BERICHT

Risikobewertung Cyberangriffe

Brauerei 120.000 hl/a, Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Brauerei, 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 und Wirtschaftlichkeit

5 Nächste Schritte

1 Management Summary

Für die fiktive Regionalbrauerei mit 120.000 hl/a wurden sechs Angriffe bewertet, die Menschen, Verbraucher und Betrieb am stärksten treffen: Manipulation der NH3-Kälteanlage, CO2 im Tankkeller, Lauge im Bier über den CIP-Ventilknoten, abgesenkte Pasteurisation, missbrauchte Fernwartung des Füllers und Ransomware aus der IT.

Ohne Härtung sind 4 Szenarien kritisch. Im typischen Planungsstand mit Zonenfirewall bleiben 1 kritisch und 3 mittel. Mikrosegmentierung senkt vor allem den Laptop am CIP-Switch und die Ausbreitung in der Flaschenlinie; mit allen Maßnahmen liegt kein Szenario über NIEDRIG.

GESAMTBEWERTUNG

Netzwerksegmentierung stoppt Angriffe, die einen Weg durchs Netz brauchen. Angriffe über den regulären Bedienweg stoppt sie nicht; dort wirken nur Maßnahmen im Prozess: Sollwertgrenzen in der SPS, Vier-Augen-Freigabe, Leitfähigkeitsüberwachung und autarke Sicherheitsfunktionen für NH3 und CO2.

SZENARIEN NACH RISIKOKLASSE

Klasse	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
KRITISCH	4	1	0	0
HOCH	1	0	0	0
MITTEL	1	3	3	0
NIEDRIG	0	2	3	6

2 Ausgangslage und Methode

Grundlage ist die Demonstrationsanlage im HTML-Leitstand (Brauerei_Leitstand_PurpleTeam.html) mit Simulation, SPS-Programmen, Netzwerkverkehr, Segmentierung und den Angriffsszenarien B1 bis B6. 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 mit Firewall, H02, H04, H07); Mikrosegmentierung (Planungsstand plus Mikrosegmentierung); 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	Fernwartung der Lieferanten nur über Jump-Host mit Freigabe je Sitzung, OEM-Router entfernt	fehlt
H02	Eigene Benutzerverwaltung im OT, keine Konten der IT-Domäne, Admin-Konten je Person	umgesetzt
H03	Zugriffsschutz der CPUs, PUT/GET aus, Know-how-Schutz	fehlt
H04	Sollwertgrenzen in der SPS: PE-Minimum KZE, Gärtemperatur, CIP-Konzentration	umgesetzt
H05	Verriegelung CIP gegen Produkt in der SPS und Leitfähigkeitsüberwachung der Produktleitung mit Umleitung	fehlt
H06	Engineering nur von der Engineering-Station, Anmeldung mit MFA	fehlt
H07	Sicherheitsfunktionen autark: NH3- und CO2-Gaswarnung, Druckbegrenzer, Kessel-Sicherheitskette hart verdrahtet	umgesetzt
H08	Rezept- und Sollwertfreigabe mit Vier-Augen-Prinzip und Signatur im Leitsystem	fehlt
H09	Härtung und Anwendungs-Whitelisting der Windows-Systeme	fehlt
H10	Offline-Sicherung, geübter Wiederanlauf, Handbetrieb Abfüllung beschrieben	fehlt
H11	OT-Monitoring mit Anomalieerkennung am Spiegelport	fehlt
H12	USB-Schleuse und Kontrolle von Wechseldatenträgern und Service-Laptops	fehlt
H13	Port Security und NAC an den Switches der Linien	fehlt
H14	Reaktionsplan, Schulung Schichtführer, Übung mit Rückrufszenario	fehlt
SEG	Segmentierung: Zonen mit Firewall, Mikrosegmente je Zelle und Maschine	Zonen umgesetzt, Mikro fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
B1	Kälteanlage NH3 über Fernwartung manipuliert	KRITISCH	MITTEL	MITTEL	NIEDRIG
B2	CO2-Warnung und Lüftung im Tankkeller abgeschaltet	KRITISCH	MITTEL	MITTEL	NIEDRIG
B3	Lauge im Bier über den CIP-Ventilknoten	KRITISCH	KRITISCH	MITTEL	NIEDRIG
B4	Pasteurisation am Kurzzeiterhitzer abgesenkt	HOCH	NIEDRIG	NIEDRIG	NIEDRIG
B5	Fernwartung des Füllers missbraucht, Linie steht	MITTEL	MITTEL	NIEDRIG	NIEDRIG
B6	Ransomware aus der IT über MES ins Leitsystem	KRITISCH	NIEDRIG	NIEDRIG	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in vier Ständen

3.2 Szenarien im Detail

3.2.1 B1 Kälteanlage NH3 über Fernwartung manipuliert

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Kälte-SPS und Bedienpanel (Z16), Fernwartungsrouter des Kälteanlagenbauers
Ort	Maschinenraum NH3, Verdunstungsverflüssiger, Glykolkreis
Angriffsweg	1. Zugangsdaten des Kälteanlagenbauers erbeutet (T0859) 2. Verbindung über den OEM-Router zur Kälte-SPS (T0822, T0886) 3. Lüfter aus, Verdichter Dauerbetrieb, Abschaltung in der SPS deaktiviert (T0836, T1692.001) 4. Hochdruck, Sicherheitsventil bläst NH3 ab (T0880, T0879)
Folgen	Hochdruck, Sicherheitsventil bläst NH3 über Dach ab, Personengefahr, Kälte fällt aus, Gärung läuft heiß.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
Mit Mikrosegmentierung	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H01
Restrisiko	Wer an der Steuerung vor Ort arbeitet, umgeht jede Netzmaßnahme. Hochdruckbegrenzer, Sicherheitsventile und NH3-Gaswarnung müssen unabhängig von der SPS wirken und wiederkehrend geprüft werden.
Schaden im Ernstfall	0,5 bis 5 Mio. €: Personenschaden bei NH3-Austritt, Evakuierung, Produktverlust durch warme Gärung, Stillstand der Kälte für Tage
Referenz	MITRE ATT&CK for ICS v20: T0859, T0822, T0886, T0836, T1692.001, T0880; IEC 62443-3-3 SR 1.13, SR 5.2; TRAS 110

3.2.2 B2 CO2-Warnung und Lüftung im Tankkeller abgeschaltet

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Bedienplätze und Leitsystem-Server (Z04), AS-30 Gär- und Lagerkeller (Z10)
Ort	Tankkeller-Bedienraum mit Ventilknoten
Angriffsweg	1. Konto eines Bedieners per Phishing übernommen oder Bedienplatz offen (T0859) 2. Bedienung über das Leitsystem, der Weg ist legitim (T1692.001) 3. Lüftung aus, CO2-Meldung unterdrückt, Ablassventil offen (T0836, T0878) 4. CO2 im Raum, Personen gefährdet (T0880)
Folgen	CO2 sammelt sich im Bedienraum, Erstickungsgefahr für das Personal am Ventilknoten.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
Mit Mikrosegmentierung	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H08
Restrisiko	Der reguläre Bedienweg muss erlaubt bleiben; Segmentierung hilft hier nicht. Die autarke CO2-Gaswarnung und Vier-Augen-Freigaben begrenzen die Wirkung.
Schaden im Ernstfall	Lebensgefahr für Personal; Betriebsunterbrechung, Ermittlungen, Haftung; finanziell 0,1 bis 1 Mio. €
Referenz	MITRE ATT&CK for ICS v20: T0859, T1692.001, T0836, T0878, T0880; IEC 62443-3-3 SR 2.1, SR 3.5

3.2.3 B3 Lauge im Bier über den CIP-Ventilknoten

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	AS-40 CIP (Z14), Ventilknoten VK-340, Produktleitung zur Abfüllung
Ort	CIP-Raum, Tankkeller-Bedienraum, Abfüllhalle
Angriffsweg	1. Laptop eines Dienstleisters mit Schadsoftware am CIP-Switch (T0847) 2. S7-Verbindung vom Laptop zur AS-40 (T1692.001) 3. Doppelsitzventil zur Produktleitung offen während Laugephase (T0836, T0831) 4. Lauge im Bier, Rückruf (T0880, T0828)
Folgen	Lauge gelangt in abgefülltes Bier, Verätzungsgefahr für Verbraucher, Rückruf aller Chargen.
Planungsstand	**KRITISCH** (A 5 × W 3 = 15); gelingt
Mit Mikrosegmentierung	**MITTEL** (A 5 × W 1 = 5); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H12, H13
Restrisiko	Der Doppelsitzventilknoten trennt nur, solange die Ventile richtig geschaltet sind. Leitfähigkeitsmessung vor dem Füller mit Umleitung ist die letzte Barriere.
Schaden im Ernstfall	1 bis 10 Mio. €: öffentlicher Rückruf, Gesundheitsgefahr für Verbraucher, Haftung, Markenschaden
Referenz	MITRE ATT&CK for ICS v20: T0847, T1692.001, T0836, T0831, T0880, T0828; IEC 62443-3-3 SR 2.3, SR 3.5, SR 5.1; VO (EG) 852/2004 HACCP

3.2.4 B4 Pasteurisation am Kurzzeiterhitzer abgesenkt

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Bedienplätze, Leitsystem-Server (Z04), AS-60 Kurzzeiterhitzer (Z12)
Ort	Abfüllhalle, KZE-540
Angriffsweg	1. Konto eines Bedieners der Abfüllung übernommen (T0859) 2. Rezeptänderung über das Leitsystem (T1692.001) 3. PE-Sollwert 5, Umleitung aus (T0836) 4. Unterpasteurisiertes Bier ausgeliefert (T0828)
Folgen	Unterpasteurisiertes Bier wird ausgeliefert, mikrobiologisch instabil, Rückruf.
Planungsstand	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H04
Mit Mikrosegmentierung	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H04
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H08, H04
Restrisiko	Grenzen in der SPS halten auch bei Fehlbedienung. Die PE-Aufzeichnung muss täglich ausgewertet und vor Auslieferung freigegeben werden.
Schaden im Ernstfall	0,5 bis 5 Mio. €: Rückruf mikrobiologisch instabiler Ware, Reklamationen, Markenschaden
Referenz	MITRE ATT&CK for ICS v20: T0859, T1692.001, T0836, T0828; IEC 62443-3-3 SR 2.1, SR 3.5

3.2.5 B5 Fernwartung des Füllers missbraucht, Linie steht

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Füller (OEM, Z12), Jump-Host (Z03), Etikettierer
Ort	Abfüllhalle, Flaschenlinie
Angriffsweg	1. Zugangsdaten des Füller-Herstellers erbeutet (T0859) 2. Sitzung über den Jump-Host zum Füller (T0822) 3. Rezepte und Antriebsparameter im Füller geändert (T0836, T0889) 4. Vom Füller zum Etikettierer (T0866) 5. Linie steht (T0828)
Folgen	Flaschenlinie steht, Lieferausfall über Tage, Neuinbetriebnahme durch den Hersteller.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt
Mit Mikrosegmentierung	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 4 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H01
Restrisiko	Der Hersteller braucht Fernzugriff. Freigabe je Sitzung, Aufzeichnung und Mikrosegmentierung der Linie begrenzen, was ein missbrauchter Zugang erreicht.
Schaden im Ernstfall	0,2 bis 2 Mio. €: Lieferausfall über Tage, Vertragsstrafen, Neuinbetriebnahme durch den Hersteller
Referenz	MITRE ATT&CK for ICS v20: T0859, T0822, T0836, T0889, T0866, T0828; IEC 62443-3-3 SR 1.13, SR 5.1; IEC 62443-2-4

3.2.6 B6 Ransomware aus der IT über MES ins Leitsystem

Ohne Härtung	**KRITISCH** (A 4 × W 4 = 16)
Betroffene Systeme	Büro-IT (Z01), MES und Linienmanagement (Z07), Leitsystem (Z04)
Ort	Serverraum, Leitwarte, Abfüllung
Angriffsweg	1. Phishing auf Büro-PC der Disposition (T0865) 2. SMB vom Büro-PC zum MES (T0866) 3. Domänenkonto der IT gilt im OT (T0859) 4. MES und Linienmanagement verschlüsselt (T0809) 5. Vom MES zu den Leitsystem-Servern (T0866) 6. Abfüllung steht, Rückverfolgung blind (T0826, T0815)
Folgen	Abfüllung ohne Chargenfreigabe gestoppt, Rückverfolgung blind, im schlimmsten Fall Leitwarte ohne Bild.
Planungsstand	**NIEDRIG** (A 4 × W 1 = 4); gestoppt in Schritt 2 durch Zonen
Mit Mikrosegmentierung	**NIEDRIG** (A 4 × W 1 = 4); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 2 durch Mikrosegmentierung
Restrisiko	Ransomware kommt auch über Wechseldatenträger oder Lieferanten. Offline-Sicherung, geübter Wiederanlauf und ein Papierverfahren für die Rückverfolgung begrenzen die Dauer.
Schaden im Ernstfall	0,5 bis 3 Mio. €: Abfüllung über Tage gestoppt, Rückverfolgung nachzutragen, Wiederherstellung, Meldepflichten
Referenz	MITRE ATT&CK for ICS v20: T0865, T0866, T0859, T0809, T0826, T0815; IEC 62443-3-3 SR 1.1, SR 3.2, SR 5.2, SR 7.3, SR 7.4

4 Maßnahmen und Wirtschaftlichkeit

Bezug zeigt, in welchen Szenarien die Maßnahme einen Schritt stoppt oder die Wirkung begrenzt. Kosten sind Erfahrungswerte; Angebote einholen.

Nr.	Maßnahme	Bezug	Priorität	Kosten
H01	Fernwartung der Lieferanten nur über Jump-Host mit Freigabe je Sitzung, OEM-Router entfernt	B1, B5	Hoch	10.000 bis 30.000 €
H02	Eigene Benutzerverwaltung im OT, keine Konten der IT-Domäne, Admin-Konten je Person	B6	umgesetzt	15.000 bis 40.000 €
H03	Zugriffsschutz der CPUs, PUT/GET aus, Know-how-Schutz	B1, B3, B5	Mittel	2.000 bis 5.000 €
H04	Sollwertgrenzen in der SPS: PE-Minimum KZE, Gärtemperatur, CIP-Konzentration	B4	umgesetzt	3.000 bis 8.000 €
H05	Verriegelung CIP gegen Produkt in der SPS und Leitfähigkeitsüberwachung der Produktleitung mit Umleitung	B3	Hoch	15.000 bis 40.000 €
H06	Engineering nur von der Engineering-Station, Anmeldung mit MFA	alle	Mittel	5.000 bis 15.000 €
H07	Sicherheitsfunktionen autark: NH3- und CO2-Gaswarnung, Druckbegrenzer, Kessel-Sicherheitskette hart verdrahtet	B1, B2	umgesetzt	20.000 bis 60.000 €
H08	Rezept- und Sollwertfreigabe mit Vier-Augen-Prinzip und Signatur im Leitsystem	B2, B4	Hoch	5.000 bis 15.000 €
H09	Härtung und Anwendungs-Whitelisting der Windows-Systeme	B6	Mittel	5.000 bis 15.000 €
H10	Offline-Sicherung, geübter Wiederanlauf, Handbetrieb Abfüllung beschrieben	B5, B6	Mittel	10.000 bis 30.000 €
H11	OT-Monitoring mit Anomalieerkennung am Spiegelport	alle	Mittel	30.000 bis 80.000 € je Jahr
H12	USB-Schleuse und Kontrolle von Wechseldatenträgern und Service-Laptops	B3	Mittel	3.000 bis 10.000 €
H13	Port Security und NAC an den Switches der Linien	B3	Hoch	5.000 bis 20.000 €
H14	Reaktionsplan, Schulung Schichtführer, Übung mit Rückrufszenario	alle	Mittel	5.000 bis 15.000 € je Jahr
SEG	Mikrosegmentierung je Zelle und Maschine	B3, B5, B6	Hoch	30.000 bis 90.000 €

Tabelle 2: Maßnahmen, Priorität im Planungsstand, geschätzte Kosten

Die fehlenden Maßnahmen mit Priorität Hoch kosten zusammen grob 100.000 bis 250.000 € einmalig. Ein einziger öffentlicher Rückruf (B3, B4) oder ein NH3-Austritt mit Verletzten (B1) liegt im Bereich von 1 bis 10 Mio. € und kann Menschen gefährden.

4.1 Rechtlicher Rahmen

- **NIS2:** Das BSIG in der NIS2-Fassung gilt seit 06.12.2025. Lebensmittel (Herstellung, Verarbeitung, Vertrieb) ist ein Sektor nach Anlage 2. Eine Brauerei dieser Größe ist ab 50 Beschäftigten oder mehr als 10 Mio. € Umsatz und Bilanzsumme in der Regel wichtige Einrichtung (§ 28 BSIG). Für den konkreten Betreiber zu prüfen.
- **Immissionsschutz:** Brauerei ab 200 hl Bier je Tag (Vierteljahresdurchschnitt) genehmigungsbedürftig nach 4. BImSchV Anhang 1 Nr. 7.27.2; NH3-Kälteanlage ab 3 t Füllmenge nach Nr. 10.25 mit TRAS 110; Störfall-Mengenschwelle Ammoniak 50 t, hier nicht erreicht.
- **Lebensmittelrecht:** Rückverfolgbarkeit und Rücknahme nach VO (EG) 178/2002 Art. 18 und 19, HACCP nach VO (EG) 852/2004. Ein Cyberangriff auf Pasteurisation oder CIP ist ein Lebensmittelsicherheitsrisiko.
- **Arbeitsschutz:** NH3 und CO2 nach BetrSichV und GefStoffV; CO2-Arbeitsplatzgrenzwert 0,5 Vol.-% (TRGS 900). Die Wirkung von Cyberangriffen gehört in die Gefährdungsbeurteilung.
- **Maschinenverordnung (EU) 2023/1230:** ab 20.01.2027 für neue Maschinen der Linie, Anhang III Nr. 1.1.9 Schutz gegen Korrumpierung.

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

- OEM-Router der Kälteanlage entfernen, Fernwartung über Jump-Host (H01).
- Verriegelung CIP gegen Produkt und Leitfähigkeit vor dem Füller (H05), Vier-Augen-Freigabe für Rezepte und Grenzwerte (H08).
- Mikrosegmentierung der Flaschenlinie und der CIP-Zelle planen.
- Reaktionsplan mit Rückrufszenario üben.