BERICHT

Risikobewertung Cyberangriffe

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Maschinenbau, OT-Sicherheitskonzept
Version	0.1 Entwurf
Datum	04.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR – Veröffentlichung, fiktive Demonstrationsanlage

Dieses Dokument enthält vertrauliche Informationen über die Sicherheitslage der betrachteten Anlagen. Weitergabe, Vervielfältigung oder Veröffentlichung nur mit Zustimmung des Auftraggebers.

Dokumentinformationen

VERSIONSHISTORIE

Version	Datum	Autor	Änderung
0.1	04.11.2026	M. Gilg	Erstentwurf

VERTEILER

Name	Organisation	Rolle
[Name]	[Auftraggeber]	Geschäftsführung
[Name]	[Auftraggeber]	Technische Leitung, Betriebsleitung

Inhalt

1 Management Summary

2 Ausgangslage und Methode

3 Ergebnisse

4 Maßnahmen

5 Nächste Schritte

1 Management Summary

Für den fiktiven Maschinenbauer mit 15 Maschinen, Lager, fahrerlosen Transportfahrzeugen und Messraum wurden sechs Angriffe bewertet: manipulierte NC-Programme, Fernwartungsrouter eines Herstellers, Doppelbelegung im Hochregallager, Fahrzeuge über das WLAN, verfälschtes Messraumklima und Ransomware gegen MES und Programmverwaltung.

Ohne Härtung sind 1 Szenarien kritisch. Im Planungsstand sind 1 hoch und 3 mittel. Am schwersten wiegen die leisen Angriffe auf die Qualität: veränderte NC-Programme und ein verfälschtes Messraumklima. Beide nutzen gewollte Wege; keine Segmentierung hält sie auf, nur Freigabe mit Prüfsumme, Erstteilmessung und eine unabhängige Messraumüberwachung.

GESAMTBEWERTUNG

Die Sicherheitsfunktionen der Maschinen schützen Menschen auch bei einem Angriff. Die Qualität schützen sie nicht: Fehlerhafte Teile beim Kunden sind für einen Maschinenbauer das größte Risiko, und sie entstehen leise.

SZENARIEN NACH RISIKOKLASSE

Klasse	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
KRITISCH	1	1	1	0
HOCH	3	1	1	0
MITTEL	2	3	1	0
NIEDRIG	0	1	3	6

2 Ausgangslage und Methode

Grundlage sind Fabrikplan und Versorgungs-R&I MB-FP-001, das Kommunikations- und Sicherheitskonzept und der HTML-Leitstand (Maschinenbau_Leitstand_PurpleTeam.html) mit Simulation, Netzwerkverkehr, Segmentierung und den Szenarien M1 bis M6. Jedes Szenario ist dort nachgestellt; der Mitschnitt zeigt denselben Verlauf.

- **Risiko** ist Auswirkung (A) mal Eintrittswahrscheinlichkeit (W), je 1 bis 5, in Anlehnung an IEC 62443-3-2.
- **Auswirkung** nach der schwersten Kategorie: Mensch, Lebensmittelsicherheit und Umwelt, Betrieb und Finanzen.
- **Vier Stände:** Ohne Härtung (flaches Netz, keine Maßnahme); Planungsstand (Zonen und Zellenfirewalls, H05, H07, H10; Herstellerrouter vorhanden); Mikrosegmentierung (Planungsstand plus Segment je Maschine); Vollständig (Mikrosegmentierung und H01 bis H14).
- **Klassen:** KRITISCH ab 15, HOCH 10 bis 14, MITTEL 5 bis 9, NIEDRIG bis 4. Tolerierbar ist NIEDRIG, MITTEL mit Freigabe des Betreibers.

HÄRTUNGSMASSNAHMEN

Nr.	Maßnahme	Planungsstand
H01	Fernwartungsrouter der Hersteller entfernen bzw. hinter die Firewall; Fernwartung nur über SINEMA RC mit Freigabe je Sitzung	fehlt
H02	Eigene Benutzerverwaltung im OT mit MFA, keine IT-Konten auf Jump-Host, MES und Programmverwaltung	fehlt
H03	Zugriffsschutz für SINUMERIK und S7-1500: Zugriffsstufen, PUT/GET aus, Bedienrechte an der Maschine	fehlt
H04	Freigabe-Workflow für NC-Programme mit Prüfsumme und Vier-Augen; Maschine lädt nur freigegebene Programme	fehlt
H05	Feste Grenzen und Plausibilisierung in den SPS: Lageraufträge, KSS-Konzentration, Argon	umgesetzt
H06	Engineering und Service nur von den Engineering-Stationen, Änderungen mit Versionsverwaltung	fehlt
H07	Sicherheitsfunktionen eigenständig: Safety Integrated, F-Programme, Laserscanner, Lichtvorhänge, O2-Mangel hart	umgesetzt
H08	Erste Teile nach Programmänderung messen; Stichprobenprüfung im Messraum unabhängig vom MES	fehlt
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Bedienrechner, Server und Messrechner	fehlt
H10	Offline-Sicherung von NC-Programmen, SPS-Projekten, MES und LVS; geübter Wiederanlauf	umgesetzt
H11	OT-Monitoring mit Auswertung von OPC UA, SMB, MQTT und S7	fehlt
H12	Messraumklima unabhängig überwacht: eigener Temperaturlogger im Messraum, Abgleich mit der Gebäudeleittechnik	fehlt
H13	WLAN mit WPA3-Enterprise, Zertifikate je Fahrzeug; Port Security und NAC in den Zellen	fehlt

Nr.	Maßnahme	Planungsstand
H14	Reaktionsplan mit Herstellern, Kunden-Information bei Qualitätsverdacht, jährliche Übung	fehlt
SEG	Zonen mit Firewall und Zellenfirewalls, Mikrosegmente	Zonen ja, Mikro fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
M1	Manipulierte NC-Programme aus der Konstruktion	KRITISCH	KRITISCH	KRITISCH	NIEDRIG
M2	Fernwartungsrouter des Herstellers an BAZ-05	HOCH	MITTEL	NIEDRIG	NIEDRIG
M3	Doppelbelegung im Hochregallager	MITTEL	NIEDRIG	NIEDRIG	NIEDRIG
M4	Fahrerlose Transportfahrzeuge über das WLAN	MITTEL	MITTEL	NIEDRIG	NIEDRIG
M5	Messraumklima über die Gebäudeleittechnik verfälscht	HOCH	HOCH	HOCH	NIEDRIG
M6	Ransomware gegen MES und Programmverwaltung	HOCH	MITTEL	MITTEL	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in vier Ständen

3.2 Szenarien im Detail

3.2.1 M1 Manipulierte NC-Programme aus der Konstruktion

Ohne Härtung	**KRITISCH** (A 4 × W 4 = 16)
Betroffene Systeme	CAM-Arbeitsplatz (Z01), NC-Gateway (Z03), Programmverwaltung (Z04), Bedientafeln BAZ-01 bis 04 (Z07)
Ort	Konstruktion, Serverraum, Zerspanung
Angriffsweg	1. CAM-Arbeitsplatz kompromittiert (T0817, T0866) 2. Veränderte Programme ins NC-Gateway (T0843) 3. Programmverwaltung überträgt an die Maschinen (T0843, T0821) 4. Maße außerhalb Toleranz, Teile beim Kunden (T0831, T0882)
Folgen	Teile mit Maßabweichungen, die erst beim Kunden auffallen; Rückruf, Haftung, bei sicherheitsrelevanten Baugruppen Gefahr für Menschen.
Planungsstand	**KRITISCH** (A 4 × W 4 = 16); gelingt
Mit Mikrosegmentierung	**KRITISCH** (A 4 × W 4 = 16); gelingt
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H04
Restrisiko	Der Programmweg ist gewollt; nur Freigabe mit Prüfsumme und Messung der ersten Teile halten ihn sicher.
Schaden im Ernstfall	0,5 bis 5 Mio. €: Rückruf, Haftung, Kundenverlust
Referenz	MITRE ATT&CK for ICS v20: T0817, T0866, T0843, T0821, T0831, T0882; IEC 62443-3-3 SR 3.4, SR 3.5

3.2.2 M2 Fernwartungsrouter des Herstellers an BAZ-05

Ohne Härtung	**HOCH** (A 3 × W 4 = 12)
Betroffene Systeme	Herstellerrouter an BAZ-05, Bedientafeln (Z07)
Ort	Zerspanung
Angriffsweg	1. Fernservice des Herstellers kompromittiert (T0866) 2. VNC über den Router an der Maschine, an der Firewall vorbei (T0822, T0886) 3. Ausbreitung auf andere Bedientafeln (T0866) 4. Bedientafeln verschlüsselt, Stillstand (T0809, T0828)
Folgen	Bedientafeln verschlüsselt, Maschinen stehen; Wiederherstellung nur mit den Herstellern, Lieferverzug über Tage.
Planungsstand	**MITTEL** (A 2 × W 4 = 8); gelingt, Wirkung begrenzt durch H10
Mit Mikrosegmentierung	**NIEDRIG** (A 2 × W 2 = 4); gestoppt in Schritt 3 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 2 durch Mikrosegmentierung
Restrisiko	Hersteller brauchen Fernzugang; ein zentraler Zugang mit Freigabe ersetzt die Router an den Maschinen.
Schaden im Ernstfall	0,3 bis 2 Mio. €: Stillstand, Wiederherstellung mit Herstellern
Referenz	MITRE ATT&CK for ICS v20: T0866, T0822, T0886, T0809, T0828; IEC 62443-3-3 SR 1.13; IEC 62443-2-4

3.2.3 M3 Doppelbelegung im Hochregallager

Ohne Härtung	**MITTEL** (A 4 × W 2 = 8)
Betroffene Systeme	Jump-Host (Z03), Lagerverwaltung (Z04), Lagersteuerung und RBG (Z11)
Ort	Serverraum, Hochregallager
Angriffsweg	1. Admin-Daten erbeutet (T0859) 2. RDP vom Jump-Host zur Lagerverwaltung (T0886) 3. Fahrauftrag auf belegtes Fach (T0836, T1692.001) 4. Absturz im Regal (T0879)
Folgen	Palette auf belegtem Fach: Absturz im Regal, Gefahr für Personen bei Wartung, Gasse über Tage gesperrt.
Planungsstand	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H05
Mit Mikrosegmentierung	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H05
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02
Restrisiko	Die Lagersteuerung prüft Aufträge gegen ihren eigenen Bestand; das hält auch Fehler ohne Angriff auf.
Schaden im Ernstfall	0,2 bis 1 Mio. €, Gefahr bei Wartung im Regal
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0836, T0879; IEC 62443-3-3 SR 3.5; DIN EN 528

3.2.4 M4 Fahrerlose Transportfahrzeuge über das WLAN

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Industrie-WLAN, Flottenmanager, Fahrzeuge (Z12)
Ort	Halle
Angriffsweg	1. WLAN-Schlüssel ausgespäht, fremdes Gerät verbunden (T0860) 2. Anmeldung am MQTT-Broker (T0886) 3. Sofortbefehle an die Fahrzeuge (T1692.001) 4. Transporte stehen, Maschinen warten (T0815, T0828)
Folgen	Fahrzeuge stehen oder fahren falsche Ziele an, Material fehlt an den Maschinen; der Personenschutz der Laserscanner bleibt wirksam.
Planungsstand	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H07
Mit Mikrosegmentierung	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H13
Restrisiko	Der Personenschutz der Laserscanner bleibt; der Schaden liegt im Stillstand.
Schaden im Ernstfall	0,05 bis 0,3 Mio. €: Stillstand, Ersatztransporte
Referenz	MITRE ATT&CK for ICS v20: T0860, T0886, T1692.001, T0815, T0828; IEC 62443-3-3 SR 1.2, SR 1.9

3.2.5 M5 Messraumklima über die Gebäudeleittechnik verfälscht

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Büro-PC (Z01), Vision Center (Z14), MES (Z04)
Ort	Büro, Messraum
Angriffsweg	1. Büro-PC der Haustechnik kompromittiert (T0817) 2. Zugriff auf das Vision Center vom Büro (T0886) 3. Sollwert 21,5 °C, Meldung an das MES 20,0 °C (T0836, T1692.002) 4. Falsche Freigaben, Teile beim Kunden (T0882)
Folgen	Messergebnisse systematisch verfälscht: Teile außerhalb Toleranz werden freigegeben und ausgeliefert.
Planungsstand	**HOCH** (A 4 × W 3 = 12); gelingt
Mit Mikrosegmentierung	**HOCH** (A 4 × W 3 = 12); gelingt
Vollständig	**NIEDRIG** (A 2 × W 2 = 4); gelingt, Wirkung begrenzt durch H12
Restrisiko	Messungen hängen am Raumklima; eine unabhängige Temperaturüberwachung ist die einzige sichere Gegenprobe.
Schaden im Ernstfall	0,5 bis 5 Mio. €: fehlerhafte Teile beim Kunden
Referenz	MITRE ATT&CK for ICS v20: T0817, T0886, T0836, T1692.002, T0882; DIN EN ISO 1

3.2.6 M6 Ransomware gegen MES und Programmverwaltung

Ohne Härtung	**HOCH** (A 3 × W 4 = 12)
Betroffene Systeme	Jump-Host (Z03), MES, Programmverwaltung, LVS (Z04)
Ort	Serverraum
Angriffsweg	1. Admin-Daten aus der IT gestohlen (T0859) 2. RDP vom Jump-Host zu den Servern (T0886) 3. Server verschlüsselt (T0809) 4. Fertigung steht (T0828)
Folgen	Keine Aufträge, keine Programme, kein Lager: Fertigung steht bis zur Wiederherstellung.
Planungsstand	**MITTEL** (A 2 × W 4 = 8); gelingt, Wirkung begrenzt durch H10
Mit Mikrosegmentierung	**MITTEL** (A 2 × W 4 = 8); gelingt, Wirkung begrenzt durch H10
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02
Restrisiko	Maschinen und Sicherheitsfunktionen arbeiten weiter; Notbetrieb mit Papierlaufkarten und lokalen Programmen.
Schaden im Ernstfall	0,3 bis 2 Mio. €: Stillstand über Tage
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0828; IEC 62443-3-3 SR 1.1, SR 3.2, SR 7.3

4 Maßnahmen

Bezug zeigt, in welchen Szenarien die Maßnahme einen Schritt stoppt oder die Wirkung begrenzt.

Nr.	Maßnahme	Bezug	Priorität
H01	Fernwartungsrouter der Hersteller entfernen bzw. hinter die Firewall; Fernwartung nur über SINEMA RC mit Freigabe je Sitzung	alle	**Hoch**
H02	Eigene Benutzerverwaltung im OT mit MFA, keine IT-Konten auf Jump-Host, MES und Programmverwaltung	M3, M6	**Hoch**
H03	Zugriffsschutz für SINUMERIK und S7-1500: Zugriffsstufen, PUT/GET aus, Bedienrechte an der Maschine	alle	**Mittel**
H04	Freigabe-Workflow für NC-Programme mit Prüfsumme und Vier-Augen; Maschine lädt nur freigegebene Programme	M1	**Hoch**
H05	Feste Grenzen und Plausibilisierung in den SPS: Lageraufträge, KSS-Konzentration, Argon	M3	umgesetzt
H06	Engineering und Service nur von den Engineering-Stationen, Änderungen mit Versionsverwaltung	alle	**Mittel**
H07	Sicherheitsfunktionen eigenständig: Safety Integrated, F-Programme, Laserscanner, Lichtvorhänge, O2-Mangel hart	M3, M4	umgesetzt
H08	Erste Teile nach Programmänderung messen; Stichprobenprüfung im Messraum unabhängig vom MES	M1	**Hoch**
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Bedienrechner, Server und Messrechner	M2, M6	**Mittel**
H10	Offline-Sicherung von NC-Programmen, SPS-Projekten, MES und LVS; geübter Wiederanlauf	M2, M6	umgesetzt
H11	OT-Monitoring mit Auswertung von OPC UA, SMB, MQTT und S7	alle	**Mittel**
H12	Messraumklima unabhängig überwacht: eigener Temperaturlogger im Messraum, Abgleich mit der Gebäudeleittechnik	M5	**Hoch**
H13	WLAN mit WPA3-Enterprise, Zertifikate je Fahrzeug; Port Security und NAC in den Zellen	M4	**Mittel**
H14	Reaktionsplan mit Herstellern, Kunden-Information bei Qualitätsverdacht, jährliche Übung	alle	**Mittel**
SEG	Mikrosegmente: jede Maschine, Fahrzeuge, Bedientafeln getrennt	M2, M4	**Hoch**

Tabelle 2: Maßnahmen und Priorität im Planungsstand

Fehlerhafte Teile beim Kunden (M1, M5) bedeuten Rückruf, Haftung und Vertrauensverlust. Die Maßnahmen mit Priorität Hoch sind dagegen überschaubar und teils rein organisatorisch.

4.1 Rechtlicher Rahmen

- **NIS2:** Maschinenbau gehört zu Anlage 2 BSIG. Mit 250 Beschäftigten ist das Unternehmen wichtige Einrichtung: Risikomanagement nach § 30, Meldepflichten nach § 32 (24 h, 72 h, Abschluss nach einem Monat), Registrierung nach § 33, Pflichten der Geschäftsleitung nach § 38 BSIG.
- **CRA:** Für die eigenen Maschinen gelten seit 11.09.2026 die Meldepflichten nach Art. 14 (aktiv ausgenutzte Schwachstellen, schwere Vorfälle) über die Single Reporting Platform der ENISA; die übrigen Pflichten ab 11.12.2027.
- **Maschinenverordnung (EU) 2023/1230:** ab 20.01.2027; Anhang III Nr. 1.1.9 verlangt Schutz gegen Korrumpierung, Nr. 1.2.1 sichere Steuerungen auch bei böswilligen Eingriffen.
- **Arbeitsschutz:** Sicherheitsfunktionen der Maschinen, Regale und Fahrzeuge nach DIN EN ISO 13849; Explosionsschutz für Metallpulver nach GefStoffV.

HINWEIS

Werte und Szenarien beziehen sich auf eine fiktive Anlage. Für einen realen Betrieb sind Bewertung, Kosten und Fristen mit Betreiber, Behörden und Lieferanten abzustimmen.

5 Nächste Schritte

- Freigabe-Workflow mit Prüfsumme für NC-Programme und Erstteilmessung (H04, H08).
- Herstellerrouter entfernen, Fernwartung nur über SINEMA RC (H01).
- Unabhängiger Temperaturlogger im Messraum, GLT-Bedienung nur aus der OT (H12).
- Planspiel mit Qualitätssicherung und Kundeninformation (H14).