

Cybersecurity in der Produktion





Inhaltsverzeichnis

Cybersecurity in der Produktion

Inhaltsverzeichnis	2
Cybersecurity in der Fertigungsindustrie	2
Der Schutzschild der digitalen Produktion	3
Warum Cybersecurity für die Fertigungsindustrie unverzichtbar ist	4
Die Verschmelzung von IT und OT	5
Typische Bedrohungen in der Fertigungsindustrie	6
Die fünf Säulen einer sicheren Produktion	7
Cybersecurity als Bestandteil von Industrie 4.0	8
Rechtliche Anforderungen und Verantwortung	9
Rechtliche Anforderungen und Verantwortung	10
MVO 2023/1230 – Cybersecurity wird Teil der Maschinensicherheit	11
Auswirkungen auf Hersteller, Integratoren und Betreiber	12
Unterstützende Normen und Standards	13
Cybersecurity als Wettbewerbsfaktor	14
Fazit	15
Rechtlicher Hinweis	16
Impressum	17

Cybersecurity in der Produktion

Der Schutzschild der digitalen Produktion

Einleitung

Die Fertigungsindustrie befindet sich mitten in der digitalen Transformation. Maschinen, Roboter, CNC-Bearbeitungszentren, Sensoren, ERP- und PPS-Systeme, CAM-Software und Cloud-Lösungen sind heute stärker vernetzt als jemals zuvor.

Diese Entwicklung schafft enorme Potenziale hinsichtlich Produktivität, Transparenz und Automatisierung. Gleichzeitig entstehen jedoch neue Risiken. Jede vernetzte Maschine, jede Schnittstelle und jeder Fernzugriff kann zu einem potenziellen Angriffspunkt werden.

Cybersecurity ist deshalb längst nicht mehr nur ein Thema der IT-Abteilung. Sie ist ein entscheidender Faktor für Produktionssicherheit, Lieferfähigkeit, Qualitätssicherung und Wettbewerbsfähigkeit.



Cybersecurity in der Produktion

Warum Cybersecurity für die Produktion unverzichtbar ist

Produktionsunternehmen unterscheiden sich wesentlich von klassischen Dienstleistungsunternehmen. Während ein Cyberangriff in einer Büroorganisation oft primär zu Datenverlust führt, kann ein Angriff in der Fertigung direkte Auswirkungen auf Maschinen, Anlagen und Lieferprozesse haben.

Mögliche Folgen sind:

- Produktionsstillstände
- Maschinen- und Anlagenausfälle
- Verlust von CAD-, CAM- und Konstruktionsdaten
- Manipulierte Fertigungsprozesse
- Qualitätsmängel
- Termin- und Lieferverzögerungen
- Personen- und Sachschäden
- Hohe finanzielle Schäden
- Verlust von Kundenvertrauen
- Reputationsschäden

Ein einziger Cybervorfall kann innerhalb weniger Stunden Schäden verursachen, die weit über die eigentlichen IT-Kosten hinausgehen.



Cybersecurity in der Produktion

Die Verschmelzung von IT und OT

Moderne Produktionssysteme verbinden: Die moderne Smart Factory basiert auf der Verbindung von:

Information Technology (IT)

- ERP-Systeme
- Office-Anwendungen
- Datenbanken
- Cloud-Plattformen
- Dokumentenmanagement

Operational Technology (OT)

- CNC-Maschinen
- SPS-Steuerungen
- Roboter
- Messmaschinen
- Handling Systeme
- Montagelinien

Diese Vernetzung ermöglicht Industrie 4.0 und digitale Zwillinge, erhöht gleichzeitig aber auch die Angriffsfläche für Cyberkriminalität.





Cybersecurity in der Produktion

Typische Bedrohungen in der Produktion

Ransomware

Cyberkriminelle verschlüsseln Systeme und Daten, um Lösegeldforderungen durchzusetzen.

Folgen:

- Produktionsstillstand
- Datenverlust
- Wiederherstellungskosten
- Lieferverzug

Unsichere Fernwartung

Maschinenhersteller und Integratoren benötigen oftmals Fernzugriffe.

Risiken:

- Unzureichende Authentifizierung
- Fehlende Protokollierung
- Dauerhaft offene Verbindungen

Veraltete Produktionssysteme

Maschinen verbleiben häufig über Jahrzehnte im Einsatz.

Herausforderungen:

- Nicht unterstützte Betriebssysteme
- Fehlende Sicherheitsupdates
- Bekannte Schwachstellen

Social Engineering und Phishing

Der Mensch bleibt häufig die grösste Sicherheitslücke.

Beispiele:

- Gefälschte E-Mails
- Manipulierte Rechnungen
- Gestohlene Zugangsdaten
- Schadsoftware über Anhänge





Cybersecurity in der Produktion

Die fünf Säulen einer sicheren Produktion

1. Transparenz über alle Systeme

Unternehmen müssen jederzeit wissen:

- Welche Geräte im Netzwerk vorhanden sind
- Welche Maschinen vernetzt sind
- Wer Zugriff besitzt
- Welche Daten übertragen werden

Man kann nur schützen, was man kennt.

2. Segmentierung der Netzwerke

Produktionsnetzwerke sollten konsequent von Büro- und Gastnetzwerken getrennt werden.

Vorteile:

- Begrenzung von Angriffen
- Höhere Verfügbarkeit
- Verbesserte Kontrolle

3. Zugriffskontrolle

Grundsatz:

„Need-to-Know“ und „Least Privilege“

Jeder Nutzer erhält nur jene Zugriffsrechte, die tatsächlich benötigt werden.

Massnahmen:

- Rollenbasierte Zugriffsverwaltung
- Mehrfaktor-Authentifizierung
- Passwortmanagement
- Protokollierung

4. Schulung der Mitarbeitenden

Cybersecurity ist kein reines Technikthema.

Wichtige Elemente:

- Awareness-Trainings
- Verhaltensrichtlinien
- Meldeprozesse
- Sicherheitskultur



5. Backup- und Notfallstrategien

Jedes Unternehmen muss davon ausgehen, dass ein Sicherheitsvorfall eintreten kann.

Deshalb sind notwendig:

- Regelmässige Backups
- Wiederherstellungstests
- Notfallpläne
- Krisenorganisation

Cybersecurity in der Produktion

Cybersecurity als Bestandteil von Industrie 4.0

Die digitale Fabrik basiert auf:

- Echtzeitdaten
- Sensorik
- Digitalen Zwillingen
- Cloud-Systemen
- Künstlicher Intelligenz
- Automatisierung

Ohne Cybersecurity werden diese Technologien zu einem erheblichen Risiko.

Cybersecurity bildet somit das Fundament für:

- Smart Factory
- Predictive Maintenance
- Digitale Geschäftsmodelle
- Automatisierte Wertschöpfungsketten
- Datengetriebene Fertigung



Cybersecurity in der Produktion

Rechtliche Anforderungen und Verantwortung

Cybersecurity ist nicht nur eine technische oder organisatorische Aufgabe, sondern zunehmend eine rechtliche Verpflichtung.

Unternehmen müssen je nach Branche und Marktumfeld verschiedene Anforderungen erfüllen.

Schweiz

Für Schweizer Unternehmen gewinnen folgende Themen zunehmend an Bedeutung:

Datenschutzgesetz (DSG)

- Meldepflicht bei Datenschutzverletzungen
- Schutz von Personendaten
- Nachweis angemessener technischer und organisatorischer Massnahmen

Die Geschäftsleitung trägt dabei eine Mitverantwortung für die angemessene Organisation des Unternehmens und die Risikobeherrschung.

Europäische Union

Viele Schweizer Industrieunternehmen liefern direkt oder indirekt in die EU und sind dadurch betroffen von:

NIS2-Richtlinie

- Erhöhung der Cybersicherheit kritischer und wichtiger Organisationen
- Risikomanagementpflichten
- Sicherheitsmassnahmen
- Meldepflichten bei Sicherheitsvorfällen

Cyber Resilience Act (CRA)

Der CRA definiert künftig Anforderungen an Produkte mit digitalen Komponenten.

Dabei werden Themen relevant wie:

- Security by Design
- Schwachstellenmanagement
- Sicherheitsupdates
- Dokumentationspflichten



Cybersecurity in der Produktion

Rechtliche Anforderungen und Verantwortung

Ist Cybersecurity Teil der Maschinensicherheit?

Die Antwort lautet heute eindeutig:

Ja.

Im Rahmen moderner Sicherheitskonzepte verschmelzen:

- Funktionale Sicherheit (Safety)
- Informationssicherheit (Security)

Manipulationen an Steuerungen oder sicherheitsrelevanten Funktionen können direkte Auswirkungen auf Personen, Maschinen, Werkzeuge, Werkstücke und Produktionsprozesse haben.



Cybersecurity in der Produktion

MVO 2023/1230 – Cybersecurity wird Teil der Maschinensicherheit

Mit der neuen Maschinenverordnung (EU) 2023/1230 wird Cybersecurity erstmals ausdrücklich als Bestandteil der Maschinensicherheit berücksichtigt.

Die Verordnung ersetzt die bisherige Maschinenrichtlinie 2006/42/EG und wird ab dem 20. Januar 2027 verbindlich angewendet.

Moderne Maschinen verfügen heute über:

- Netzwerkverbindungen
- Fernwartungszugänge
- Cloud-Anbindungen
- Software-Updates
- Datenschnittstellen
- KI-basierte Funktionen



Dadurch entstehen neue digitale Gefährdungen, welche bereits bei der Konstruktion und Risikobeurteilung berücksichtigt werden müssen.

Die Maschinenverordnung fordert deshalb, dass Maschinen, Sicherheitsbauteile und zugehörige Systeme gegen unbefugte Zugriffe, Manipulationen und Cyberangriffe geschützt werden, soweit dies nach dem Stand der Technik möglich ist.

Cybersecurity als Bestandteil der Risikobeurteilung

Hersteller müssen künftig zusätzliche Fragestellungen betrachten:

- Können Sicherheitsfunktionen manipuliert werden?
- Können Steuerungen von aussen beeinflusst werden?
- Bestehen Risiken durch Fernwartungszugänge?
- Sind Kommunikationsschnittstellen ausreichend geschützt?
- Können Softwarestände unbefugt verändert werden?
- Sind Updates nachvollziehbar und sicher durchführbar?

Cybersecurity wird damit Teil der technischen Risikobeurteilung und CE-Konformitätsbewertung.

Cybersecurity in der Produktion

Auswirkungen auf Hersteller, Integratoren und Betreiber

Die Anforderungen betreffen künftig die gesamte Wertschöpfungskette.

Security by Design

Cybersecurity muss bereits in der Konzept- und Entwicklungsphase berücksichtigt werden.

Schutz vor unbefugtem Zugriff

- Benutzer- und Rechteverwaltung
- Authentifizierungsverfahren
- Passwortkonzepte
- Zugriffskontrollen

Sichere Kommunikation

- Netzwerksegmentierung
- Verschlüsselte Datenübertragung
- Kontrollierte Fernzugriffe
- Dokumentierte Schnittstellen

Software- und Update-Management

- Nachvollziehbare Softwarestände
- Kontrollierte Updates
- Änderungsmanagement
- Schwachstellenmanagement



Safety und Security gemeinsam denken

Die MVO 2023/1230 verdeutlicht, dass funktionale Sicherheit und Cybersecurity nicht mehr getrennt betrachtet werden können.

Ein erfolgreicher Cyberangriff kann unmittelbar zu:

- Personenrisiken
 - Maschinenbeschädigungen
 - Produktionsausfällen
 - Qualitätsproblemen
 - Lieferverzögerungen
- führen.

Cybersecurity wird damit zu einem festen Bestandteil des sicherheitstechnischen Gesamtkonzepts moderner Maschinen, Anlagen und Fertigungssysteme.

Cybersecurity in der Produktion

Unterstützende Normen und Standards

Zur Umsetzung einer professionellen Cybersecurity-Strategie haben sich insbesondere folgende Standards etabliert:

IEC 62443

Cybersecurity für industrielle Automatisierungs- und Steuerungssysteme

ISO 27001

Managementsystem für Informationssicherheit

ISO 12100

Risikobeurteilung und Risikominderung

EN ISO 13849

Sicherheitsbezogene Teile von Steuerungen

IEC 62061

Funktionale Sicherheit von Maschinensteuerungen

Diese Normen unterstützen Unternehmen dabei, die Anforderungen der MVO 2023/1230 systematisch und nachvollziehbar umzusetzen.





Cybersecurity in der Produktion

Cybersecurity als Wettbewerbsfaktor

Immer mehr Kunden verlangen heute Nachweise über:

- Informationssicherheit
- Datenschutz
- Risikomanagement
- Lieferantensicherheit

Cybersecurity wird dadurch zunehmend Teil von:

- Lieferantenaudits
- Qualitätsmanagementsystemen
- Kundenfreigaben
- Compliance-Anforderungen

Unternehmen mit einer professionellen Sicherheitsstrategie stärken nicht nur ihre Resilienz, sondern auch ihre Marktposition.



Cybersecurity in der Produktion

Fazit

Die vernetzte Fertigung bietet enorme Chancen. Gleichzeitig steigen die Anforderungen an den Schutz von Daten, Maschinen, Produktionsprozessen und Geschäftsgeheimnissen.

Cybersecurity ist heute weit mehr als eine technische Schutzmassnahme. Sie ist ein wesentlicher Bestandteil von Unternehmensführung, Risikomanagement, Compliance und Wettbewerbsfähigkeit.

Mit der Maschinenverordnung (EU) 2023/1230 wird Cybersecurity zusätzlich zu einer relevanten Anforderung für Hersteller, Integratoren und Betreiber von Maschinen und automatisierten Fertigungssystemen.

Wer Industrie 4.0 erfolgreich umsetzen will, muss Cybersecurity von Beginn an mitdenken.

Kernaussage

Cybersecurity ist die digitale Schutzvorrichtung der modernen Fertigung – unsichtbar, aber unverzichtbar.

Sie schützt nicht nur Daten und IT-Systeme, sondern sichert die Verfügbarkeit von Maschinen, die Stabilität von Prozessen, die Sicherheit von Menschen und letztlich die Zukunftsfähigkeit des gesamten Unternehmens.





Cybersecurity in der Produktion

Rechtlicher Hinweis

Die Inhalte dieses Dokuments dienen ausschliesslich der allgemeinen Information, Schulung, Sensibilisierung, Beratung und organisatorischen Weiterentwicklung von Unternehmen und Mitarbeitenden. Sie vermitteln allgemeines Fachwissen und stellen keine Rechts-, Steuer-, Unternehmens-, Investitions-, Finanzierungs-, Wirtschafts-, Compliance-, Datenschutz-, Informationssicherheits-, Cybersecurity-, KI-Regulierungs- oder sonstige Fachberatung dar. Ebenso ersetzen sie keine Zertifizierung, Unternehmensprüfung, produktspezifische Normenprüfung, Vertragsprüfung, Risikobeurteilung, Konformitätsbewertung oder verbindliche technische Beurteilung.

Alle dargestellten Beispiele, Methoden, Handlungsempfehlungen, Organisationsansätze sowie technischen und organisatorischen Lösungsansätze dienen ausschliesslich der Veranschaulichung und allgemeinen Orientierung. Sie müssen vor einer Anwendung auf ihre Eignung für die jeweilige Unternehmens-, Produkt-, Prozess-, Projekt- oder Anwendungssituation geprüft, bewertet und gegebenenfalls angepasst werden.

Die Verantwortung für sämtliche unternehmerischen, organisatorischen, personellen, technischen, wirtschaftlichen und rechtlichen Entscheidungen sowie deren Umsetzung liegt ausschliesslich beim jeweiligen Unternehmen bzw. den verantwortlichen Personen.

Die Inhalte dieses Dokuments ersetzen weder gesetzliche Vorgaben noch behördliche Anforderungen, vertragliche Vereinbarungen, branchenspezifische Regelungen, betriebliche Vorgaben oder geltende Normen und Standards. Die Umsetzung hat stets unter Berücksichtigung der jeweils geltenden gesetzlichen, regulatorischen, arbeitsrechtlichen, datenschutzrechtlichen, sicherheitsrelevanten, produktsicherheitsrechtlichen und technischen Anforderungen zu erfolgen.

Rechtliche, technische und regulatorische Anforderungen können je nach Branche, Unternehmensgrösse, Land, Markt, Produkt, Maschine, Anlage, Software, Anwendung oder Einsatzgebiet unterschiedlich sein. Insbesondere sind die jeweils einschlägigen Gesetze, Verordnungen, Richtlinien, Normen und Standards durch das verantwortliche Unternehmen im konkreten Einzelfall zu prüfen und einzuhalten.

Aussagen zu technologischen Entwicklungen, Digitalisierung, Künstlicher Intelligenz, Industrie 4.0, Markttrends, Zukunftsszenarien oder wirtschaftlichen Entwicklungen dienen ausschliesslich der allgemeinen Orientierung. Sie stellen weder Prognosen noch Garantien für zukünftige technische, wirtschaftliche oder regulatorische Entwicklungen oder Unternehmenserfolge dar.

Personenbezeichnungen, Rollenmodelle, Organisationsformen, Generationenmodelle oder vergleichbare Darstellungen dienen ausschliesslich der Veranschaulichung und stellen keine Bewertung einzelner Personen oder Personengruppen dar.

Die Gremotool GmbH übernimmt keine Gewähr für die Vollständigkeit, Aktualität, Richtigkeit oder uneingeschränkte Anwendbarkeit der dargestellten Inhalte auf konkrete Unternehmen, Produkte, Projekte oder individuelle Anwendungsfälle. Massgebend sind stets die zum jeweiligen Zeitpunkt geltenden gesetzlichen Vorschriften, Verordnungen, Normen, behördlichen Anforderungen sowie die projektspezifischen Rahmenbedingungen.

Jegliche Haftung für direkte oder indirekte Schäden sowie Folgeschäden, die aus der Nutzung, Anwendung oder Umsetzung der dargestellten Inhalte entstehen, wird im gesetzlich zulässigen Umfang ausgeschlossen.

Die dargestellten Cybersecurity-Massnahmen ersetzen keine individuelle Sicherheitsanalyse, Risikoanalyse, Penetrationstests, Sicherheitsbewertung oder technische Umsetzung von Schutzmassnahmen. Die Verantwortung für die angemessene Absicherung von Informationssystemen, Netzwerken, Maschinen, Anlagen und Daten verbleibt beim jeweiligen Unternehmen bzw. den verantwortlichen Personen.



Impressum

Gremotool GmbH
Wilerstrasse 3
CH-9200 Gossau
Schweiz

www.gremotool.ch
info@gremotool.ch
+41 (0)71 930 03 90

Es gelten unsere AGB, welche auf www.gremotool.ch abgerufen werden können.

Weiter Kataloge können auf der Website www.gremotool.ch abgerufen werden.

Handelsregister:
UID-Nr. CHE-498.310.590

Dieses Dokument ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Jegliche, auch nur teilweise Verwendung, insbesondere Veröffentlichung, Vervielfältigung, Verbreitung, Wiedergabe, Bearbeitung und/oder Änderung, bedarf der vorherigen schriftlichen Genehmigung der Gremotool GmbH. Druckfehler und Irrtümer, sowie technische Änderungen vorbehalten.

Veröffentlichung Juli 2026, Auflage 1

