BERICHT

Angriffspfade und Reaktionsplan

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Maschinenbau, Incident Response
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 Vorgehen

3 Angriffspfade und Playbooks je Szenario

4 Reaktionsplan

5 Nächste Schritte

1 Management Summary

Für die sechs Hochrisiko-Szenarien zeigt dieses Dokument die Wege eines Angreifers bis zur Wirkung, die Barrieren, die ihn stoppen, und die Punkte, an denen Leitwarte, Schichtführer und OT-Security ihn erkennen. Daraus ist je Szenario ein Playbook abgeleitet.

Zwei Grundsätze bestimmen den Plan: Menschen und Kunden vor Terminen, und bei Zweifel an Programmen oder Messungen nichts ausliefern. Die Reaktion setzt in der Halle an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Die Fertigung bleibt beherrschbar, wenn freigegebene Programme offline gesichert sind und Messungen unabhängig gegengeprüft werden können. Lose mit Zweifel werden gesperrt, bis die Messung sie freigibt.

ID	Szenario	Erster Erkennungspunkt	Playbook
M1	Manipulierte NC-Programme aus der Konstruktion	Prüfsumme weicht ab, Freigabe fehlt	PB-M1
M2	Fernwartungsrouter des Herstellers an BAZ-05	SMB zwischen Maschinen, VNC ohne Wartung	PB-M2
M3	Doppelbelegung im Hochregallager	RDP zur Lagerverwaltung ohne Wartung	PB-M3
M4	Fahrerlose Transportfahrzeuge über das WLAN	Neues Gerät im WLAN	PB-M4
M5	Messraumklima über die Gebäudeleittechnik verfälscht	Sollwertänderung außerhalb der Wartung	PB-M5
M6	Ransomware gegen MES und Programmverwaltung	RDP außerhalb der Wartung	PB-M6

2 Vorgehen

- **Pfade** in fünf Stufen nach MITRE ATT&CK for ICS v20: Erstzugang, Ausbreitung, Zugriff auf Steuerung, Manipulation, Wirkung.
- **Barrieren** (rot) sind die Härtungsmaßnahmen H01 bis H14 und die Segmentierung.
- **Erkennungspunkte** (grün) sind die Auslöser der Playbooks.
- **Playbooks** mit Auslöser, Sofortmaßnahmen, Eindämmen, Beseitigen, Wiederherstellen und Melden, jeweils mit Zuständigkeit.

3 Angriffspfade und Playbooks je Szenario

3.1 M1 Manipulierte NC-Programme aus der Konstruktion

Ein CAM-Arbeitsplatz in der IT ist kompromittiert. Die Schadsoftware verändert beim Postprozessieren Werkzeugkorrekturen und Zustellungen um wenige hundertstel Millimeter. Die Programme laufen auf dem regulären Weg über NC-Gateway und Programmverwaltung an die Bearbeitungszentren. Risiko: **KRITISCH** ohne Härtung, **KRITISCH** im Planungsstand, **KRITISCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.

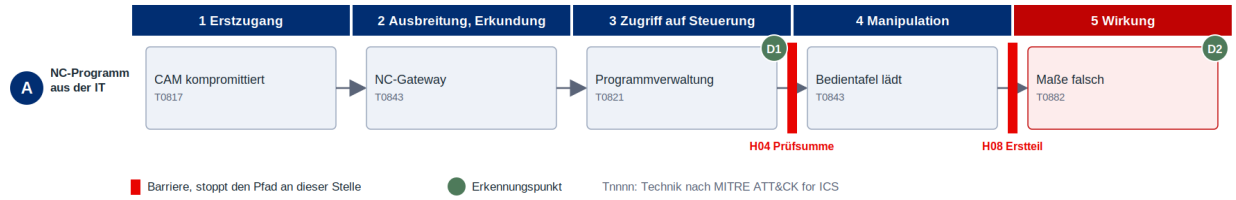


Abbildung: Angriffspfade M1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Prüfsumme weicht ab, Freigabe fehlt	Programmverwaltung
D2	Ausschuss steigt an mehreren Maschinen	Qualität, MES

PLAYBOOK PB-M1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Fertigung mit betroffenen Programmen stoppen, Lose sperren.	Meister
Eindämmen	NC-Gateway sperren, CAM-Arbeitsplätze prüfen, Programme aus der Offline-Sicherung.	OT-Security
Melden	BSI (wichtige Einrichtung, § 32 BSIG), Kunden nach Vertrag, Polizei.	Geschäftsführung
Wiederherstellen	Freigabe-Workflow mit Prüfsumme, Erstteilmessung nach jeder Programmänderung.	Fertigungsleitung, Hersteller

3.2 M2 Fernwartungsrouter des Herstellers an BAZ-05

Der Fernservice des Werkzeugmaschinenherstellers wird kompromittiert. Über den eigenen Router an BAZ-05 erreicht der Angreifer per VNC die Bedientafel, an der Firewall vorbei. Von dort breitet sich Ransomware auf die anderen Bedientafeln aus. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade M2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	SMB zwischen Maschinen, VNC ohne Wartung	OT-Monitoring
D2	Erpresserhinweis an den Bedientafeln	Werker

PLAYBOOK PB-M2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Router aller Hersteller trennen, betroffene Zelle isolieren.	Meister
Eindämmen	Bedientafeln vom Netz, Umfang feststellen.	OT-Security
Melden	BSI (§ 32 BSIG), Hersteller, Polizei.	Geschäftsführung
Wiederherstellen	Bedientafeln mit Hersteller neu aufsetzen, Router durch zentralen Fernzugang ersetzen.	Fertigungsleitung, Hersteller

3.3 M3 Doppelbelegung im Hochregallager

Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host auf die Lagerverwaltung, verändert den Bestand und schickt Fahraufträge auf belegte Fächer. Risiko: **MITTEL** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

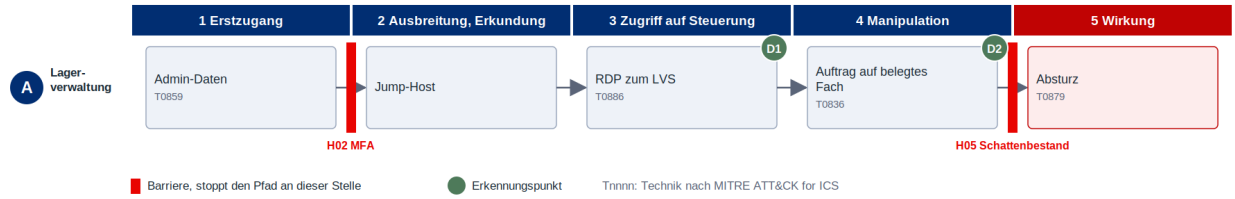


Abbildung: Angriffspfade M3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP zur Lagerverwaltung ohne Wartung	OT-Monitoring
D2	Lagersteuerung meldet Doppelbelegung	Lager

PLAYBOOK PB-M3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Automatik aus, Gasse sperren.	Meister
Eindämmen	Zugang sperren, Bestand gegen SPS und Sicherung vergleichen.	OT-Security
Melden	BSI (§ 32 BSIG), Berufsgenossenschaft bei Verletzung.	Geschäftsführung
Wiederherstellen	Bestand korrigieren, Regalprüfung nach DIN EN 15635.	Fertigungsleitung, Hersteller

3.4 M4 Fahrerlose Transportfahrzeuge über das WLAN

Der WLAN-Schlüssel ist bekannt geworden. Ein fremdes Gerät verbindet sich, meldet sich am MQTT-Broker des Flottenmanagers an und schickt den Fahrzeugen Sofortbefehle nach VDA 5050. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade M4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Neues Gerät im WLAN	WLAN-Controller
D2	Befehle ohne Auftrag des Flottenmanagers	Flottenmanager, Monitoring

PLAYBOOK PB-M4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Fahrzeuge in sicheren Halt, Ersatztransporte.	Meister
Eindämmen	WLAN-Schlüssel tauschen, fremdes Gerät suchen.	OT-Security
Melden	BSI bei erheblicher Wirkung, Polizei.	Geschäftsführung
Wiederherstellen	WPA3-Enterprise mit Zertifikaten, Broker nur für bekannte Clients.	Fertigungsleitung, Hersteller

3.5 M5 Messraumklima über die Gebäudeleittechnik verfälscht

Ein Büro-PC der Haustechnik ist kompromittiert. Über die Bedienoberfläche des Vision Center hebt der Angreifer den Sollwert des Messraums auf 21,5 °C und lässt dem MES weiter 20,0 °C melden. Die Freigabe der Messprotokolle bleibt aktiv. Risiko: **HOCH** ohne Härtung, **HOCH** im Planungsstand, **HOCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade M5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Sollwertänderung außerhalb der Wartung	Gebäudeleittechnik
D2	Unabhängiger Logger weicht ab	Qualität

PLAYBOOK PB-M5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Freigaben sperren, Messraum auf unabhängigen Logger prüfen.	Meister
Eindämmen	Zugang aus dem Büro sperren.	OT-Security
Melden	BSI (§ 32 BSIG), Kunden nach Vertrag.	Geschäftsführung
Wiederherstellen	Unabhängige Messraumüberwachung, GLT-Bedienung nur aus der OT.	Fertigungsleitung, Hersteller

3.6 M6 Ransomware gegen MES und Programmverwaltung

Ransomware aus der IT scheitert am direkten Weg. Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host auf MES, Programmverwaltung und Lagerverwaltung und verschlüsselt sie. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

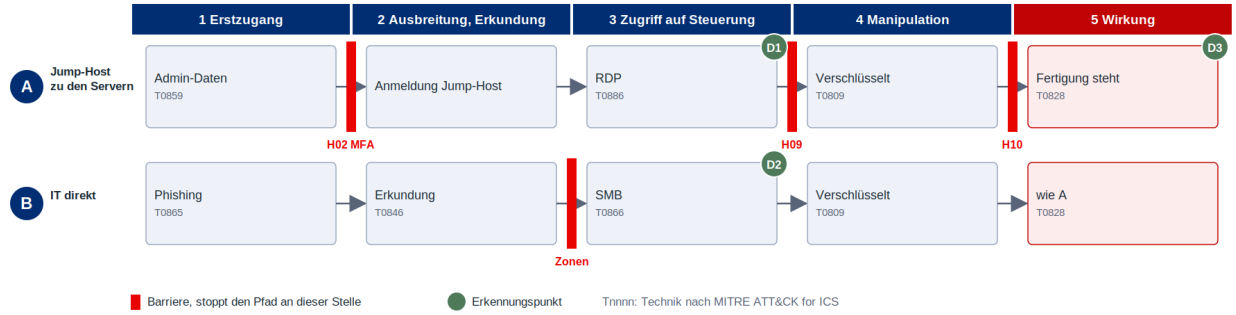


Abbildung: Angriffspfade M6

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP außerhalb der Wartung	OT-Monitoring
D2	Firewall deny vom Büro-PC	Log-Sammler
D3	Leitstand ohne Daten	Meister

PLAYBOOK PB-M6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Jump-Host und IT-Verbindung trennen.	Meister
Eindämmen	Konten sperren, Umfang feststellen.	OT-Security
Melden	BSI (24 h, 72 h, 1 Monat), Polizei, Versicherung.	Geschäftsführung
Wiederherstellen	Server aus Offline-Sicherung, Programme gegen freigegebenen Stand prüfen.	Fertigungsleitung, Hersteller

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Menschen, Kunden, Maschinen, Termine.
- **Bei Zweifel nichts ausliefern:** betroffene Lose sperren, Messprotokolle prüfen.
- **Programme nicht blind neu laden:** erst gegen die Offline-Sicherung vergleichen.
- **Hersteller einbinden:** bei Maschinen mit eigener Fernwartung sofort informieren.
- **Alles mit Uhrzeit festhalten:** Programmstände und Logs sind Beweismittel.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Maschinen	Programme lokal vom freigegebenen Stand, Bedienung vor Ort
Lager	Handbetrieb mit Bestandsliste auf Papier, RBG nur im Automatik mit gültigem Bestand
FTS	Transporte mit Stapler und Routenzug
Messraum	Freigabe nur mit unabhängigem Temperaturnachweis
MES	Papierlaufkarten, Rückerfassung nach Wiederanlauf

4.3 Rollen

Rolle	Aufgabe	Besetzung
Meister	erkennt, setzt Sofortmaßnahmen, alarmiert	[Name, Telefon]
Fertigungsleitung	Fertigung, Notbetrieb, Termine	[Name, Telefon]
Qualitätssicherung	Lose sperren, Messungen, Kunden	[Name, Telefon]
Gasmeister, Chemie	GDRM, Speicher, Wasserchemie	[Name, Telefon]
OT-Security	Bewertung, Zugänge trennen, Beweise, Wiederherstellung	[Name, Telefon]
Geschäftsführung	Stufe 3, Krisenstab, Meldungen, Öffentlichkeit	[Name, Telefon]

4.4 Stufen

Stufe	Merkmal	Entscheidet
1 Verdacht	einzelne Auffälligkeit ohne Wirkung	Meister mit OT-Security
2 Angriff bestätigt	Fertigung betroffen, kein Teil beim Kunden	Fertigungsleitung
3 Krise	fehlerhafte Teile beim Kunden, Verletzung, Stillstand über Tage	Geschäftsführung, Krisenstab

4.5 Meldungen

Anlass	Stelle	Frist
erheblicher Sicherheitsvorfall (§ 32 BSIG, wichtige Einrichtung)	gemeinsame Meldestelle BSI und BBK	Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h nach Kenntnis, Abschlussmeldung einen Monat nach der 72-h-Meldung
Aktiv ausgenutzte Schwachstelle oder schwerer Vorfall an eigenen Produkten (Art. 14 CRA, seit 11.09.2026)	Single Reporting Platform der ENISA, zuständiges CSIRT	Frühwarnung 24 h, Meldung 72 h, Abschlussbericht nach Art. 14 CRA
Qualitätsmangel ausgelieferter Teile	Kunden nach Vertrag	unverzüglich
Arbeitsunfall	Berufsgenossenschaft Holz und Metall	nach Vorgabe
Straftat	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarmliste mit Maschinenherstellern, Intralogistiker, FTS-Hersteller
- Offline-Sicherung der freigegebenen NC-Programme und SPS-Projekte
- Papierlaufkarten und Bestandsliste für den Notbetrieb
- Kontaktliste Qualitätsverantwortliche der Kunden
- Planspiel einmal im Jahr mit Qualitätssicherung

5 Nächste Schritte

- Rollen besetzen, Telefonliste mit Maschinenherstellern.
- Playbooks mit Fertigung, Qualität und Herstellern abstimmen.
- Erstes Planspiel mit Szenario M1 und Kundeninformation.