BERICHT

Angriffspfade und Reaktionsplan

Hartkäserei im Bestand, Playbooks für die Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Käserei, 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 vor Anlage (Ammoniak, Lauge) und im Zweifel nichts freigeben (Erhitzung, Fremdkörper, Füllmenge). Die Reaktion setzt vor Ort an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Die Käserei bleibt sicher, wenn Schreiber, Mannlochschalter und Druckbegrenzer unabhängig von der Leittechnik arbeiten und wenn bei Zweifeln an Erhitzung, Reinigung oder Röntgenprüfung keine Charge freigegeben wird. Mit 5 Personen braucht jede Rolle einen benannten Vertreter in der Rufbereitschaft.

ID	Szenario	Erster Erkennungspunkt	Playbook
K1	Kesselmilch-Erhitzung KZE-302 manipuliert	Tunnel außerhalb des Wartungsfensters, Schlüsselschalter ein	PB-K1
K2	Ventilknoten und CIP: Lauge ins Produkt	Engineering-Verbindung von einem Bedienplatz	PB-K2
K3	Kälteanlage KA-802 mit Ammoniak manipuliert	Modbus-Schreibbefehle vom Jump-Host	PB-K3
K4	Fernwartung der Würfellinie: Füllgewicht und Röntgen verstellt	Schlüsselschalter meldet Fernwartung nachts	PB-K4
K5	Fremder Laptop im Schaltschrank der Käsefertigung	Neue MAC-Adresse am Switch-Port	PB-K5
K6	Ransomware legt den Leitstand lahm	RDP außerhalb der Wartung	PB-K6

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 K1 Kesselmilch-Erhitzung KZE-302 manipuliert

Mit gestohlenen Zugangsdaten des Erhitzer-Lieferanten baut der Angreifer nachts einen Tunnel über SINEMA RC auf und schreibt per S7 PUT/GET Umschaltgrenze und Sollwert der Erhitzung: 62 °C statt 72 °C. Das Leitsystem zeigt weiter Werte aus derselben Steuerung. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade K1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Tunnel außerhalb des Wartungsfensters, Schlüsselschalter ein	SINEMA RC, Leitstand
D2	S7-Schreibzugriff aus dem Fernwartungsnetz	OT-Monitoring
D3	Schreiber RSG45 alarmiert, FDV-302 auf Rücklauf	Leitstand, Anlagenführer

PLAYBOOK PB-K1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	KZE auf Rücklauf, Käsefertiger anhalten, betroffene Chargen sperren.	Anlagenführer, Rufbereitschaft
Eindämmen	Fernwartung trennen, Erhitzersteuerung gegen octoplant-Sollstand prüfen.	OT-Security
Melden	Lebensmittelüberwachung bei ausgelieferter Ware, Polizei; BSI falls NIS2-pflichtig.	Geschäftsführung
Wiederherstellen	PUT/GET aus, Fernwartung je Sitzung freigeben, VW-Firewall vor der Erhitzersteuerung.	Betriebsleitung, Lieferant

3.2 K2 Ventilknoten und CIP: Lauge ins Produkt

Ein übernommener Bedienplatz im Leitsystem-Netz baut eine Engineering-Verbindung zur AS-100 auf und lädt einen Baustein mit aufgehobener Wegeverriegelung. Das Projektpasswort stammt von einem Dienstleister-Laptop. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

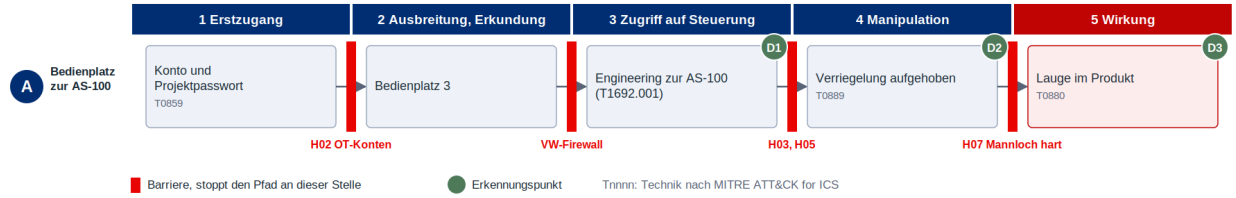


Abbildung: Angriffspfade K2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Engineering-Verbindung von einem Bedienplatz	OT-Monitoring
D2	octoplant meldet geänderten Baustein	octoplant, OT-Security
D3	pH im Käsefertiger, Leitfähigkeit im Ventilknoten	Leitstand

PLAYBOOK PB-K2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	CIP stoppen, Käsefertiger und Kesselmilch anhalten, Personen aus Behältern.	Anlagenführer, Rufbereitschaft
Eindämmen	Bedienplatz vom Netz, Projektpasswort ändern, AS-100 gegen Sollstand prüfen.	OT-Security
Melden	Lebensmittelüberwachung bei Auslieferung, BGN bei Verletzten; BSI falls NIS2-pflichtig.	Geschäftsführung
Wiederherstellen	Sollstand aus octoplant, Zugriffsschutz der CPU, Mannlochverriegelung zusätzlich hart.	Betriebsleitung, Lieferant

3.3 K3 Kälteanlage KA-802 mit Ammoniak manipuliert

Vom Jump-Host aus werden per Modbus die Hochdruckgrenze im Kälteregler hochgesetzt und die Verdichter gegen geschlossene Ventile gefahren. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade K3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Modbus-Schreibbefehle vom Jump-Host	OT-Monitoring
D2	Hochdruck steigt	Leitstand
D3	Druckbegrenzer, NH3-Gaswarnung	alle vor Ort

PLAYBOOK PB-K3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Räumen, Notabschaltung, bei NH3-Alarm Feuerwehr 112 und Nachbarn warnen.	Anlagenführer, Rufbereitschaft
Eindämmen	Sitzung trennen, Regler prüfen, Reifelager und Rohmilch überwachen.	OT-Security
Melden	Feuerwehr, Immissionsschutzbehörde bei Austritt, BGN; BSI falls NIS2-pflichtig.	Geschäftsführung
Wiederherstellen	Modbus nur lesend, Schreiben nur vom Panel vor Ort, Druckbegrenzer prüfen lassen.	Betriebsleitung, Lieferant

3.4 K4 Fernwartung der Würfellinie: Füllgewicht und Röntgen verstellt

Mit gestohlenen Zugangsdaten des Linienlieferanten baut der Angreifer um 02:10 Uhr einen Tunnel auf. Der Schlüsselschalter steht seit der letzten Wartung auf ein. Er setzt das Sollgewicht der Kontrollwaage auf 199 g und schaltet die Ausschleusung des Röntgens ab. Risiko: **KRITISCH** ohne Härtung, **KRITISCH** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

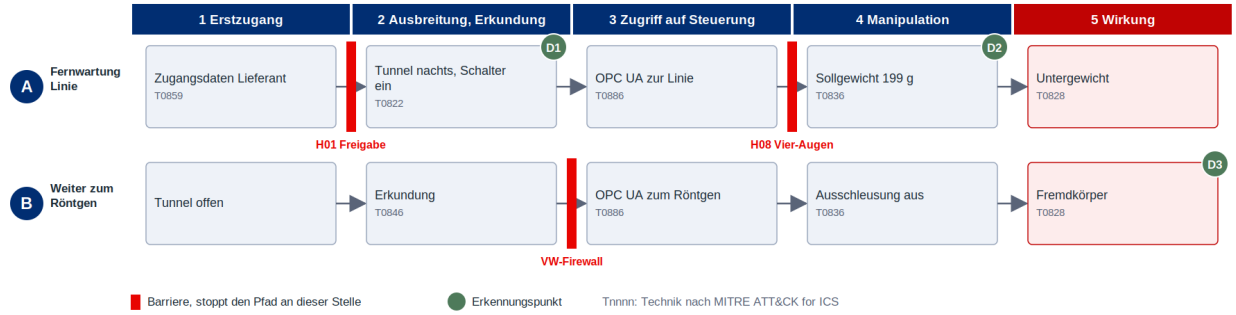


Abbildung: Angriffspfade K4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Schlüsselschalter meldet Fernwartung nachts	Leitstand
D2	Sollwertänderung ohne Auftrag	Leitstand, Anlagenführer
D3	Prüfkörpertest am Röntgen fällt durch	Qualitätssicherung

PLAYBOOK PB-K4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Linie stoppen, Sollwerte zurücksetzen, Ware seit Beginn sperren und nachprüfen.	Anlagenführer, Rufbereitschaft
Eindämmen	Fernwartung trennen, Schlüsselschalter aus, Zugang sperren.	OT-Security
Melden	Kunden und Eichbehörde bei Untergewicht; Lebensmittelüberwachung bei Fremdkörpern.	Geschäftsführung
Wiederherstellen	Freigabe je Sitzung, Schlüsselschalter mit Rückmeldung, Grenzen in der Liniensteuerung.	Betriebsleitung, Lieferant

3.5 K5 Fremder Laptop im Schaltschrank der Käsefertigung

Ein Servicetechniker steckt einen infizierten Laptop an den Feld-Switch der Käsefertigung. Die Schadsoftware benennt per PROFINET DCP eine Station um; die Peripherie der Käsefertigung fällt aus. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

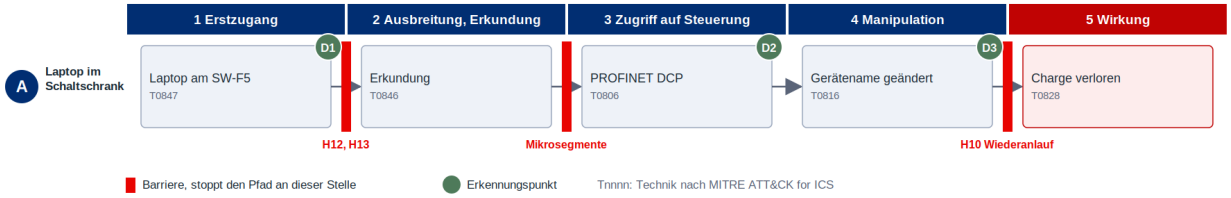


Abbildung: Angriffspfade K5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Neue MAC-Adresse am Switch-Port	Switch, OT-Monitoring
D2	DCP-Set an fremde Station	OT-Monitoring
D3	Station RIO-KF ausgefallen	Leitstand

PLAYBOOK PB-K5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Laptop trennen, Käsefertiger anhalten.	Anlagenführer, Rufbereitschaft
Eindämmen	Port sperren, Switch-Logs sichern.	OT-Security
Melden	Dienstleister, Versicherung.	Geschäftsführung
Wiederherstellen	Gerätenamen aus Sollstand, Laptopkontrolle, Port Security.	Betriebsleitung, Lieferant

3.6 K6 Ransomware legt den Leitstand lahm

Mit gestohlenen Admin-Daten meldet sich der Angreifer am Jump-Host an, springt per RDP auf den WinCC-Server und verschlüsselt ihn. Der Versuch vom infizierten Büro-PC direkt ins Leitsystem scheitert an der Firewall. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

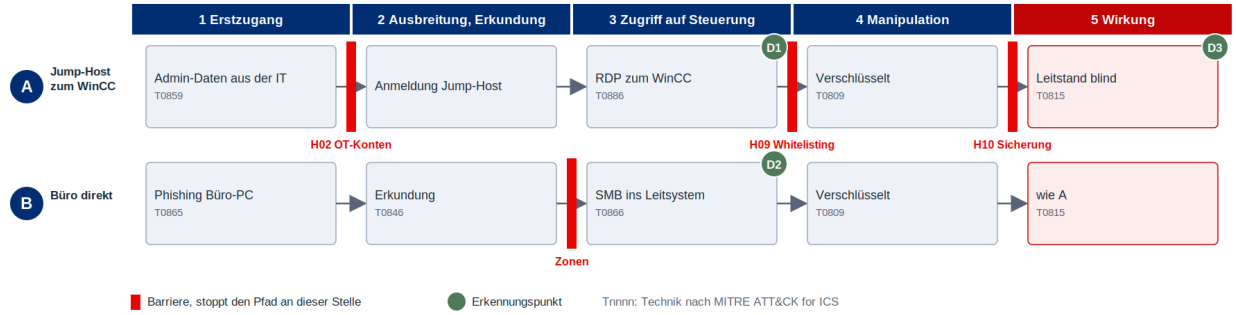


Abbildung: Angriffspfade K6

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP außerhalb der Wartung	OT-Monitoring
D2	FortiGate deny vom Büro-PC	Log-Sammler
D3	Bildschirme mit Erpresserhinweis	Leitstand

PLAYBOOK PB-K6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Jump-Host und Verbindungen zur IT sperren, Steuerungen weiterlaufen lassen.	Anlagenführer, Rufbereitschaft
Eindämmen	Konten sperren, betroffene Systeme identifizieren.	OT-Security
Melden	BSI falls NIS2-pflichtig (24 h, 72 h, 1 Monat), Polizei, Versicherung.	Geschäftsführung
Wiederherstellen	WinCC aus Offline-Sicherung, octoplant-Sollstände prüfen, Wiederanlauf.	Betriebsleitung, Lieferant

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Menschen, Verbraucher, Anlage, Betrieb.
- **Bei Zweifel nichts freigeben:** Chargen sperren, Schreiberstreifen und Rückstellmuster sichern.
- **Steuerungen nicht abschalten:** und nicht neu starten ohne Rücksprache mit der OT-Security; Diagnosepuffer sind Beweismittel.
- **Zugänge zuerst trennen:** SINEMA RC, Jump-Host, Schlüsselschalter der Fernwartung.
- **Alles mit Uhrzeit festhalten:** Fotos von Bildschirmen und Schaltschränken.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Erhitzung KZE-302	OEM-Steuerung regelt eigenständig, Schreiber RSG45 schaltet hart auf Rücklauf
Käsefertiger	laufende Charge mit Bedienpanel vor Ort zu Ende, keine neue Charge ohne Leitsystem
Salzbad, Reifelager	Kälte und Klima regeln eigenständig, Temperatur unabhängig überwacht
Würfellinie	nur mit Röntgen und Waage im Sollstand weiter, sonst Stopp
CIP	nur vor Ort, Mannlochschalter hart
Alarmierung	Gaswarnung NH3 und Störmelder unabhängig vom Leitsystem

4.3 Rollen

Rolle	Aufgabe	Besetzung
Anlagenführer	erkennt, setzt Sofortmaßnahmen, alarmiert	[Name, Telefon]
Lebensmitteltechniker	Produkt, Chargen, Freigaben	[Name, Telefon]
Elektriker, Instandhalter	Kälte, Schaltanlagen, Schlüsselschalter	[Name, Telefon]
Qualitätssicherung	Chargen sperren, Rückruf vorbereiten	[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	Anlagenführer mit OT-Security

Stufe	Merkmal	Entscheidet
2 Angriff bestätigt	keine Gefahr für Menschen oder Verbraucher	Betriebsleitung, Lebensmitteltechniker
3 Krise	NH3-Gefahr, Erreger oder Fremdkörper in ausgelieferter Ware	Geschäftsführung, Krisenstab

4.5 Meldungen

Anlass	Stelle	Frist
Lebensmittel mit Gesundheitsrisiko in Verkehr gebracht	zuständige Lebensmittelüberwachung; Rückruf nach VO (EG) 178/2002 Art. 19	unverzüglich
NH3-Austritt	Feuerwehr, Immissionsschutzbehörde	sofort
erheblicher Sicherheitsvorfall (§ 32 BSIG)	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
Arbeitsunfall	Berufsgenossenschaft Nahrungsmittel und Gastgewerbe (BGN)	nach Vorgabe des Trägers
Straftat	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarm- und Telefonliste in Leitstand und bei der Rufbereitschaft
- Notbetriebshandbuch je Bereich, Papierprotokoll für Chargen
- Offline-Sicherung mit octoplant, Wiederanlauf einmal im Jahr geübt
- Reaktionszeiten der Lieferanten von Erhitzer, Käsefertiger, Linie, Kälte und Leitsystem im Vertrag
- Planspiel zweimal im Jahr, eines mit Rückrufszenario

5 Nächste Schritte

- Rollen besetzen, Rufbereitschaft und Telefonliste festlegen.
- Playbooks mit Lebensmitteltechniker und Lieferanten abstimmen.
- Erstes Planspiel mit Szenario K1 (Erhitzung) und Rückruf.