



Cyber Security made by Lenze

Nürnberg | 26. November 2025 |
Denis Göllner | © Lenze

Lenze
engineers *in motion*

MOVE STRONGER.

Die
5-Punkte
Checkliste für
Ihre Sicherheit



- 1 Rechtliche Vorgaben & Normen kennen**
CRA, MVO, RED-DA, IEC 62443 – Mitarbeiterschulungen sicherstellen
- 2 Security-Schwachstellen managen**
PSIRT-Team & SBOM etablieren, Meldeprozesse definieren
- 3 Risiken systematisch analysieren**
Bedrohungen bewerten, Maßnahmen priorisieren
- 4 Technische Schutzmaßnahmen umsetzen**
Zugriffskontrollen, Updates – sichere & nutzerfreundliche Umsetzungen
- 5 Kooperation mit Partnern stärken**
Anforderungen abstimmen, Security offen besprechen

Lenze ist als
Partner für
Cyber Security
an Ihrer Seite

Gesetzliche Vorgaben & Branchenstandards

Regulatorien, Standards, Normen



Betroffene Rolle	Maschinenhersteller		Maschinenbetreiber		
	Komponentenhersteller/Zulieferer				
Anwendungsbereich	Verkaufsfähige Produkte		OT	IT	
Verantwortliche Abteilung	Produktentwicklung		OT-Abteilung	IT-Abteilung	
Betroffene Geräte/Systeme	Maschinen		Maschinen	PCs	
	Automatisierungskomponenten		MES	Mailsysteme	
	Smart Home Devices uvm.		Fernwartung	ERP-Systeme	
				Cloudservices	
Vorhandene Standards	IEC 62443	EN 50742	EN 18031	IEC 62443	ISO 27001

Machen Sie sich mit rechtlichen Regularien (wie z.B. CRA, MVO, RED) vertraut und schulen Sie Ihre Mitarbeiter in Bezug auf relevante Cyber-Security – Normen (z.B. IEC 62443)

Gesetzliche Vorgaben & Branchenstandards

Regulatorien, Standards, Normen

Unser Support



Security-Whitepaper

- Überblick über die rechtlichen Anforderungen der EU.
- Umriss der Security-Norm für OT-Geräte (IEC 62443).
- Informationen für Security-Experten.



Security-Flyer

Überblick über die Security-Funktionen von Lenze.



Security Website

- Kontaktangaben für Berichte über Security-Vorfälle.
- Link zu CERT@VDE
- Sonstige Security-Benachrichtigungen

Nutzen Sie die frei verfügbaren Lenze-Dokumente, um Wissen zu Cyber Security und den zugehörigen Gesetzen und den Features im Lenze Portfolio aufzubauen.

Schwachstellenmanagement & Transparenz

Schwachstellen, Meldepflichten, PSIRT, SBOM



- Ab **September 2026**:
Meldung aktiv ausgenutzter
Schwachstellen
- Ab **Dezember 2027**:
strukturiertes Schwachstellen-
management

➔ Ziel ist es, Security-
Schwachstellen
frühzeitig zu erkennen,
angemessen zu
bewerten und zeitnah
zu beheben

Maschinenbauer müssen künftig:

- Schwachstellen in ihren
Maschinen und den
eingesetzten Komponenten
kontinuierlich überwachen
- Klare Prozesse zur Bewertung
und Weitergabe security-
relevanter Informationen
etablieren
- Ihre Kunden über relevante
Security-Risiken in ihren
Maschinen informieren

Wie Sie den Überblick behalten:

- Installation eines **PSIRT**

Product
Security
Incident
Response
Team

- Erstellung einer **SBOM**

Software
Bill
Of
Materials

Detaillierte Liste aller
**Komponenten, Bibliotheken
und Abhängigkeiten**, die im
Produkt enthalten sind.

**Das Tracken
von Risiken und
Schwachstellen** wird
unerlässlich und sogar
gesetzlich erforderlich!

Schwachstellenmanagement & Transparenz

Schwachstellen, Meldepflichten, PSIRT, SBOM



Unser Support



Schwachstellenmanagement & Transparenz

Schwachstellen, Meldepflichten, PSIRT, SBOM



Unser Support

Wir stellen alle benötigten Informationen transparent, maschinenlesbar und damit automatisierungsfreundlich zur Verfügung. So können Sie gesetzliche Anforderungen einfach und effizient erfüllen.

security.txt



VDE
CERT

CSAF

Etablieren Sie Prozesse zur Erkennung und Meldung von Sicherheitslücken. Ein PSIRT-Team und eine Software-Stückliste der Maschine helfen dabei.

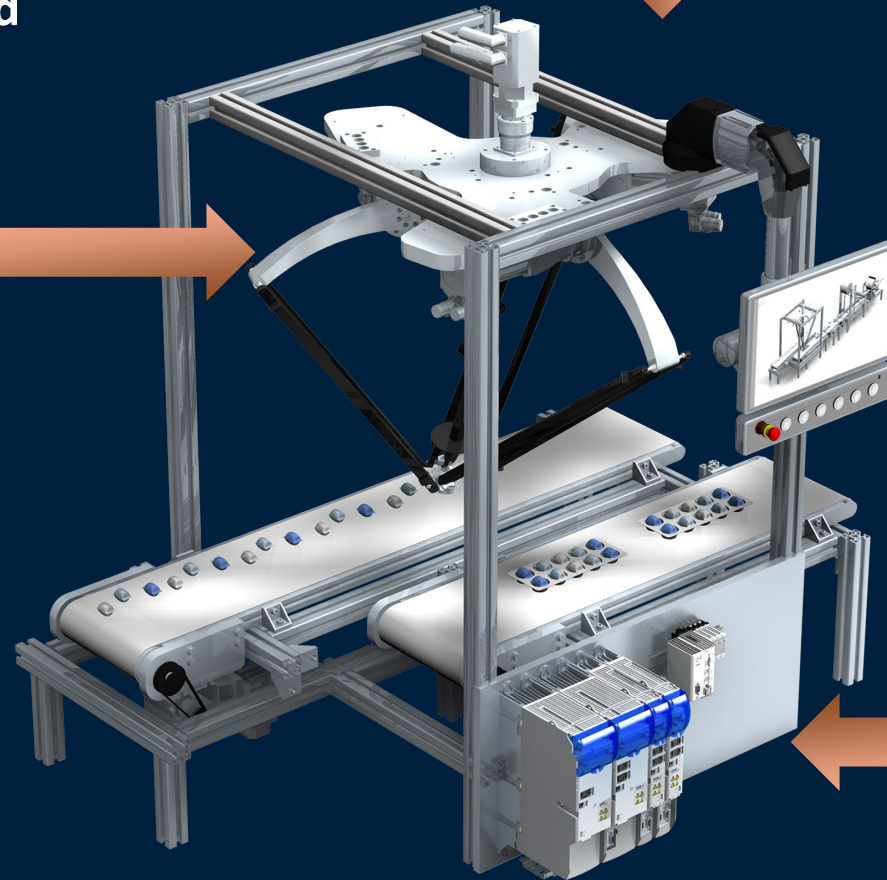
Risiko- und Bedrohungsanalyse

Schutzmaßnahmen einleiten

Datenverlust während
der Kommunikation

Maschine-zu-
Maschine-
Kommunikation

Verlust von
Know-how



Kommunikation
mit höheren
Ebenen



Maschinenstillstand

Zugriff auf
Maschinen-HMI

Manipulierte
Produktionsprozesse

Zugang zum
Maschinen-
netzwerk

Im Ernstfall werden
unberücksichtigte
Risiken teuer!

Risiko- und Bedrohungsanalyse

Schutzmaßnahmen einleiten

Unser Support

- Risiken systematisch analysieren
- Bedrohungen bewerten
- Maßnahmen priorisieren
- Transparenz schaffen



Lenze unterstützt mit Expertise und der Vermittlung von externen Partnern, die Sicherheitskonzepte und Risikobewertungen durchführen und beratend zur Seite stehen.

Umsetzung von Security Maßnahmen

Zugriffsschutz, Updates, Schnittstellen, etc.



Datenverlust während der Kommunikation

Verschlüsselte Kommunikation

Verlust von Know-how

Verschlüsselung vertraulicher Daten



Maschinenstillstand

Schützen Sie Systeme mit Zugriffskontrolle

Manipulierte Produktionsprozesse

Manipulationen mit Auditlogs erkennen

**Angriff/
Vorbereitung**
ist die beste
Verteidigung!

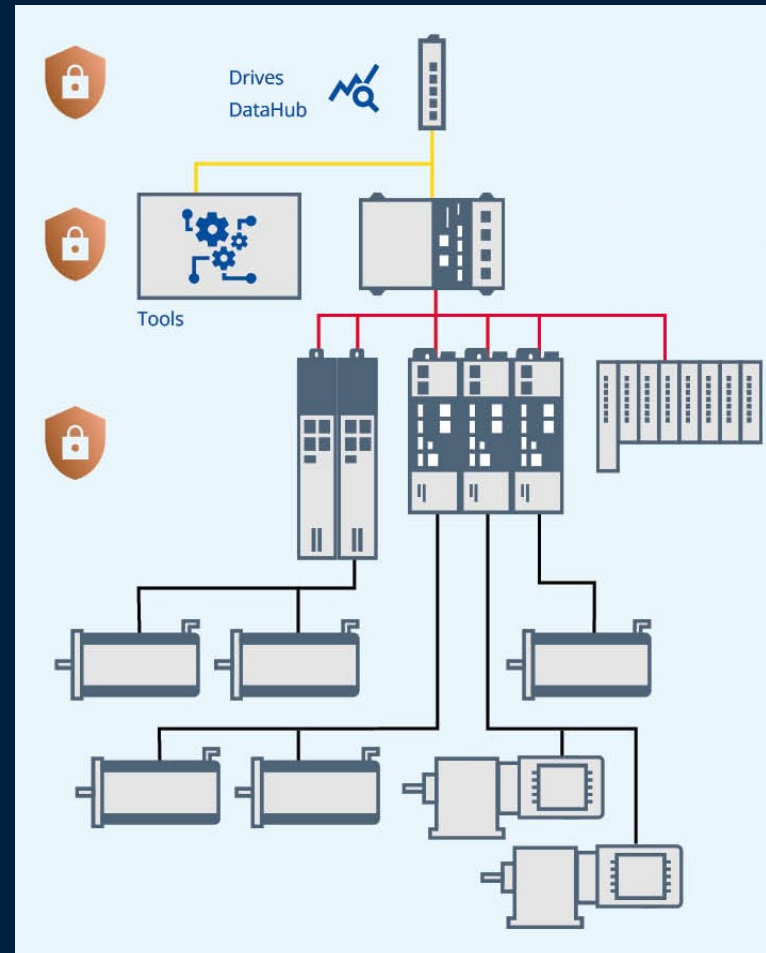
Umsetzung von Security Maßnahmen

Zugriffsschutz, Updates, Schnittstellen, etc.



Unser Support

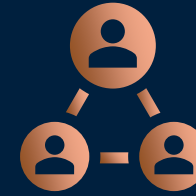
Die Security-Features in unseren Produkten unterstützen zusätzlich Ihre getroffenen Security Maßnahmen.



Implementieren Sie technische Schutzmaßnahmen wie Zugriffskontrollen, regelmäßige Updates und sichere Schnittstellen. Achten Sie dabei auf eine hohe Usability

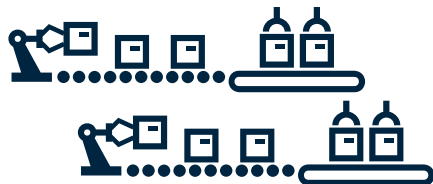
Dialog mit Kunden und Zulieferern

Gemeinsam sind wir stark



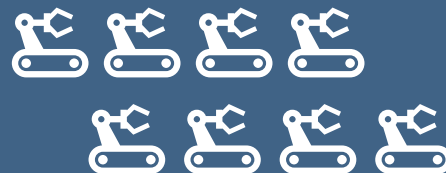
Maschinenbetreiber

- Entwickelt und fordert Security-Konzepte für seine Produktionsanlagen
- Schützt Daten und Know-how seiner Prozesse
- Möchte Maschinenstillstände verhindern
- Stellt ein Expertenteam (**CSIRT**) für schnelle Reaktion im Notfall
- Hält die Gesetze (NIS-2) ein



Maschinenbauer

- Entwickelt Security-Konzepte für seine Maschinen
- Schützt Daten und Know-how der Betreiber
- Verhindert Maschinenstillstände
- Stellt ein Expertenteam (**PSIRT**) für schnelle Reaktion im Notfall
- Hält die Gesetze (CRA, MVO) ein



Lenze

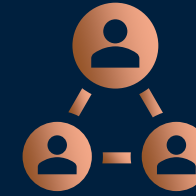
- Ermöglicht sichere Maschinen durch sichere Produkte mit Security-Features
- Schützt so Daten und Know-how der Maschinenbauer und -betreiber sowie die Maschinenverfügbarkeit
- Experte und Sparringspartner
- Lenze-Expertenteam (PSIRT) für schnelle Reaktion im Notfall
- Hält die Gesetze (CRA, MVO) ein



**Partnerschaft
und ein Dialog auf
Augenhöhe** führen zu
optimalen Security-
Konzepten.

Dialog mit Kunden und Zulieferern

Gemeinsam sind wir stark



Unser Support



Save the Date

Lenze Zukunftswerkstatt 2026
Cybersecurity

10.3. Garching
17.3. Groß Berkel



Suchen Sie aktiv den Austausch mit Ihren Zulieferern und Kunden, um gemeinsam Anforderungen zu definieren. Eine offene Kommunikation fördert Vertrauen und erleichtert die gemeinsame Reaktion auf Sicherheitsvorfälle.

Die 5-Punkte Checkliste für Ihre Sicherheit



- 1 Rechtliche Vorgaben & Normen kennen**
CRA, MVO, RED-DA, IEC 62443 – Mitarbeiterschulungen sicherstellen
- 2 Security-Schwachstellen managen**
PSIRT-Team & SBOM etablieren, Meldeprozesse definieren
- 3 Risiken systematisch analysieren**
Bedrohungen bewerten, Maßnahmen priorisieren
- 4 Technische Schutzmaßnahmen umsetzen**
Zugriffskontrollen, Updates – sichere & nutzerfreundliche Umsetzungen
- 5 Kooperation mit Partnern stärken**
Anforderungen abstimmen, Security offen besprechen

Lenze ist als
Partner für
Cyber Security
an Ihrer Seite

Weitere Informationen



Denis Göllner



**Lenze ist als
Partner für
Cyber Security
an Ihrer Seite**

Thank you!



Lenze SE

Referent/in	Denis Göllner
Bereich	BSAS
Adresse	Postfach 10 13 52 31763 Hameln GERMANY
Standort	Hans-Lenze-Straße 1 31855 Aerzen GERMANY
Telefon	+49 5154 82-2649
Telefax	
E-Mail	denis.goellner@Lenze.de

Dieses Dokument ist das geistige Eigentum von Lenze SE, Aerzen (Germany). Lenze ist der alleinige und exklusive Besitzer des Copyrights und des Leistungsschutzrechtes. Jegliche Nutzung dieses Dokuments ist nur mit der ausdrücklichen, schriftlichen Zustimmung durch Lenze gestattet. Technische Änderungen vorbehalten.

Lenze
engineers *in motion*

MOVE STRONGER.