BERICHT

Angriffspfade und Reaktionsplan

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Klinikum, 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: Patienten vor Gebäude, und die Medizin entscheidet mit. Die Reaktion setzt in der Leitwarte und vor Ort an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Die Klinik bleibt versorgt, wenn jede Anlage vor Ort bedient werden kann und die Leitwarte weiß, wen sie in der Medizin sofort anruft. Notbedienkarten an jeder Automationsstation sind dafür Pflicht.

ID	Szenario	Erster Erkennungspunkt	Playbook
K1	OP-Lüftung über die Schnittstelle zur OP-Planung abgeschaltet	Viele Betriebsartwechsel in kurzer Zeit	PB-K1
K2	Probelauf des Netzersatzes mit Last während laufender OPs	OPC-UA-Schreibzugriff außerhalb des Plans	PB-K2
K3	Ladepunkte im Parkhaus über das Betreiber-Backend	Ladeprofile für alle Ladepunkte gleichzeitig	PB-K3
K4	Trinkwassertemperatur über einen Service-Laptop abgesenkt	Neues Gerät am Switch	PB-K4
K5	Rohrpostzentrale über die Herstellerfernwartung verschlüsselt	RDP ohne Wartungsauftrag	PB-K5
K6	Ransomware im Vision Center: Leitwarte blind	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 OP-Lüftung über die Schnittstelle zur OP-Planung abgeschaltet

Ein Angreifer übernimmt den Server der OP-Planung in der IT. Über die reguläre Schnittstelle schickt er für alle Säle die Betriebsart Aus; das Vision Center übernimmt sie, auch für belegte Säle. Risiko: **KRITISCH** ohne Härtung, **KRITISCH** im Planungsstand, **KRITISCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.

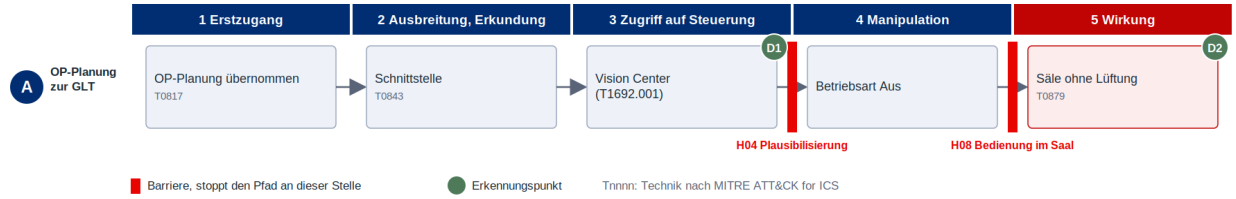


Abbildung: Angriffspfade K1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Viele Betriebsartwechsel in kurzer Zeit	OT-Monitoring, Vision Center
D2	Druckhaltung im belegten Saal verloren	Leitwarte, OP-Personal

PLAYBOOK PB-K1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	RLT-OP1 bis 3 auf Hand, Betriebsart OP vor Ort, Schnittstelle zur OP-Planung trennen.	Leitwarte Technik
Eindämmen	OP-Planungsserver isolieren, Konten sperren.	OT-Security
Melden	BSI (§ 32 BSIG, kritische Anlage), Krisenstab, Hygiene.	Krankenhausleitung
Wiederherstellen	Plausibilisierung in der Schnittstelle, Bestätigung im Saal.	Technische Leitung, Hersteller

3.2 K2 Probelauf des Netzersatzes mit Last während laufender OPs

Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host auf das Energiemanagement und fordert per OPC UA einen Probelauf mit Lastumschaltung an. Die Sicherheitsversorgung wird kurz unterbrochen. Risiko: **MITTEL** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.

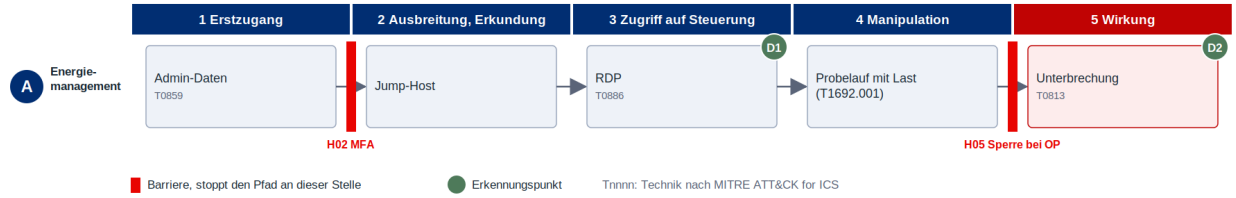


Abbildung: Angriffspfade K2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	OPC-UA-Schreibzugriff außerhalb des Plans	OT-Monitoring
D2	Netzersatz läuft ohne Plan	Leitwarte

PLAYBOOK PB-K2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Probelauf abbrechen, Netzersatz in Automatik nur für Netzausfall.	Leitwarte Technik
Eindämmen	Zugang zum Energiemanagement sperren.	OT-Security
Melden	BSI (§ 32 BSIG), Krisenstab.	Krankenhausleitung
Wiederherstellen	Freigabe für Probeläufe nur mit Schlüsselschalter.	Technische Leitung, Hersteller

3.3 K3 Ladepunkte im Parkhaus über das Betreiber-Backend

Das Backend des Ladepunktbetreibers wird kompromittiert. Über die bestehende OCPP-Verbindung setzt der Angreifer alle Ladeprofile auf Höchstleistung; die Einspeisung des Parkhauses löst aus. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade K3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Ladeprofile für alle Ladepunkte gleichzeitig	OT-Monitoring
D2	Einspeisung Parkhaus aus	Leitwarte

PLAYBOOK PB-K3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Ladepunkte aus, Einspeisung wieder einschalten, Schranken öffnen.	Leitwarte Technik
Eindämmen	OCPP-Verbindung zum Betreiber trennen.	OT-Security
Melden	BSI bei erheblicher Wirkung, Betreiber.	Krankenhausleitung
Wiederherstellen	Leistungsgrenze lokal, CO-Lüftung an der Sicherheitsversorgung.	Technische Leitung, Hersteller

3.4 K4 Trinkwassertemperatur über einen Service-Laptop abgesenkt

Ein infizierter Service-Laptop wird in der Energiezentrale angeschlossen. Die Schadsoftware schreibt per BACnet den Sollwert der Trinkwassererwärmung auf 42 °C. Risiko: **MITTEL** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade K4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Neues Gerät am Switch	Switch, Monitoring
D2	Trinkwasser unter 55 °C	Leitwarte

PLAYBOOK PB-K4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Sollwert 60 °C, Laptop vom Netz.	Leitwarte Technik
Eindämmen	Port sperren, weitere Geräte prüfen.	OT-Security
Melden	BSI, Gesundheitsamt bei Grenzwertüberschreitung.	Krankenhausleitung
Wiederherstellen	Schreibschutz in den AS, Mindesttemperatur fest.	Technische Leitung, Hersteller

3.5 K5 Rohrpostzentrale über die Herstellerfernwartung verschlüsselt

Der Fernwartungszugang des Rohrpostherstellers wird missbraucht. Über SINEMA RC und RDP gelangt der Angreifer auf die Rohrpostzentrale mit Windows 7 und verschlüsselt sie. Die Rohrpost steht. Risiko: **HOCH** ohne Härtung, **HOCH** im Planungsstand, **HOCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade K5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP ohne Wartungsauftrag	OT-Monitoring
D2	Rohrpost meldet Stillstand	Leitwarte, Labor

PLAYBOOK PB-K5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Botendienst für Labor und Blutkonserven, Fernzugang sperren.	Leitwarte Technik
Eindämmen	Rohrpostzentrale vom Netz.	OT-Security
Melden	BSI (§ 32 BSIG), Rettungsleitstelle bei Abmeldung.	Krankenhausleitung
Wiederherstellen	Zentrale neu aufsetzen mit Hersteller, Windows-Stand anheben.	Technische Leitung, Hersteller

3.6 K6 Ransomware im Vision Center: Leitwarte blind

Ransomware aus der IT scheitert am direkten Weg. Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host auf beide Vision-Center-Server und verschlüsselt sie. Die Automationsstationen regeln weiter, aber Alarme erreichen niemanden. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

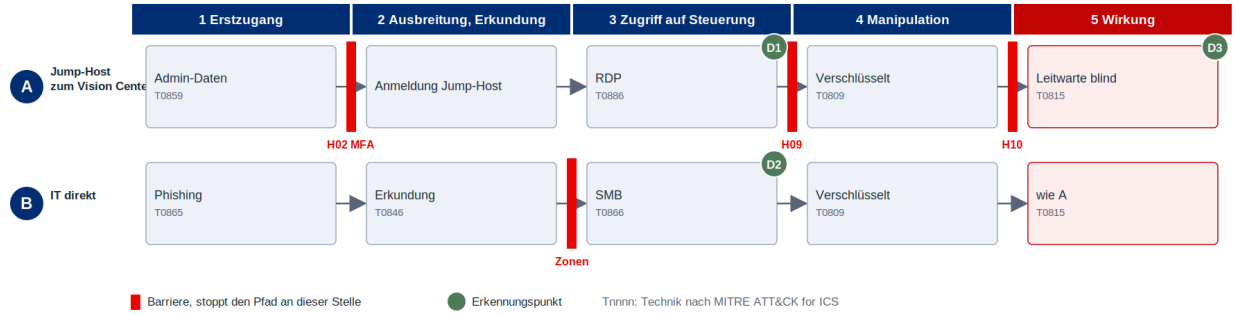


Abbildung: Angriffspfade K6

ERKENNUNGSPUNKTE

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

PLAYBOOK PB-K6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Rundgänge an OP-Trakt, med. Gasen und Kälte, Stationen informieren.	Leitwarte Technik
Eindämmen	Jump-Host und IT-Verbindung trennen.	OT-Security
Melden	BSI (24 h, 72 h, 1 Monat), Krisenstab, Polizei.	Krankenhausleitung
Wiederherstellen	Vision Center aus Offline-Sicherung.	Technische Leitung, Hersteller

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Patienten, Personal, Versorgung, Gebäude.
- **Medizin sofort einbinden:** OP-Koordination, Intensiv, Notaufnahme entscheiden über Verschiebung und Abmeldung.
- **Vor Ort bedienen:** Handebene an den Automationsstationen, Bedienung im Saal.
- **Feuerwehr und Brandschutz nie blockieren:** Brandmeldeanlage bleibt führend.
- **Alles mit Uhrzeit festhalten:** Protokolle der GLT und der Firewall sind Beweismittel.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
OP-Lüftung	Betriebsart im Saal, Handebene an AS-01 bis 03, Druckhaltung messen
Energie	Netzersatz startet selbst; Probeläufe aussetzen
Medizinische Gase	Alarmzentralen vor Ort beobachten, Reserve-Bündel bereit
Rohrpost	Botendienst für Labor und Blutkonserven
Parkhaus	Schranken offen, Ladepunkte aus

4.3 Rollen

Rolle	Aufgabe	Besetzung
Leitwarte Technik	erkennt, setzt Sofortmaßnahmen, alarmiert	[Name, Telefon]
Technischer Leiter	Technik, Notbetrieb, Hersteller	[Name, Telefon]
OP-Koordination, Intensiv, Notaufnahme	medizinische Entscheidungen	[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	Leitwarte Technik mit OT-Security
2 Angriff bestätigt	Gebäudetechnik gestört, Versorgung läuft	Technischer Leiter, OP-Koordination

Stufe	Merkmal	Entscheidet
3 Krise	OPs abgesagt, Notaufnahme abgemeldet, Gefahr für Patienten	Krankenhausleitung, Krisenstab

4.5 Meldungen

Anlass	Stelle	Frist
erheblicher Sicherheitsvorfall (§ 32 BSIG, kritische Anlage)	gemeinsame Meldestelle BSI und BBK	Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h, Abschlussmeldung einen Monat nach der 72-h-Meldung
Abmeldung der Notaufnahme, Verlegungen	Rettungsleitstelle, Gesundheitsamt	sofort
Datenschutzverletzung	Landesdatenschutzbehörde (Art. 33 DSGVO)	binnen 72 h
Straftat	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarmliste mit GLT-Errichter, BMA-Errichter, Rohrpostherstellers, Gaselieferant
- Offline-Sicherung der GLT- und SPS-Projekte
- Notbedienkarten an jeder Automationsstation
- Kontaktliste OP-Koordination, Intensiv, Notaufnahme, Rettungsleitstelle
- Planspiel einmal im Jahr mit Krisenstab

5 Nächste Schritte

- Rollen besetzen, Telefonliste mit Medizin und Herstellern.
- Playbooks mit Technik, Medizin und Hygiene abstimmen.
- Erstes Planspiel mit Szenario K1 und OP-Koordination.