BERICHT

Angriffspfade und Reaktionsplan

Brauerei 120.000 hl/a, Playbooks für die Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Brauerei, 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 (NH3, CO2) und im Zweifel nichts ausliefern (Lauge, Pasteurisation). Die Reaktion setzt vor Ort an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Die Brauerei bleibt sicher, wenn Gaswarnung, Hochdruckbegrenzer und Kesselsicherheit unabhängig von der Leittechnik arbeiten und wenn bei Zweifeln an Pasteurisation oder Reinigung keine Charge freigegeben wird.

ID	Szenario	Erster Erkennungspunkt	Playbook
B1	Kälteanlage NH3 über Fernwartung manipuliert	Tunnel des OEM-Routers ins Internet, Verbindung zur Kälte-SPS	PB-B1
B2	CO2-Warnung und Lüftung im Tankkeller abgeschaltet	Änderung Lüftung und Grenzwert ohne zweite Freigabe	PB-B2
B3	Lauge im Bier über den CIP-Ventilknoten	Neue MAC-Adresse am Switch, Port gesperrt	PB-B3
B4	Pasteurisation am Kurzzeiterhitzer abgesenkt	Rezeptänderung wartet auf zweite Freigabe	PB-B4
B5	Fernwartung des Füllers missbraucht, Linie steht	Sitzung ohne Wartungsauftrag	PB-B5
B6	Ransomware aus der IT über MES ins Leitsystem	SMB aus der IT in Richtung OT	PB-B6

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 B1 Kälteanlage NH3 über Fernwartung manipuliert

Ein Angreifer nutzt die Zugangsdaten des Kälteanlagenbauers. Ohne Jump-Host kommt er über den eigenen Fernwartungsrouter direkt an die Kälte-SPS, schaltet die Verflüssigerlüfter ab, zwingt die Verdichter in Dauerbetrieb und nimmt die Abschaltung aus der SPS. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade B1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Tunnel des OEM-Routers ins Internet, Verbindung zur Kälte-SPS	OT-Monitoring
D2	Verflüssigungsdruck steigt, Lüfter aus	Leitwarte
D3	Hochdruckbegrenzer, NH3-Gaswarnung, Geruch	Leitwarte, alle vor Ort
D4	Sitzungsanfrage ohne Wartungsauftrag	Jump-Host, Schichtführer

PLAYBOOK PB-B1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder D3	jeder
Sofort, 0 bis 15 min	Maschinenraum räumen, Notabschaltung Kälte, bei NH3-Alarm Feuerwehr 112, Windrichtung beachten, Umgebung warnen.	Schichtführer, Betriebstechnik
Eindämmen, bis 4 h	OEM-Router vom Netz, Zugang des Lieferanten sperren, Kälte-SPS gegen Sollstand prüfen, Tanktemperaturen von Hand überwachen.	OT-Security, Betriebstechnik
Beseitigen	Programm und Parameter der Kälte-SPS mit dem Kälteanlagenbauer wiederherstellen.	Kälteanlagenbauer
Wiederherstellen	Fernwartung nur über Jump-Host, Begrenzer und Gaswarnung durch befähigte Person prüfen lassen, Kälte schrittweise anfahren.	Betriebsleitung
Melden	Feuerwehr, Immissionsschutzbehörde bei Austritt, BGN bei Verletzten, BSI falls NIS2-pflichtig.	Geschäftsführung

3.2 B2 CO2-Warnung und Lüftung im Tankkeller abgeschaltet

Über einen übernommenen Bedienplatz schaltet der Angreifer auf dem regulären Bedienweg die Lüftung im Tankkeller ab, nimmt die CO2-Meldung aus der SPS und öffnet das CO2-Ablassventil eines gärenden Tanks in den Raum. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

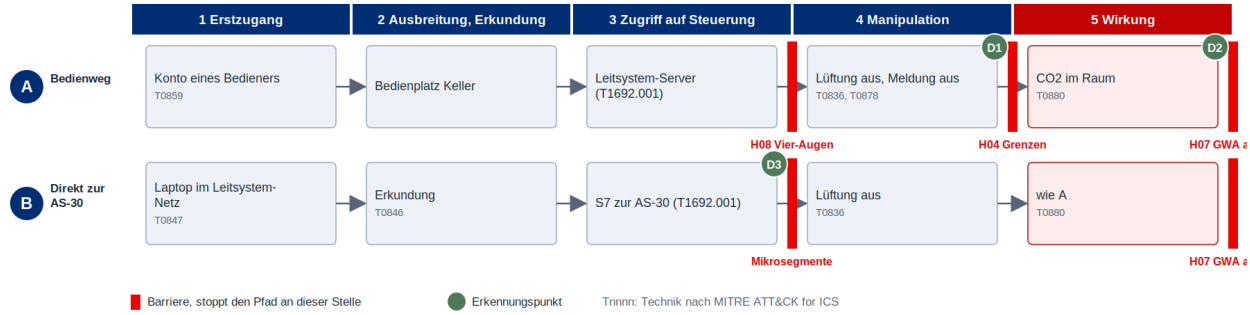


Abbildung: Angriffspfade B2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Änderung Lüftung und Grenzwert ohne zweite Freigabe	Leitsystem, Schichtführer
D2	Gaswarnanlage CO2 warnt und schaltet Lüftung	alle im Keller
D3	S7-Verbindung vom Bedienplatz direkt zur Steuerung	OT-Monitoring

PLAYBOOK PB-B2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder Beschwerden des Personals	jeder
Sofort, 0 bis 15 min	Raum räumen, nicht ohne Personenwarngerät betreten, Lüftung von Hand auf Stufe 2, Ablassventil schließen.	Kellermeister, Schichtführer
Eindämmen, bis 4 h	Bedienplatz vom Netz, Konto sperren, Bedienprotokoll der letzten Stunden prüfen.	OT-Security
Beseitigen	Rechte und Grenzwerte im Leitsystem prüfen, Passwörter tauschen.	OT-Security, Leitsystem-Lieferant
Wiederherstellen	Vier-Augen-Freigabe für Lüftung und Grenzwerte, Gaswarnanlage prüfen.	Betriebsleitung
Melden	BGN bei Verletzten, Polizei; BSI falls NIS2-pflichtig.	Geschäftsführung

3.3 B3 Lauge im Bier über den CIP-Ventilknoten

Ein infizierter Laptop eines Dienstleisters hängt am CIP-Switch. Er schreibt in die AS-40 und öffnet während der Laugephase das Doppelsitzventil zwischen CIP-Vorlauf und Produktleitung zur Abfüllung. Risiko: **KRITISCH** ohne Härtung, **KRITISCH** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade B3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Neue MAC-Adresse am Switch, Port gesperrt	Switch, OT-Monitoring
D2	S7-Schreibzugriff von unbekanntem Gerät	OT-Monitoring
D3	Leitfähigkeit vor dem Füller steigt, Umleitung	Leitwarte, Abfüllung

PLAYBOOK PB-B3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D3, Reklamation	jeder
Sofort, 0 bis 15 min	Füller stoppen, Produktleitung in den Kanal, betroffene Paletten sperren, Rückstellmuster sichern.	Schichtführer Abfüllung
Eindämmen, bis 4 h	Laptop vom Netz, Port sperren, CIP-Programme gegen Sollstand prüfen, Chargen eingrenzen.	OT-Security, Qualitätssicherung
Beseitigen	AS-40 aus Sicherung wiederherstellen, Ventilknoten mechanisch prüfen.	Automatisierer, Instandhaltung
Wiederherstellen	Verriegelung CIP gegen Produkt und Leitfähigkeitsüberwachung in Betrieb nehmen, Laptopkontrolle.	Betriebsleitung
Melden	Lebensmittelüberwachung, Rückruf nach VO (EG) 178/2002 Art. 19, Versicherung, Polizei.	Geschäftsführung, Qualitätssicherung

3.4 B4 Pasteurisation am Kurzzeiterhitzer abgesenkt

Über einen übernommenen Bedienplatz Abfüllung senkt der Angreifer im Rezept des Kurzzeiterhitzers den PE-Sollwert auf 5 und die Grenze für die Umleitung auf 0. Risiko: **HOCH** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade B4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Rezeptänderung wartet auf zweite Freigabe	Leitsystem
D2	SPS weist Sollwert unter 20 PE ab	Leitwarte
D3	PE-Aufzeichnung unter Soll, Laborbefund	Qualitätssicherung

PLAYBOOK PB-B4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort, 0 bis 15 min	Rezept zurücksetzen, KZE auf Umleitung prüfen, abgefüllte Paletten sperren.	Schichtführer Abfüllung
Eindämmen, bis 4 h	Bedienplatz vom Netz, Konto sperren, PE-Aufzeichnung auswerten.	OT-Security, Qualitätssicherung
Beseitigen	Rezepte und Grenzwerte gegen Sollstand prüfen.	Automatisierer
Wiederherstellen	Grenzen in der SPS und Vier-Augen-Freigabe für Rezepte.	Betriebsleitung
Melden	Lebensmittelüberwachung, falls Ware ausgeliefert wurde.	Qualitätssicherung

3.5 B5 Fernwartung des Füllers missbraucht, Linie steht

Mit erbeuteten Zugangsdaten des Füller-Herstellers verbindet sich der Angreifer über den Jump-Host zum Füller, ändert Rezepte und Antriebsparameter und springt vom Füller weiter zum Etikettierer. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

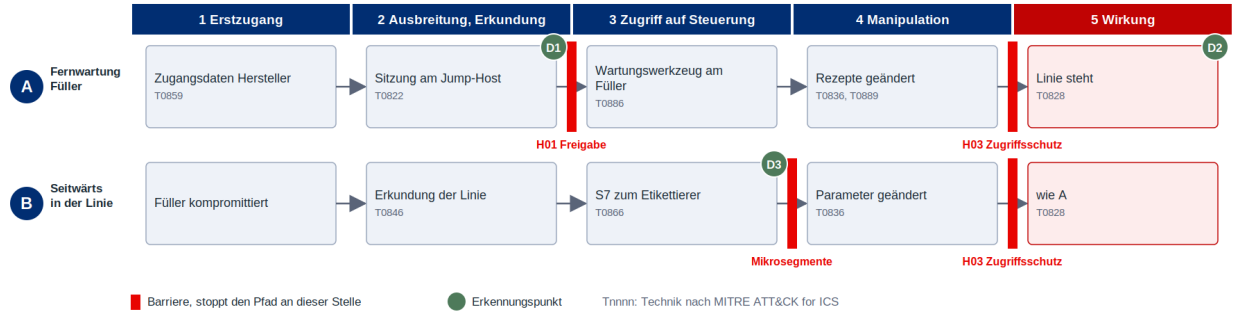


Abbildung: Angriffspfade B5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Sitzung ohne Wartungsauftrag	Jump-Host
D2	Füller im Zustand Störung im Linienmanagement	Schichtführer
D3	Verbindung zwischen Maschinen, die es sonst nie gibt	OT-Monitoring

PLAYBOOK PB-B5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort, 0 bis 15 min	Sitzung trennen, Füller stoppen, Zustand fotografieren, Hersteller anrufen.	Schichtführer, OT-Security
Eindämmen, bis 4 h	Konto des Herstellers sperren, andere Maschinen der Linie prüfen.	OT-Security
Beseitigen	Sollstand der Steuerung vom Hersteller einspielen.	Maschinenhersteller
Wiederherstellen	Freigabe je Sitzung, Mikrosegmentierung der Linie, Probelauf mit Qualitätskontrolle.	Betriebsleitung
Melden	Kunden über Lieferverzug, Polizei; BSI falls NIS2-pflichtig.	Geschäftsführung

3.6 B6 Ransomware aus der IT über MES ins Leitsystem

Schadsoftware von einem Büro-PC der Disposition breitet sich mit dem Domänenkonto der IT über SMB auf den MES-Server aus, verschlüsselt MES und Linienmanagement und greift von dort die Leitsystem-Server an. Risiko: **KRITISCH** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

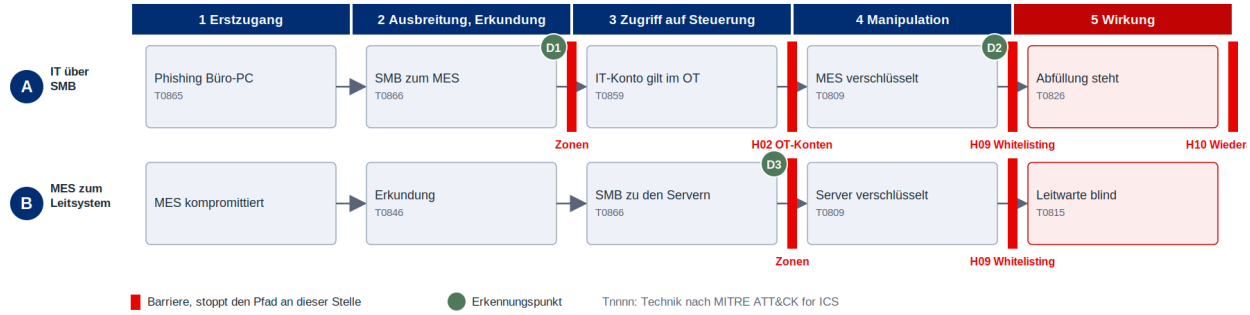


Abbildung: Angriffspfade B6

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	SMB aus der IT in Richtung OT	Firewall, OT-Monitoring
D2	MES meldet Dateifehler, viele Schreibzugriffe	OT-Monitoring, IT
D3	SMB vom MES zu den Leitsystem-Servern	Firewall, OT-Monitoring

PLAYBOOK PB-B6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, Erpresserhinweis	jeder
Sofort, 0 bis 15 min	Verbindungen IT zu OT an der Firewall sperren, MES und Linienmanagement vom Netz, Abfüllung geordnet stoppen.	IT-Leitung, Schichtführer
Eindämmen, bis 4 h	Konten zurücksetzen, betroffene Systeme identifizieren, Papierverfahren für die Rückverfolgung.	OT-Security, Qualitätssicherung
Beseitigen	Systeme aus Offline-Sicherung neu aufsetzen.	OT-Security, Dienstleister
Wiederherstellen	Leitsystem prüfen, MES und Linienmanagement schrittweise anfahren, Rückverfolgung nachtragen.	Betriebsleitung
Melden	BSI falls NIS2-pflichtig (24 h, 72 h, 1 Monat), Polizei, Versicherung, Kunden.	Geschäftsführung

4 Reaktionsplan

4.1 Grundsätze

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

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Sudhaus	laufenden Sud mit Bedienpanel vor Ort zu Ende fahren, keinen neuen Sud beginnen
Gär- und Lagerkeller	Temperaturregelung in der AS-30 mit letztem Sollwert, Tanktemperaturen von Hand prüfen
Kälte NH3	Kälte-SPS regelt eigenständig, Hochdruckbegrenzer und Gaswarnung hart verdrahtet
Abfüllung	Linie geordnet stoppen; ohne MES nur mit Papierprotokoll für die Rückverfolgung weiter
CIP	keine Reinigung parallel zur Abfüllung, Ventilknoten vor Ort prüfen
Alarmierung	Gaswarnanlagen NH3 und CO2 warnen unabhängig vom Leitsystem

4.3 Rollen

Rolle	Aufgabe	Besetzung
Schichtführer	erkennt, setzt Sofortmaßnahmen, alarmiert	[Name, Telefon]
Braumeister, Kellermeister	Produkt, Tanks, Freigaben	[Name, Telefon]
Betriebstechnik	Kälte, Kessel, Druckluft, Schaltanlagen	[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	Schichtführer mit OT-Security
2 Angriff bestätigt	keine Gefahr für Menschen oder Verbraucher	Betriebsleitung, Braumeister
3 Krise	NH3- oder CO2-Gefahr, Produkt mit Gesundheitsrisiko ausgeliefert, Abfüllung über Tage gestoppt	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, Brand	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 Leitwarte und bei Schichtführern
- Notbetriebshandbuch je Bereich, Papierprotokoll für Rückverfolgung
- Offline-Sicherung aller Steuerungen und Server, Wiederanlauf einmal im Jahr geübt
- Reaktionszeiten der Lieferanten von Kälte, Füller, Leitsystem und MES im Vertrag
- Planspiel zweimal im Jahr, eines mit Rückrufszenario

5 Nächste Schritte

- Rollen besetzen, Telefonliste erstellen.
- Playbooks mit Braumeister, Betriebstechnik und Qualitätssicherung abstimmen.
- Erstes Planspiel mit Szenario B3 (Lauge im Bier) und Rückruf.