BERICHT

Risikobewertung Cyberangriffe

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Klinikum, 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 das fiktive Klinikum mit 650 Betten wurden sechs Angriffe auf die technische Gebäudeausrüstung bewertet: OP-Lüftung über die Schnittstelle zur OP-Planung, Probelauf des Netzersatzes mit Last, Ladepunkte im Parkhaus, Trinkwassertemperatur, Rohrpost über die Herstellerfernwartung und Ransomware im Vision Center.

Ohne Härtung sind 1 Szenarien kritisch. Im Planungsstand sind 1 hoch und 2 mittel. Am schwersten wiegt die Abschaltung der OP-Lüftung über die Schnittstelle zur OP-Planung: Sie nutzt einen gewollten Weg aus der IT, und keine Segmentierung hält sie auf. Nur Plausibilisierung in der Schnittstelle und die Bedienung im Saal schützen die Patienten.

GESAMTBEWERTUNG

Brandfallsteuerung, Netzersatzstart, Druckregelung der medizinischen Gase und CO-Lüftung arbeiten eigenständig. Gefährdet sind die Funktionen, die über die Gebäudeleittechnik laufen: OP-Lüftung, Trinkwasser und die Alarmierung der Leitwarte.

SZENARIEN NACH RISIKOKLASSE

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

2 Ausgangslage und Methode

Grundlage sind die Anlagenschemata KL-TS-001, das Kommunikations- und Sicherheitskonzept und der HTML-Leitstand (Klinikum_Leitstand_PurpleTeam.html) mit Simulation, Netzwerkverkehr, Segmentierung und den Szenarien K1 bis K6. 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; LTE-Zugänge der Dienstleister vorhanden); Mikrosegmentierung (Planungsstand plus Segmente je Gewerk); 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	LTE-Zugänge der Dienstleister (O2-Telemetrie, Aufzugsnotruf) ohne Verbindung ins OT-Netz; Fernwartung nur über SINEMA RC mit Freigabe je Sitzung	fehlt
H02	Eigene Benutzerverwaltung im OT mit MFA; keine IT-Konten auf Jump-Host, Vision Center und Leitwarte	fehlt
H03	BACnet absichern: nur das Vision Center darf schreiben, Schreibschutz für Sollwerte in den Automationsstationen, BACnet/SC prüfen	fehlt
H04	Plausibilisierung der KIS-Schnittstelle: belegte OP-Säle werden nie aus der Ferne abgeschaltet; Betriebsart nur mit Bestätigung im Saal	fehlt
H05	Feste Grenzen in Automationsstationen und SPS: Mindestvolumenstrom OP, Trinkwasser ≥ 55 °C, Probelauf Netzersatz nur mit Freigabe	umgesetzt
H06	Engineering nur von den Engineering-Stationen, Änderungen mit Versionsverwaltung und Vier-Augen-Freigabe	fehlt
H07	Sicherheitsfunktionen eigenständig: Brandfallsteuerung der BMZ, Netzersatzstart, Druckregelung medizinische Gase, CO-Lüftung	umgesetzt
H08	Notbedienung vor Ort: Handebene an den Automationsstationen, Bedienung im OP-Saal, Rohrpost-Notbetrieb mit Boten, Schranken offen	fehlt
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Vision Center, Rohrpostzentrale, Parkhaus und Leitwarte	fehlt
H10	Offline-Sicherung von GLT-Projekten, SPS-Programmen und Konfigurationen; geübter Wiederanlauf	umgesetzt
H11	OT-Monitoring mit Auswertung von BACnet, Modbus, OCPP und S7	fehlt
H12	OCPP mit TLS und Zertifikaten je Ladepunkt, feste Leistungsgrenze am Netzanschluss des Parkhauses	fehlt

Nr.	Maßnahme	Planungsstand
H13	Port Security und NAC; Netzwerkdosen in öffentlichen Bereichen (Parkhaus, Flure) gesperrt	fehlt
H14	Reaktionsplan mit Krisenstab, Medizin und Feuerwehr, Übung einmal im Jahr	fehlt
SEG	Zonen mit Firewall und Zellenfirewalls, Mikrosegmente	Zonen ja, Mikro fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
K1	OP-Lüftung über die Schnittstelle zur OP-Planung abgeschaltet	KRITISCH	KRITISCH	KRITISCH	NIEDRIG
K2	Probelauf des Netzersatzes mit Last während laufender OPs	MITTEL	NIEDRIG	NIEDRIG	NIEDRIG
K3	Ladepunkte im Parkhaus über das Betreiber-Backend	MITTEL	MITTEL	MITTEL	NIEDRIG
K4	Trinkwassertemperatur über einen Service-Laptop abgesenkt	MITTEL	NIEDRIG	NIEDRIG	NIEDRIG
K5	Rohrpostzentrale über die Herstellerfernwartung verschlüsselt	HOCH	HOCH	HOCH	NIEDRIG
K6	Ransomware im Vision Center: Leitwarte blind	HOCH	MITTEL	MITTEL	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in vier Ständen

3.2 Szenarien im Detail

3.2.1 K1 OP-Lüftung über die Schnittstelle zur OP-Planung abgeschaltet

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	OP-Planung (Z01), KIS-Schnittstelle (Z03), Vision Center (Z04), AS-01 bis 03 (Z07)
Ort	OP-Trakt
Angriffsweg	1. OP-Planungsserver in der IT übernommen (T0817, T0866) 2. Manipulierte Betriebsarten an die Schnittstelle (T0843) 3. Vision Center schaltet die Säle ab (T1692.001) 4. Belegte Säle ohne Lüftung (T0879, T0826)
Folgen	Belegte OP-Säle verlieren Druckhaltung und Reinluft; laufende Eingriffe müssen beendet werden, geplante OPs entfallen, Infektionsrisiko.
Planungsstand	**KRITISCH** (A 5 × W 3 = 15); gelingt
Mit Mikrosegmentierung	**KRITISCH** (A 5 × W 3 = 15); gelingt
Vollständig	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 3 durch H04
Restrisiko	Die Schnittstelle ist gewollt; nur Plausibilisierung und Bedienung im Saal halten sie sicher.
Schaden im Ernstfall	0,5 bis 5 Mio. €: abgesagte OPs, Infektionen, Haftung
Referenz	MITRE ATT&CK for ICS v20: T0817, T0866, T0843, T1692.001, T0879, T0826; DIN 1946-4; IEC 62443-3-3 SR 3.5

3.2.2 K2 Probelauf des Netzersatzes mit Last während laufender OPs

Ohne Härtung	**MITTEL** (A 4 × W 2 = 8)
Betroffene Systeme	Jump-Host (Z03), Energiemanagement (Z04), AS-NEA (Z08)
Ort	Energiezentrale
Angriffsweg	1. Admin-Daten erbeutet (T0859) 2. RDP vom Jump-Host zum Energiemanagement (T0886) 3. Probelauf mit Last per OPC UA (T1692.001) 4. Unterbrechung der Sicherheitsversorgung (T0813)
Folgen	Kurze Unterbrechung aller nicht USV-gestützten Verbraucher der Sicherheitsversorgung: OP-Lüftung, Beleuchtung, Aufzüge; Geräte starten neu.
Planungsstand	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 3 durch H05
Mit Mikrosegmentierung	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 3 durch H05
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02
Restrisiko	Der Probelauf ist gewollt; die Sperre bei OP-Betrieb in der SPS hält ihn auf.
Schaden im Ernstfall	0,1 bis 1 Mio. €, Gefährdung bei laufenden Eingriffen
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T1692.001, T0813; DIN VDE 0100-710; IEC 62443-3-3 SR 3.5

3.2.3 K3 Ladepunkte im Parkhaus über das Betreiber-Backend

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Backend Ladepunktbetreiber (Z02), Lastmanagement und Ladepunkte (Z12)
Ort	Parkhaus
Angriffsweg	1. Backend des Ladepunktbetreibers kompromittiert (T0862) 2. Befehle über die bestehende OCPP-Verbindung (T0886) 3. Alle Ladepunkte auf Höchstleistung (T0831) 4. Einspeisung löst aus, Lüftung aus (T0813, T0879)
Folgen	Parkhaus stromlos: Schranken, Kassen, Beleuchtung, CO-Lüftung aus; Gefahr durch Abgase, Rettungswege dunkel.
Planungsstand	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H07
Mit Mikrosegmentierung	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H07
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H12
Restrisiko	Der Betreiber sitzt außerhalb; lokale Leistungsgrenze und CO-Lüftung an der Sicherheitsversorgung sind die Barrieren.
Schaden im Ernstfall	0,05 bis 0,5 Mio. €, Gefahr durch Abgase
Referenz	MITRE ATT&CK for ICS v20: T0862, T0886, T0831, T0813, T0879; OCPP 1.6J Security Whitepaper

3.2.4 K4 Trinkwassertemperatur über einen Service-Laptop abgesenkt

Ohne Härtung	**MITTEL** (A 4 × W 2 = 8)
Betroffene Systeme	Service-Laptop (Z18), AS-13 Trinkwasser (Z07)
Ort	Energiezentrale
Angriffsweg	1. Infizierter Service-Laptop angeschlossen (T0847) 2. BACnet zur Automationsstation AS-13 (T0886) 3. Sollwert auf 42 °C (T0836) 4. Trinkwasser über Tage zu kalt (T0879)
Folgen	Legionellenwachstum im Warmwassernetz über Tage; Duschverbote, Gefahr für immungeschwächte Patienten.
Planungsstand	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 2 durch Zonen
Mit Mikrosegmentierung	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H13
Restrisiko	Mindesttemperatur fest in der AS und Port Security halten den Angriff auf.
Schaden im Ernstfall	0,1 bis 1 Mio. €: Desinfektion, Duschverbote, Gesundheitsgefahr
Referenz	MITRE ATT&CK for ICS v20: T0847, T0886, T0836, T0879; DVGW W 551; IEC 62443-3-3 SR 1.2

3.2.5 K5 Rohrpostzentrale über die Herstellerfernwartung verschlüsselt

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Fernwartung Hersteller (Z02), SINEMA RC (Z03), Rohrpostzentrale (Z11)
Ort	Haupthaus
Angriffsweg	1. Zugang beim Rohrpostthersteller missbraucht (T0866) 2. VPN über SINEMA RC ohne Freigabe der Sitzung (T0822) 3. RDP zur Rohrpostzentrale, Verschlüsselung (T0886, T0809) 4. Rohrpost steht, Notaufnahme abgemeldet (T0828)
Folgen	Laborproben und Blutkonserven bleiben liegen; Befunde verzögern sich, die Notaufnahme meldet sich ab.
Planungsstand	**HOCH** (A 4 × W 3 = 12); gelingt
Mit Mikrosegmentierung	**HOCH** (A 4 × W 3 = 12); gelingt
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 2 durch H01
Restrisiko	Hersteller brauchen Fernzugang; Freigabe je Sitzung und Botendienst begrenzen den Schaden.
Schaden im Ernstfall	0,2 bis 1 Mio. €, Verzögerung von Befunden
Referenz	MITRE ATT&CK for ICS v20: T0866, T0822, T0886, T0809, T0828; IEC 62443-2-4

3.2.6 K6 Ransomware im Vision Center: Leitwarte blind

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Jump-Host (Z03), Vision Center (Z04)
Ort	Serverraum, Leitwarte
Angriffsweg	1. Admin-Daten aus der IT gestohlen (T0859) 2. RDP vom Jump-Host zum Vision Center (T0886) 3. Server verschlüsselt (T0809) 4. Leitwarte ohne Anzeige (T0815)
Folgen	Störungen bei OP-Lüftung, medizinischen Gasen oder Kälte bleiben unbemerkt, bis Stationen anrufen.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H10
Mit Mikrosegmentierung	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H10
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02
Restrisiko	Automationsstationen regeln weiter; Rundgänge und Alarmzentralen vor Ort ersetzen die Leitwarte.
Schaden im Ernstfall	0,3 bis 2 Mio. €: Wiederherstellung, Personal für Rundgänge
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0815; 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	LTE-Zugänge der Dienstleister (O2-Telemetrie, Aufzugsnotruf) ohne Verbindung ins OT-Netz; Fernwartung nur über SINEMA RC mit Freigabe je Sitzung	K5	**Hoch**
H02	Eigene Benutzerverwaltung im OT mit MFA; keine IT-Konten auf Jump-Host, Vision Center und Leitwarte	K2, K6	**Hoch**
H03	BACnet absichern: nur das Vision Center darf schreiben, Schreibschutz für Sollwerte in den Automationsstationen, BACnet/SC prüfen	K4	**Mittel**
H04	Plausibilisierung der KIS-Schnittstelle: belegte OP-Säle werden nie aus der Ferne abgeschaltet; Betriebsart nur mit Bestätigung im Saal	K1	**Hoch**
H05	Feste Grenzen in Automationsstationen und SPS: Mindestvolumenstrom OP, Trinkwasser ≥ 55 °C, Probelauf Netzersatz nur mit Freigabe	K2, K4	umgesetzt
H06	Engineering nur von den Engineering-Stationen, Änderungen mit Versionsverwaltung und Vier-Augen-Freigabe	alle	**Mittel**
H07	Sicherheitsfunktionen eigenständig: Brandfallsteuerung der BMZ, Netzersatzstart, Druckregelung medizinische Gase, CO-Lüftung	K2, K3	umgesetzt
H08	Notbedienung vor Ort: Handebene an den Automationsstationen, Bedienung im OP-Saal, Rohrpost-Notbetrieb mit Boten, Schranken offen	K1, K5	**Hoch**
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Vision Center, Rohrpostzentrale, Parkhaus und Leitwarte	K5, K6	**Mittel**
H10	Offline-Sicherung von GLT-Projekten, SPS-Programmen und Konfigurationen; geübter Wiederanlauf	K6	umgesetzt
H11	OT-Monitoring mit Auswertung von BACnet, Modbus, OCPP und S7	alle	**Mittel**
H12	OCPP mit TLS und Zertifikaten je Ladepunkt, feste Leistungsgrenze am Netzanschluss des Parkhauses	K3	**Mittel**
H13	Port Security und NAC; Netzwerkdosen in öffentlichen Bereichen (Parkhaus, Flure) gesperrt	K4	**Hoch**
H14	Reaktionsplan mit Krisenstab, Medizin und Feuerwehr, Übung einmal im Jahr	alle	**Mittel**
SEG	Mikrosegmente: nur das Vision Center schreibt, Messgeräte und Alarmzentralen lesend	K4	**Mittel**

Tabelle 2: Maßnahmen und Priorität im Planungsstand

Abgesagte OPs und eine abgemeldete Notaufnahme (K1, K5) treffen Patienten unmittelbar. Die Maßnahmen mit Priorität Hoch sind dagegen überschaubar und teils rein organisatorisch.

4.1 Rechtlicher Rahmen

- **Kritische Anlage:** Mit über 30.000 vollstationären Fällen je Jahr ist das Klinikum kritische Anlage nach Anhang 5 BSI-KritisV und damit besonders wichtige Einrichtung: Risikomanagement nach § 30, Meldepflichten nach § 32, Nachweise alle drei Jahre nach § 39 BSIG.
- **§ 391 SGB V:** verpflichtet jedes Krankenhaus zu angemessenen Vorkehrungen nach dem Stand der Technik; der branchenspezifische Sicherheitsstandard (B3S) medizinische Versorgung beschreibt sie.
- **Meldungen:** erhebliche Sicherheitsvorfälle an die gemeinsame Meldestelle von BSI und BBK: Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h, Abschlussmeldung einen Monat danach.
- **Technik:** DIN 1946-4 (Raumlufttechnik im Gesundheitswesen), DIN VDE 0100-710 (medizinisch genutzte Bereiche), DIN EN ISO 7396-1 (medizinische Gase), DIN 14675 (Brandmeldeanlagen), DVGW W 551 (Trinkwasser).

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

- Plausibilisierung der Schnittstelle zur OP-Planung, Bedienung im Saal (H04, H08).
- Fernwartung nur mit Freigabe je Sitzung, LTE-Zugänge trennen (H01).
- Notbedienung vor Ort üben: Handebene, Botendienst, Rundgänge (H08).
- Planspiel mit Krisenstab, OP-Koordination und Notaufnahme (H14).