BERICHT

Angriffspfade und Reaktionsplan

Kläranlage 110.000 EW mit Kanalnetz, Playbooks für die Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Kläranlage, 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, Bereitschaft und OT-Security ihn erkennen. Daraus ist je Szenario ein Playbook abgeleitet.

Zwei Muster bestimmen den Plan: Angreifer nutzen den regulären Bedienweg, und das Kanalnetz besteht aus unbemannten Außenstationen. Die Reaktion setzt deshalb vor Ort an: Pumpen auf Hand, Fackel starten, Gebläse und Dosierung fest einstellen, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Die Kläranlage läuft ohne Leitsystem weiter, wenn Steuerungen, Unterstationen und Sicherheitsfunktionen unabhängig sind. Jede Reaktion beginnt damit, den Prozess laufen zu lassen und vor Ort zu prüfen.

ID	Szenario	Erster Erkennungspunkt	Playbook
A1	Pumpwerke im Regen fern abgeschaltet	ungewöhnliches Bedienmuster: Abschaltbefehle an mehrere Pumpwerke bei Regen	PB-A1
A2	Fremder Laptop in der Außenstation PW3	Meldung Türkontakt in der Leitwarte	PB-A2
A3	Gasmanagement manipuliert, Biogas tritt aus	Verbindung des Herstellerzugangs außerhalb eines Wartungsauftrags	PB-A3
A4	Belüftung abgeschaltet, Ammonium steigt	S7-Schreibzugriff von fremder Adresse	PB-A4
A5	Ransomware im Leitsystem	RDP außerhalb der Zeiten, Sitzung ohne Auftrag	PB-A5
A6	Fällmitteldosierung abgeschaltet, Phosphor steigt	S7-Schreibzugriff von fremder Adresse	PB-A6

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 H16 aus der Risikobewertung.
- **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 A1 Pumpwerke im Regen fern abgeschaltet

Ein Angreifer übernimmt einen Bedienplatz und schaltet über die normale Bedienung des Leitsystems zwei Pumpwerke ab, während es stark regnet. Der Befehl geht regulär über das Fernwirk-Frontend per IEC 104 an die Unterstationen. Risiko: **KRITISCH** ohne Härtung, **KRITISCH** im Planungsstand, **MITTEL** vollständig gehärtet.

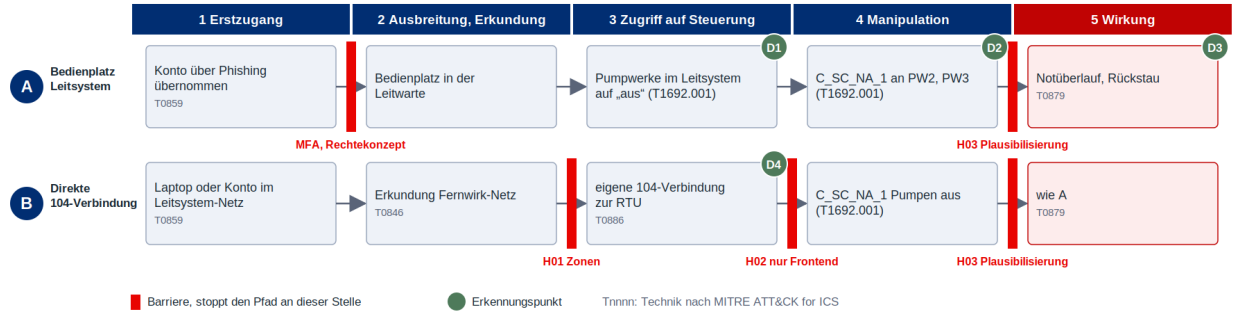


Abbildung: Angriffspfade A1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	ungewöhnliches Bedienmuster: Abschaltbefehle an mehrere Pumpwerke bei Regen	OT-Monitoring, Leitwarte
D2	negative Bestätigung der Unterstation (Befehl abgewiesen)	Leitwarte
D3	Hochwasser und Notüberlauf in den Pumpwerken, Bürgerbeschwerden	Leitwarte, Bereitschaft
D4	104-Verbindung von einer Adresse, die nicht das Frontend ist	Firewall, OT-Monitoring

PLAYBOOK PB-A1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder D3	jeder
Sofort, 0 bis 15 min	Pumpen fern wieder ein; wenn das nicht geht, Bereitschaft zu den Pumpwerken, Wahlschalter auf Hand. Verdächtigen Bedienplatz abmelden und vom Netz.	Leitwarte, Bereitschaft Kanal
Eindämmen, bis 4 h	Fernsteuerung aller Pumpwerke auf „Ort“, Konten sperren, Bedienprotokoll und Mitschnitt sichern.	OT-Security, Schichtleitung
Beseitigen	Bedienplatz neu aufsetzen, Passwörter tauschen, Rechte prüfen.	OT-Security
Wiederherstellen	Plausibilisierung in den Unterstationen aktivieren und testen, Fernbetrieb schrittweise freigeben.	Automatisierer, Betriebsleitung
Melden	Wasserbehörde (außerplanmäßige Entlastung), Polizei, Versicherung; NIS2 falls anwendbar.	Werkleitung

3.2 A2 Fremder Laptop in der Außenstation PW3

Jemand bricht in den Schaltschrank des abgelegenen Pumpwerks ein, klemmt einen Laptop zwischen RTU und Router und meldet der Leitstelle ein ruhiges Niveau, während die Pumpen vor Ort aus sind. Risiko: **KRITISCH** ohne Härtung, **HOCH** im Planungsstand, **NIEDRIG** vollständig gehärtet.

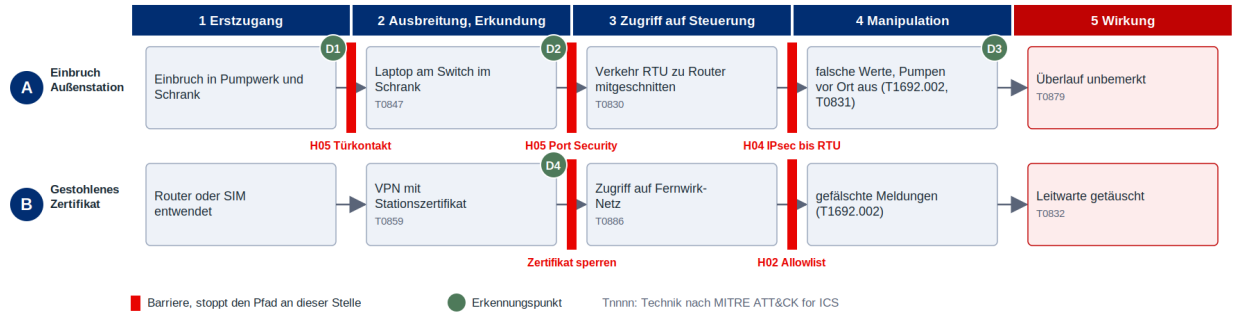


Abbildung: Angriffspfade A2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Meldung Türkontakt in der Leitwarte	Leitwarte
D2	neue MAC-Adresse, ARP-Auffälligkeiten im Stationsnetz	OT-Monitoring
D3	Niveau seit Stunden konstant, Zulauf aus dem Gebiet fehlt an der Kläranlage	Leitwarte, Betriebsleitung
D4	zweite VPN-Sitzung derselben Station, Anmeldung von unbekannter IP	VPN-Konzentrator, SIEM

PLAYBOOK PB-A2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D3 oder D4	jeder
Sofort, 0 bis 15 min	Bereitschaft mit Polizei zur Station, nicht allein ins Bauwerk. Pumpen vor Ort auf Hand, Laptop nicht abziehen, Fotos.	Bereitschaft Kanal, Leitwarte
Eindämmen, bis 4 h	VPN-Zertifikat der Station sperren, Station im Notbetrieb über Schwimmer.	OT-Security
Beseitigen	Station neu aufsetzen, Schrank und Bauwerk sichern.	Fernwirk-Lieferant, Elektriker
Wiederherstellen	IPsec bis in die RTU, Port Security, neue Zertifikate.	Fernwirk-Lieferant
Melden	Polizei (Einbruch), Wasserbehörde bei Überlauf.	Werkleitung

3.3 A3 Gasmanagement manipuliert, Biogas tritt aus

Über die Fernüberwachung des BHKW-Herstellers werden beide BHKW gesperrt und die Fackel blockiert. Der Gasspeicher läuft voll. Risiko: **KRITISCH** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** vollständig gehärtet.

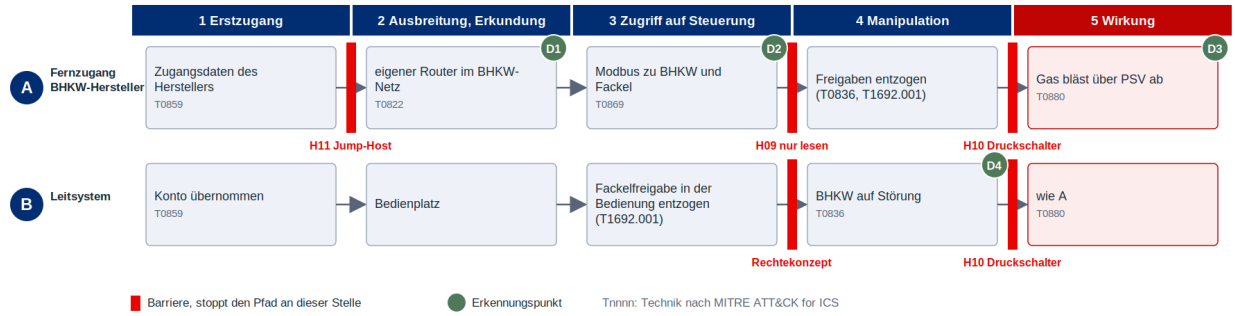


Abbildung: Angriffspfade A3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Verbindung des Herstellerzugangs außerhalb eines Wartungsauftrags	SIEM, Leitwarte
D2	Modbus-Schreibzugriff auf BHKW oder Fackel	OT-Monitoring
D3	Speicher über 95 %, Meldung Überdrucksicherung, Gaswarnung außen, Geruch	Leitwarte, alle vor Ort
D4	Meldung „Fackel gesperrt bei hohem Füllstand“	Leitwarte

PLAYBOOK PB-A3

Phase	Maßnahmen	Zuständig
Auslöser	D2, D3 oder D4	jeder
Sofort, 0 bis 15 min	Bereich um den Gasspeicher absperren, Zündquellen fern, Fackel vor Ort starten, bei Gaswarnung Feuerwehr 112.	Maschinist, Leitwarte
Eindämmen, bis 4 h	Herstellerzugang trennen, BHKW lokal freigeben, Freigaben in der AS-40 prüfen.	OT-Security, Elektriker
Beseitigen	Parameter der BHKW mit Hersteller prüfen, Konten des Herstellers sperren.	BHKW-Hersteller
Wiederherstellen	Fernüberwachung nur lesend und über Jump-Host, Abnahme der Gasanlage nach Explosionsschutzdokument.	Betriebsleitung, befähigte Person
Melden	Feuerwehr, Immissionsschutzbehörde bei Gasaustritt, Unfallversicherungsträger bei Verletzten.	Werkleitung

3.4 A4 Belüftung abgeschaltet, Ammonium steigt

Von einem infizierten Service-Laptop im Leitsystem-Netz wird der Sauerstoff-Sollwert der AS-20 auf 0,2 mg/l geschrieben, die Gebläse fahren herunter. Risiko: **HOCH** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** vollständig gehärtet.

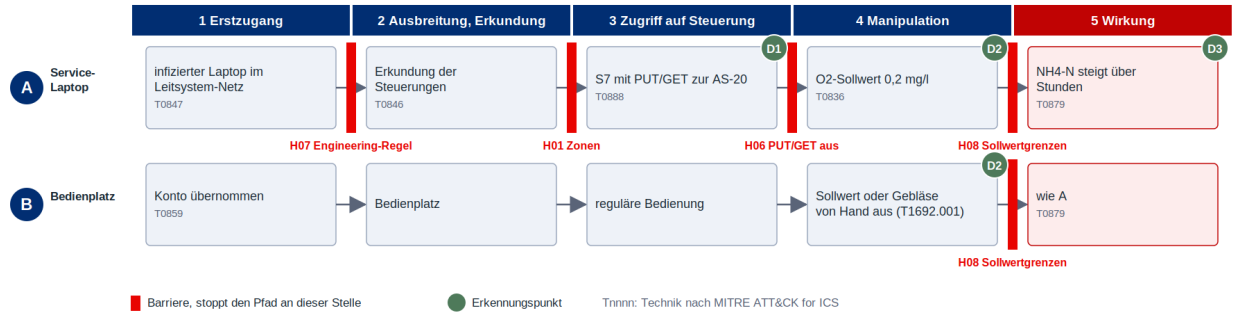


Abbildung: Angriffspfade A4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	S7-Schreibzugriff von fremder Adresse	OT-Monitoring
D2	Gebläse aus, O2 unter 0,5 mg/l, Energieverbrauch fällt	Leitwarte
D3	NH4-N im Ablauf steigt	Messstation, Labor

PLAYBOOK PB-A4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder D3	jeder
Sofort, 0 bis 15 min	Gebläse auf Handbetrieb mit fester Drehzahl, Sollwert 2 mg/l, O2 vor Ort messen.	Leitwarte, Klärwerker
Eindämmen, bis 4 h	Quelle finden und isolieren, Engineering-Zugang sperren, Ablauf häufiger beproben.	OT-Security, Labor
Beseitigen	Programm der AS-20 gegen Sollstand vergleichen.	Automatisierer
Wiederherstellen	Zugriffsschutz und Sollwertgrenzen aktivieren, Nitrifikation beobachten.	Betriebsleitung
Melden	Wasserbehörde bei Überschreitung des Überwachungswerts.	Werkleitung

3.5 A5 Ransomware im Leitsystem

Über gestohlene Admin-Daten am Jump-Host wird Ransomware auf die Leitsystem-Server gebracht. Risiko: **KRITISCH** ohne Härtung, **HOCH** im Planungsstand, **NIEDRIG** vollständig gehärtet.

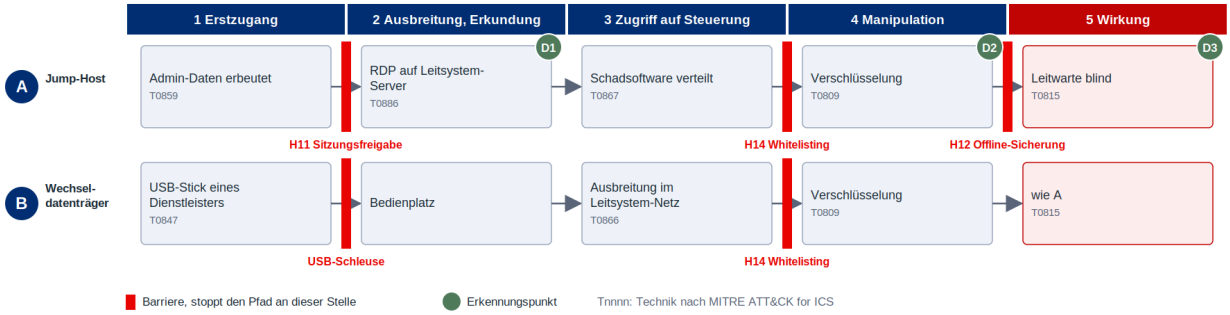


Abbildung: Angriffspfade A5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP außerhalb der Zeiten, Sitzung ohne Auftrag	SIEM
D2	viele SMB-Schreibzugriffe von einem Server	OT-Monitoring
D3	Bildschirme schwarz oder Erpresserhinweis; Störmelder alarmiert weiter per GSM	Leitwarte, Bereitschaft

PLAYBOOK PB-A5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder D3	jeder
Sofort, 0 bis 15 min	Verbindung DMZ zu Leitsystem trennen. Steuerungen und Unterstationen laufen lassen, Panels vor Ort nutzen, Bereitschaft auf Rundgang.	Schichtleitung, OT-Security
Eindämmen, bis 4 h	Betroffene Server vom Netz, Konten sperren, Krisenstab, Notbetrieb mit Handmessungen und Kontrollfahrten im Kanalnetz.	Werkleitung, Betriebsleitung
Beseitigen	Ursache finden, Systeme aus Offline-Sicherung neu aufsetzen, Passwörter tauschen.	OT-Security, externer Dienstleister
Wiederherstellen	Leitsystem schrittweise wieder an, erst dann Fernzugriffe.	Leitsystem-Lieferant
Melden	BSI falls NIS2 anwendbar, Polizei, Versicherung, Aufsichtsbehörde.	Werkleitung

3.6 A6 Fällmitteldosierung abgeschaltet, Phosphor steigt

Über eine ungeschützte S7-Verbindung wird der Dosierfaktor auf 0 gesetzt. Risiko: **MITTEL** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** vollständig gehärtet.



Abbildung: Angriffspfade A6

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	S7-Schreibzugriff von fremder Adresse	OT-Monitoring
D2	Dosierpumpen aus, Tankstand konstant	Leitwarte, Klärwerker
D3	PO4-P im Ablauf steigt	Messstation, Labor

PLAYBOOK PB-A6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2 oder D3	jeder
Sofort, 0 bis 15 min	Dosierpumpen von Hand auf Auslegungsmenge.	Klärwerker
Eindämmen, bis 4 h	Quelle isolieren, Proben.	OT-Security, Labor
Beseitigen	Programm gegen Sollstand vergleichen.	Automatisierer
Wiederherstellen	Sollwertgrenzen und Mindestdosierung in der SPS.	Automatisierer
Melden	Wasserbehörde bei Überschreitung.	Werkleitung

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Menschen, Gewässer, Anlage, Betrieb.
- **Prozess laufen lassen:** Steuerungen und Unterstationen nicht abschalten oder neu starten ohne Rücksprache; Diagnosepuffer sind Beweismittel.
- **Zugänge zuerst trennen:** Fernwartung, Jump-Host, betroffene Fernwirkverbindungen.
- **Vor Ort messen:** Bei zweifelhaften Werten gilt die Handmessung.
- **Alles mit Uhrzeit festhalten**, Fotos von Bildschirmen und Schaltschränken.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Pumpwerke	Niveausteuerung vor Ort, Schwimmer startet Pumpe 2 hart verdrahtet, Kontrollfahrten
Regenüberlaufbecken	Drosselregelung vor Ort, Entlastung über feste Schwelle
Biologie	Sauerstoffregelung in der AS-20 mit letztem Sollwert, Ersatzluftmenge bei Sondenausfall
Gas	Staffelung in der AS-40, Fackel über Druckschalter, mechanische Über- und Unterdrucksicherung
Alarmierung	unabhängiger Störmelder per GSM an die Bereitschaft

4.3 Rollen

Rolle	Aufgabe	Besetzung
Leitwarte, Schichtleitung	erkennt, setzt Sofortmaßnahmen, alarmiert	[Name, Telefon]
Bereitschaft Kanal	Pumpwerke und RÜB vor Ort, Handbetrieb	[Name, Telefon]
Maschinist, Elektriker	Gasanlage, BHKW, Fackel, Schaltanlagen	[Name, Telefon]
OT-Security	Bewertung, Trennen von Zugängen, Beweise, Wiederherstellung	[Name, Telefon]
Betriebsleitung	Stufe 2, Notbetrieb, Lieferanten	[Name, Telefon]
Werkleitung	Stufe 3, Krisenstab, Meldungen, Öffentlichkeit	[Name, Telefon]
Externe Unterstützung	OT-Forensik, Wiederanlauf	[Dienstleister]

4.4 Stufen

Stufe	Merkmal	Entscheidet
1 Verdacht	einzelne Auffälligkeit ohne Wirkung	Schichtleitung mit OT-Security
2 Angriff bestätigt	keine Gefahr für Menschen oder Gewässer	Betriebsleitung
3 Krise	Gefahr für Menschen, Gasaustritt, Rückstau oder Gewässerschaden	Werkleitung, Krisenstab

4.5 Meldungen

Anlass	Stelle	Frist
Überschreitung von Überwachungswerten, Störung mit Gewässerbelastung	zuständige Wasserbehörde	unverzüglich, nach Bescheid und Landesrecht
außerplanmäßige Entlastung, Notüberlauf	Wasserbehörde, bei Badegewässern Gesundheitsamt	unverzüglich
Gasaustritt, Brand	Feuerwehr, Immissionsschutzbehörde	sofort
erheblicher Sicherheitsvorfall (§ 32 BSIG)	Meldestelle BSI und BBK	Erstmeldung 24 h, Bewertung 72 h nach Kenntnis, Abschluss einen Monat nach der 72-h-Meldung
Arbeitsunfall	Unfallkasse oder Berufsgenossenschaft	nach Vorgabe des Trägers
Straftat, Einbruch	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarm- und Telefonliste in Leitwarte und Bereitschaftsfahrzeugen, Schlüssel für alle Außenstationen.
- Notbetriebshandbuch je Bereich.
- Offline-Sicherung aller Steuerungen, Unterstationen und Server; Wiederanlauf einmal im Jahr geübt.
- Reaktionszeiten der Lieferanten von Fernwirk, BHKW und Leitsystem im Vertrag.
- Planspiel zweimal im Jahr mit den Szenarien des HTML-Leitstands.

5 Nächste Schritte

- Rollen besetzen, Telefonliste erstellen.

- Playbooks mit Betriebsleitung und Bereitschaft abstimmen.
- Erstes Planspiel mit Szenario A1 im Regenfall.