

Revolution in der Fertigung: Wie Cybersecurity die Zukunft sichert!

Erfahren Sie, wie IoT und smarte Fertigungssysteme Effizienz steigern und neue Risiken für die Cybersicherheit mit sich bringen.



Smart Factory, Deutschland - Wie steht es um die Fabriken der Zukunft? Die Fertigungsindustrie befindet sich in einem aufregenden Wandel hin zu smarten Fertigungssystemen. Hierbei kommen vernetzte Maschinen, IoT-Sensorik, KI-Analysen und cloudbasierte Steuerungen zum Einsatz. Doch die Chancen, die diese Technologien bieten, bringen auch Risiken mit sich, vor allem im Bereich der Cybersicherheit. Laut **Security Insider** ist es entscheidend, dass nur sichere Fertigung auch als produktive Fertigung gilt. Immer mehr Unternehmen müssen sich mit der Erkenntnis auseinandersetzen, dass ihre Produktionssysteme oftmals unzureichend abgesichert sind. Angriffe auf Fertigungsunternehmen werden nicht nur häufiger, sondern auch komplexer, wie der Data Breach Investigations Report

(DBIR) 2025 zeigt.

Besonders alarmierend: 53% der Sicherheitsvorfälle betrafen gezielte Systemintrusionen in der IT- und OT-Infrastruktur. Ransomware ist eine der gefährlichsten Bedrohungen und war an 44% der Datenpannen beteiligt, insbesondere in kleinen und mittleren Unternehmen (KMU), wo 88% der Sicherheitsverletzungen durch Ransomware verursacht wurden. Darüber hinaus kombinieren Angreifer technische Schwachstellen mit gestohlenen Zugangsdaten und nutzen oft VPNs und Edge-Geräte als Einfallstore.

Die Transformation zur Smarten Fabrik

Die Umstellung auf Smart Factories steigert nicht nur die Effizienz und Flexibilität in der Produktion, sondern birgt auch neue Sicherheitsrisiken. An dieser Stelle hebt **Industrieanzeiger** hervor, dass die Sicherheit das gesamte Unternehmen betrifft – von der OT-Infrastruktur über die Lieferkette bis zur qualifizierten Schulung der Mitarbeiter. Die Angriffsfläche der industriellen Systeme wächst durch das Zusammenwachsen von IT und OT, was Cyberrisiken anzieht, die oft gar nicht richtig adressiert werden. Klassische IT-Sicherheitsmaßnahmen, wie Firewalls und VPNs, sind notwendig, aber nicht ausreichend.

Einfallsreiche Angreifer nutzen häufig Firmware-Schwachstellen, um in Systeme einzudringen. Daher sind umfassende Prüfungen der Geräte-Firmware entlang der Lieferkette und regelmäßige Scans beim Bootvorgang unerlässlich. Um die Herausforderungen der smarten Fertigung zu bewältigen, sind moderne Technologien wie KI und Edge Computing entscheidend. Diese Technologien ermöglichen es Unternehmen, große Datenmengen in Echtzeit zu verarbeiten und dabei Sicherheitsprotokolle zu integrieren.

Strategien zur Verbesserung der

Cybersicherheit

Die Verbesserung der Cybersicherheit in der Fertigungsbranche erfordert ein mehrschichtiges Konzept. Laut **Deloitte** setzen 90 Prozent der Hersteller zwar auf Cyber-Ereigniserkennung, jedoch haben nur wenige Unternehmen die Überwachung auf ihre OT-Umgebungen ausgeweitet. Der Schwerpunkt auf Cybersicherheit sollte als zentraler Treiber für stabile und effiziente Produktionsprozesse betrachtet werden. Dazu gehört auch die Umsetzung von Zero-Trust-Prinzipien und regelmäßige Schwachstellenanalysen.

- Netzwerksegmentierung zwischen Produktions- und IT-Netzwerken
- Multi-Faktor-Authentifizierung für kritische Systeme
- Monitoring und Anomalie-Erkennung durch KI
- Sensibilisierung und Schulungen für Mitarbeitende

Das Beispiel des Unternehmens BWT zeigt, wie man durch intelligente Fertigungslösungen Effizienzsteigerungen um 30 %, eine Senkung der Arbeitskosten um 20 % sowie eine Reduzierung des Energieverbrauchs um 40 % erreichen kann. Durch proaktive Cybersicherheitsmaßnahmen wird zudem sichergestellt, dass Manipulationen vorgebeugt wird.

Die Zukunft der smarten Fertigung sieht vielversprechend aus, doch ohne eine robuste Sicherheitsarchitektur bleibt das Potenzial ungenutzt. Um wirklich von diesen Entwicklungen zu profitieren, müssen Unternehmen ihre Sicherheitsstrategien kontinuierlich an neue Bedrohungen anpassen und bereit sein, innovative Lösungen zur Cybersicherheit zu implementieren.

Details	
Ort	Smart Factory, Deutschland
Quellen	• www.security-insider.de • industrieanzeiger.industrie.de

- www.deloitte.com

Besuchen Sie uns auf: wom87.de