zugang zu Ihrem Netzwerk zu ermöglichen.

Der Fertigungssektor ist geprägt von komplexen Lieferketten und einer hohen geschäftlichen Vernetzung. Viele Hersteller sind sowohl Produzent als auch Konsument und arbeiten oft mit alleinigen Zulieferern. Fällt einer dieser Partner aufgrund eines Angriffs aus, kann dies weitreichende Auswirkungen auf die gesamte Lieferkette haben.

Unabhängig davon, wie ausgereift Ihr Sicherheitsprogramm ist: Ihre Sicherheit ist nur so stark wie die Ihrer Geschäftspartner und Kunden. Viele kleinere Unternehmen unterschätzen ihre Cyberrisiken. Selbst bei umfassenden Audits Ihrer Zulieferer bleibt die Frage offen: Wie können Sie sicherstellen, dass auch deren Geschäftspartner ein ausreichendes Sicherheitsniveau haben?

Laut dem Weltwirtschaftsforum war Ransomware das größte Risiko für die Fertigungsindustrie, gefolgt von Social Engineering und Angriffen auf Lieferketten. Diese dienen oft als erste Angriffsphase und können letztlich in Ransomware-Angriffen münden.

54 %

mangelnde
Transparenz der
Schwachstellen in
ihrer Lieferkette



41 %

eine Verletzung
einer dritten Partei
angelastet



Organisationsstruktur und Unternehmenskultur

Im Vergleich zu Branchen wie dem Bank- und Finanzwesen verfügen Fertigungsunternehmen oft über weniger ausgereifte Sicherheitsprogramme, die nicht mit der Geschwindigkeit der digitalen Transformation Schritt gehalten haben. Zudem fehlt es häufig an einer Kultur des Sicherheitsbewusstseins.

Fertigungsunternehmen setzen sich aus vielen Abteilungen zusammen, in denen Mitarbeitende mit unterschiedlichen Erfahrungen, Fähigkeiten und Prioritäten tätig sind. Oft mangelt es an Wissen und Ressourcen in Bereichen wie IT, OT, Cybersicherheit, Informationssicherheit sowie Governance, Risiko und Compliance (GRC). Dies führt häufig zu fragmentierten Transformationsstrategien und Entscheidungsprozessen, die Sicherheitslücken entstehen lassen.

Regulatorische Anforderungen

Die regulatorischen Anforderungen passen sich zunehmend an die sich verändernden Geschäftspraktiken und die digitale Transformation an. Viele Vorschriften enthalten spezifische Klauseln, die direkte Auswirkungen auf die Fertigungsindustrie haben.

Beispielsweise reguliert die EU-Richtlinie über Netz- und Informationssicherheit (NIS2) Hersteller, die kritische Infrastrukturen beliefern. Der Cyber Resilience Act betont Prinzipien wie „Security by Design“, um Risiken durch Cyberangriffe in Fertigungsumgebungen zu minimieren. Ebenso entwickeln sich branchenspezifische Vorschriften weiter. Die Maschinenverordnung (2023/1230) enthält beispielsweise aktualisierte Klauseln, um neue Risiken durch Cyberbedrohungen zu berücksichtigen.

Angesichts der Häufigkeit von Ransomware-Angriffen ist eine der wichtigsten Vorschriften jedoch die EU-Datenschutz-Grundverordnung (DSGVO), die für alle Unternehmen gilt. Ransomware-Gruppen setzen oft auf doppelte Erpressung. Daten werden nicht nur verschlüsselt, sondern auch gestohlen, mit der Drohung, diese zu veröffentlichen. Dies könnte für das Opfer hohe Strafen nach sich ziehen, wenn die DSGVO verletzt wird.



EU-Agentur für Cybersicherheit (ENISA):
Bedrohungslandschaft für 2024

72 % der auf das produzierende Gewerbe abzielenden Bedrohungen waren Ransomware



Ransomware ist die größte
Bedrohung für die Industrie.



Das verarbeitende Gewerbe
ist die Branche, die am
zweithäufigsten Ziel von
Ransomware ist.



Das produzierende Gewerbe
gilt als das häufigste und am
stärksten betroffene Opfer
von Ransomware.



Viele Gruppen von
Bedrohungsakteuren
konzentrieren sich auf
bestimmte Branchen, aber
die meisten von ihnen haben
es auf das verarbeitende
Gewerbe abgesehen.

4.

Warum ist die Fertigungsindustrie so stark betroffen?

Warum sind die Hersteller stärker betroffen als jeder andere Bereich? Die Antwort liegt in den oben beschriebenen Herausforderungen - eine große Angriffsfläche, anfällige Systeme und ein hohes Maß an Technologie und Geschäftskonnektivität. Dies zusammen mit unausgereifteren Sicherheitsprogrammen im Vergleich zu anderen Industrien, macht die Fertigungsindustrie zu einem leichten Angriffsziel für Ransomware-Bedrohungen.

Warum Ransomware?

- 1.** In der verarbeitenden Industrie haben Unterbrechungen des laufenden Betriebs, beispielsweise durch einen Cyberangriff, weitaus schwerwiegendere Auswirkungen als in anderen Branchen. Die Hersteller sind in hohem Maße auf einen kontinuierlichen Betrieb angewiesen, und die Nichteinhaltung fester Liefertermine kann für die gesamte Lieferkette katastrophale Auswirkungen haben. Hersteller sind daher oftmals eher bereit, Lösegeld zu bezahlen.
- 2.** Neben sensiblen persönlichen und geschäftlichen Informationen verfügen Hersteller über beträchtliche Mengen an weiteren wertvollen Daten, wie Geschäftsgeheimnisse und geistiges Eigentum, die im Dark Web an den Meistbietenden verkauft werden können.



5.

**Schützen Sie Ihr
Fertigungsunternehmen
mit 9 wichtigen
Sicherheitsmaßnahmen**

1.

Befolgen Sie bewährte Programme

Es gibt viele Rahmenprogramme für Cyber- und Informationssicherheit, die von Regierungsorganisationen wie dem US National Institute of Standards and Technology (NIST), dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem niederländischen National Cyber Security Centre (NCSC) erstellt worden sind. Wählen Sie unbedingt das Programm aus, das der Unternehmensgröße und dem Reifegrad Ihres Unternehmens in Bezug auf Cybersicherheit am besten entspricht.

2.

Verstehen Sie Ihre Sicherheitslage

Es ist schwierig, Ihr Unternehmen zu schützen, wenn Sie nicht wissen, was genau Sie schützen sollten. Identifizieren Sie ihre kritischen Anlagen und Informationen, bewerten Sie Ihre Infrastruktur, erkennen Sie Ihre Schwachstellen und wie Sie diese verbessern können.

3.

Erstellen Sie Sicherheitskopien außerhalb ihres Standorts

Wenn das Schlimmste eintritt und ein Ransomware-Angriff erfolgreich ist, kann es sein, dass selbst die Zahlung des Lösegelds nicht dazu führt, dass Sie die verschlüsselten Daten wiederherstellen können. Sie benötigen eine zuverlässige, nicht manipulierte Sicherung Ihrer wichtigen Informationen.

4.

Setzen Sie präventive Sicherheitsmaßnahmen ein

Präventive Sicherheitsmaßnahmen bilden das Fundament Ihrer Cybersicherheitsstrategie. Dazu gehören Technologien, die darauf ausgelegt sind, Angriffe abzuwehren, wie „Endpoint Protection Platforms“ (EPP), Firewalls sowie E-Mail- und Websicherheitslösungen. Segmentieren Sie Ihre IT-, OT-, BYOD- („Bring Your Own Device“) und Gastnetzwerke, um die Angriffsfläche zu minimieren. Ziehen Sie zudem eine Mikrosegmentierungsstrategie in Betracht, um unterschiedliche Sicherheitszonen effektiv voneinander abzuschirmen und so die Widerstandsfähigkeit Ihrer Systeme weiter zu erhöhen.

5.

Schaffen Sie ein Bewusstsein für Cybersicherheit in Ihrem Unternehmen

Implementieren Sie ein nachhaltiges Programm zur Schulung des Cybersicherheit-Bewusstseins („Security Awareness Training“, SAT) in Ihrem Unternehmen. Viele Unternehmen betrachten dies als eine schnelle Übung, einzig um Vorschriften einzuhalten oder sich für eine Cyberversicherung zu qualifizieren. Phishing-Simulationen tragen zwar dazu bei, dass Ihre Mitarbeiter lernen, E-Mail-Bedrohungen zu erkennen. Um jedoch das Verhalten der Mitarbeiter nachhaltig zu ändern und ein Bewusstsein für Cybersicherheit zu schaffen, sollten Sie mit einem SAT-Anbieter arbeiten, der computergestützte und von Hackern, Bildungs- und Cybersicherheitsexperten entwickelte Schulungen anbietet.

6. Implementieren Sie strenge Passwortrichtlinien

Der „Verizon Data Breach Investigation Report 2024“ stellte fest, dass 25 % der Sicherheitsverletzungen in der Fertigungsindustrie auf die Verwendung gestohlener Anmeldedaten zurückzuführen sind und 55 % der Systemeinträge durch Phishing erfolgen. Um dieses Risiko zu minimieren, sollten Sie strenge Passwortrichtlinien aufstellen und eine Multi-Faktor-Authentifizierung verwenden.

Setzen Sie „Cloud Detection and Response“ (CDR) ein, um die Benutzeraktivitäten in Ihren Cloud-Anwendungen kontinuierlich zu überwachen. Dadurch werden verdächtige Verhaltensweisen sofort erkannt. Wenn Sie Microsoft-Anwendungen lizenzieren, prüfen Sie bestehende Berechtigungen, da Sie möglicherweise bereits für Microsoft Sentinel lizenziert sind, das Entra ID-Schutz bietet.

7. Rechnen Sie mit Angriffen

Vorbeugende Maßnahmen können nicht jeden Angriff abwehren. Bereiten Sie sich auf den Fall vor, dass Angreifer erfolgreich in Ihr Netz oder Ihre Anwendungen eingedrungen sind.

Unabhängig davon, ob ein Zugriff über einen Benutzer, einen Laptop oder ein ICS erfolgt, ein Ransomware-Angreifer bewegt sich immer seitlich durch Ihr Netzwerk und sucht nach hochwertigen Informationen, die gestohlen und verschlüsselt werden können. Dazu muss ein Server oder ein Computer kompromittiert werden. Um Bedrohungsakteure aufzuspüren, noch während sie den Angriff durchführen, sollten Sie „Endpoint Detection and Response“ (EDR) einsetzen.

Wenn Sie sich für eines der führenden EPPs wie CrowdStrike oder Microsoft Defender entschieden haben, sind diese Funktionen bereits integriert. Wenn Ihr EPP kein EDR enthält, sollten Sie auf ein EPP mit EDR upgraden.



8. Lagern Sie an einen MDR-Anbieter mit 24/7-SOC aus

Wie oben beschrieben, verfügen viele Industrieunternehmen bereits über „Detection and Response“-Werkzeuge. Um jedoch den vollen Nutzen auszuschöpfen, benötigen Sie qualifizierte Mitarbeiter für den ständigen Sicherheitsbetrieb (SecOps). Weltweit fehlt es aber an Cyber-Fachkräften. Um diesen finanziellen und zeitlichen Engpass zu überwinden, lagern viele Unternehmen diese Aufgabe an einen „Managed Detection and Response Provider“ (MDR) aus.

Ein MDR-Anbieter überwacht Ihr CDR und EDR und reagiert, um Angriffe abzuwehren. Einige gehen sogar noch weiter und bieten einen „Incident-Response-Service“ und eine umfassende Partnerschaft für Ihr Sicherheitsprogramm an.


9. Schließen Sie eine Cyberversicherung ab

Dies ist die letzte und äußerst wichtige Sicherheitsmaßnahme.

Wenn Sie akzeptiert haben, dass es immer zu Sicherheitsverletzungen kommen kann, und Sie daher „Detection and Response“-Tools, SecOps und Spezialisten einsetzen, um das Risiko eines erfolgreichen Angriffs zu verringern, sollten Sie dennoch auf das Schlimmste vorbereitet sein.

Ihre Cyberversicherung sollte direkte und indirekte Kosten abdecken, einschließlich aller potenziellen Haftungen, die aus Ihrer komplexen Lieferkette entstehen können.

Viele MDR-Anbieter haben enge Beziehungen zu Maklernetzwerken, und die Kombination von Versicherungen mit deren Dienstleistungen führt oft zu erheblichen Prämiennachlässen und vereinfachten Antragsverfahren.



Dieser Leitfaden hat sich auf das Thema Ransomware fokussiert, und der Schutz Ihres Unternehmens davor sollte oberste Priorität haben. Bedenken Sie jedoch, dass es noch andere Bedrohungen gibt, denen Sie ausgesetzt sein können, wie Wirtschaftsspionage und Sabotage.

Sobald Sie die Grundlagen geschaffen haben, besteht der nächste Schritt darin, sich auch vor diesen weniger verbreiteten Bedrohungen zu schützen. Zu diesem Zweck könnten Sie den Aufbau eines eigenen „Security Operations Center“ mit entsprechenden Tools und die Einstellung von spezialisierten SecOps-Mitarbeitern in Betracht ziehen. Sobald dies geschehen ist, sollten Sie Ihre OT-Umgebung durch ein spezialisiertes Asset- und Schwachstellenmanagement weiter absichern. Netzwerkerkennungs- und -reaktionswerkzeuge („Network Detection and Response“, NDR) bieten einen umfassenden Einblick in Ihren gesamten Netzwerkverkehr, erfordern jedoch Experten für die Bereitstellung und Überwachung. Weitere Informationen finden Sie in dem Artikel [„EDR vs. NDR: Warum Endpunktsicherheit einen klaren Vorteil hat“](#).

6.

Schlussfolgerungen und nächste Schritte

Bei der Festlegung Ihrer Prioritäten für zusätzliche Sicherheitsmaßnahmen sollten Sie bedenken, dass der Schutz vor Ransomware für Sie oberste Priorität haben sollte und dass die meisten Angriffe die Kompromittierung von Anmeldeinformationen und/oder Endgeräten sowie die Exfiltration von Daten beinhalten. Daher sollten Sie sich auf die Erkennung, Reaktion und Eindämmung solcher Angriffe konzentrieren.

Weitere Ressourcen für die Fertigungsindustrie



Fallstudie: KeyTec Niederlande

Als die Berichte über Ransomware in der Branche immer häufiger wurden, beschloss das Fertigungsunternehmen KeyTec Netherlands, Maßnahmen zu ergreifen. Erfahren Sie, wie Eye Security das Unternehmen dabei unterstützt hat, seine Abwehrkräfte proaktiv zu stärken und eine Sicherheitskultur zu schaffen.



Signature Foods*

Fallstudie: Signature Foods

Da die Internetkriminalität immer raffinierter wird, wenden sich Unternehmen vermehrt an externe Anbieter. Erfahren Sie, wie Eye Security Signature Foods in nur wenigen Wochen zu einem umfassenden Cyberschutz verholfen hat.





Eye Security schützt Industrieunternehmen mit 24/7-Bedrohungsüberwachung, schneller Reaktion auf Vorfälle und integrierter Cyberversicherung. Wir machen Cybersicherheit einfach und effektiv, damit Sie sich auf Ihren Betrieb und die Einhaltung von Produktionsfristen konzentrieren können.

Über www.eye.security

