BERICHT

Risikobewertung Cyberangriffe

Kläranlage 110.000 EW mit Kanalnetz, Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Kläranlage, 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 Kläranlage mit 110.000 EW und Kanalnetz wurden sechs Angriffe bewertet, die den größten Schaden für Menschen, Gewässer und Betrieb anrichten können: Abschalten von Pumpwerken im Regen, Manipulation einer Außenstation, Eingriff in das Gasmanagement, Abschalten der Belüftung, Ransomware im Leitsystem und Abschalten der Fällung.

Ohne Härtung sind 4 Szenarien kritisch. Im typischen Planungsstand bleiben 1 kritisch und 2 hoch. Den größten Einzeleffekt hat die Plausibilisierung von Fernbefehlen in den Unterstationen: Ein Angreifer, der einen Bedienplatz übernimmt, nutzt den regulären Bedienweg, und Firewalls helfen dagegen nicht. Mit allen 16 Maßnahmen liegt kein Szenario über MITTEL.

GESAMTBEWERTUNG

Die gefährlichsten Angriffe nutzen den regulären Bedienweg oder unbemannte Außenstationen. Wirksam sind Maßnahmen im Prozess selbst: Plausibilisierung in den Unterstationen, Sollwertgrenzen in der SPS und eine Fackel, die hart verdrahtet startet. Netzwerktrennung allein reicht nicht.

SZENARIEN NACH RISIKOKLASSE

Klasse	Ohne Härtung	Planungsstand	Vollständig
KRITISCH	4	1	0
HOCH	1	2	0
MITTEL	1	1	1
NIEDRIG	0	2	5

2 Ausgangslage und Methode

Grundlage ist die Demonstrationsanlage im HTML-Leitstand (Klaeranlage_Leitstand_PurpleTeam.html) mit Simulation, SPS-Programmen, Netzwerkverkehr und den Angriffsszenarien A1 bis A6. 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, Gewässer und Umwelt, Betrieb und Finanzen.
- **Drei Stände:** ohne Härtung, typischer Planungsstand (H01, H05, H08, H10, H13 umgesetzt), vollständige Härtung H01 bis H16.
- **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	Zonen und Conduits mit Firewall zwischen Leitsystem und Zellen	umgesetzt
H02	Fernwirk: 104-Verbindungen nur vom Fernwirk-Frontend (Firewall, Allowlist in der RTU)	fehlt
H03	Plausibilisierung von Fernbefehlen in der Unterstation (Pumpen aus bei Hochwasser abgewiesen)	fehlt
H04	104 Ende-zu-Ende gesichert: TLS nach IEC 62351-3 und Secure Authentication nach IEC 60870-5-7, kein Klartext im Schaltschrank	fehlt
H05	Außenstation: Türkontakt als Meldung, Port Security, abgeschlossene Schränke	umgesetzt
H06	Zugriffsschutz der CPUs aktiv, PUT/GET aus	fehlt
H07	Engineering nur von der Engineering-Station, Anmeldung mit MFA	fehlt
H08	Sollwertgrenzen und Mindestdosierung in der SPS	umgesetzt
H09	Modbus nur lesend: Firewall vor BHKW, Fackel und Analysatoren	fehlt
H10	Fackelstart über Druckschalter hart verdrahtet, unabhängig von der SPS	umgesetzt
H11	Fernwartung der Lieferanten nur über Jump-Host mit Freigabe je Sitzung	fehlt
H12	Offline-Sicherung von Leitsystem und Steuerungen, geübter Wiederanlauf	fehlt
H13	Unabhängiger Störmelder (GSM) für Prio-1-Alarme	umgesetzt
H14	Härtung und Anwendungs-Whitelisting der Windows-Systeme	fehlt
H15	OT-Monitoring mit Anomalieerkennung am Spiegelport	fehlt
H16	Reaktionsplan, Bereitschaft geschult, Awareness	fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Vollständig
A1	Pumpwerke im Regen fern abgeschaltet	KRITISCH	KRITISCH	MITTEL
A2	Fremder Laptop in der Außenstation PW3	KRITISCH	HOCH	NIEDRIG
A3	Gasmanagement manipuliert, Biogas tritt aus	KRITISCH	MITTEL	NIEDRIG
A4	Belüftung abgeschaltet, Ammonium steigt	HOCH	NIEDRIG	NIEDRIG
A5	Ransomware im Leitsystem	KRITISCH	HOCH	NIEDRIG
A6	Fällmitteldosierung abgeschaltet, Phosphor steigt	MITTEL	NIEDRIG	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in drei Härtungsständen

3.2 Szenarien im Detail

3.2.1 A1 Pumpwerke im Regen fern abgeschaltet

Ohne Härtung	**KRITISCH** (A 5 × W 4 = 20)
Betroffene Systeme	Leitsystem Z04, Fernwirk-Frontend Z07, Unterstationen PW2 und PW3 (Z08)
Ort	Kanalnetz, Pumpwerke PW2, PW3, Notüberläufe
Angriffsweg	1. Konto eines Bedienplatzes über Phishing übernommen (T0859) 2. Pumpwerke im Leitsystem auf „Pumpen aus“ geschaltet, der Weg ist legitim (T1692.001) 3. Frontend sendet C_SC_NA_1 an PW2 und PW3, die Unterstation prüft den Befehl (T1692.001) 4. Pumpensümpfe laufen voll, Notüberlauf (T0879)
Folgen	Notüberlauf in Unterstadt und Altstadt, Rückstau in Keller, ungeklärtes Abwasser im Gewässer.
Planungsstand	**KRITISCH** (A 5 × W 4 = 20)
Ergebnis Planungsstand	gelingt
Vollständige Härtung	**MITTEL** (A 5 × W 1 = 5)
Ergebnis vollständig	gestoppt in Schritt 3 durch H03
Restrisiko	Ein Angreifer mit Zugriff auf die Unterstation selbst umgeht die Plausibilisierung. Physischer Schutz der Außenstationen (A2) bleibt nötig.
Schaden im Ernstfall	0,5 bis 5 Mio. €: Rückstauschäden in Gebäuden, Haftung, Gewässerschaden; Gefahr für Menschen in überfluteten Kellern
Referenz	MITRE ATT&CK for ICS v20: T0859, T1692.001, T0879; IEC 62443-3-3 SR 2.1, SR 3.5; DWA-M 1060

3.2.2 A2 Fremder Laptop in der Außenstation PW3

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Außenstation PW3 (Z08): RTU, Switch, LTE-Router
Ort	Pumpwerk Unterstadt
Angriffsweg	1. Einbruch in den Schaltschrank des Pumpwerks (physisch) 2. Laptop am Switch im Schrank (T0847) 3. Verkehr zwischen RTU und Router im Klartext mitgeschnitten und verändert (T0830) 4. Gefälschte Messwerte an die Leitstelle, Pumpen vor Ort aus (T1692.002, T0831)
Folgen	Leitwarte sieht 0,8 m und „alles in Ordnung“, tatsächlich läuft der Sumpf über.
Planungsstand	**HOCH** (A 5 × W 2 = 10)
Ergebnis Planungsstand	gestoppt in Schritt 2 durch H05
Vollständige Härtung	**NIEDRIG** (A 4 × W 1 = 4)
Ergebnis vollständig	gestoppt in Schritt 2 durch H05
Restrisiko	Wer genug Zeit im Schrank hat, kann auch Port Security umgehen. Erkennung über Türkontakt, Plausibilität der Werte (Zulauf Kläranlage) und Monitoring.
Schaden im Ernstfall	0,5 bis 5 Mio. € wie A1, Erkennung später, weil die Leitwarte falsche Werte sieht
Referenz	MITRE ATT&CK for ICS v20: T0847, T0830, T1692.002, T0831; IEC 62443-3-3 SR 3.1, SR 7.7; IEC 62351

3.2.3 A3 Gasmanagement manipuliert, Biogas tritt aus

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	BHKW-Steuerungen (Z13), Fackelsteuerung und AS-40 (Z12), Hersteller-Fernzugang
Ort	Gasspeicher GS-400, BHKW-1/-2, FA-420, PSV 401
Angriffsweg	1. Zugangsdaten der Hersteller-Fernüberwachung erbeutet (T0859, T0822) 2. Modbus-Schreibbefehle an BHKW-Steuerungen und Fackel (T1692.001, T0836) 3. Gasspeicher steigt, keine Verbrennung (T0813) 4. Überdrucksicherung spricht an, Biogas tritt aus (T0880)
Folgen	Überdrucksicherung bläst Biogas ab: Explosionsgefahr im Umfeld, Methan in die Atmosphäre, Geruch, Stromzukauf.
Planungsstand	**MITTEL** (A 3 × W 3 = 9)
Ergebnis Planungsstand	gelingt, Wirkung begrenzt durch H10
Vollständige Härtung	**NIEDRIG** (A 3 × W 1 = 3)
Ergebnis vollständig	gestoppt in Schritt 1 durch H11
Restrisiko	Die mechanische Überdrucksicherung bleibt die letzte Barriere. Explosionsschutzdokument und Ex-Zonen müssen den Abblasefall abdecken.
Schaden im Ernstfall	0,3 bis 3 Mio. € bei Gasaustritt ohne Zündung; bei Zündung Personen- und Gebäudeschäden in anderer Größenordnung
Referenz	MITRE ATT&CK for ICS v20: T0822, T1692.001, T0836, T0880; IEC 62443-3-3 SR 1.13, SR 5.2; Explosionsschutz

3.2.4 A4 Belüftung abgeschaltet, Ammonium steigt

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	AS-20 Biologie (Z10), Gebläsestation, Leitsystem-Netz
Ort	Belebung BB-201 bis 204, Gebläse G-210 bis 212
Angriffsweg	1. Infizierter Service-Laptop im Leitsystem-Netz (T0847) 2. S7-Verbindung mit PUT/GET zur AS-20 (T0888) 3. Sauerstoff-Sollwert auf 0,2 mg/l geschrieben (T0836) 4. Nitrifikation bricht ein (T0879)
Folgen	NH4-N im Ablauf steigt über Stunden über 10 mg/l, Überschreitung des Überwachungswerts, erhöhte Abwasserabgabe, Schaden im Gewässer.
Planungsstand	**NIEDRIG** (A 4 × W 1 = 4)
Ergebnis Planungsstand	gestoppt in Schritt 2 durch H01
Vollständige Härtung	**NIEDRIG** (A 4 × W 1 = 4)
Ergebnis vollständig	gestoppt in Schritt 1 durch H07
Restrisiko	Über die reguläre Bedienung bleibt eine Sollwertänderung möglich; dagegen helfen Sollwertgrenzen in der SPS und ein Rechtekonzept.
Schaden im Ernstfall	0,1 bis 1 Mio. €: erhöhte Abwasserabgabe, Gewässerschaden, Wiederaufbau der Nitrifikation über Tage bis Wochen
Referenz	MITRE ATT&CK for ICS v20: T0847, T0888, T0836, T0879; IEC 62443-3-3 SR 2.1, SR 3.5

3.2.5 A5 Ransomware im Leitsystem

Ohne Härtung	**KRITISCH** (A 4 × W 4 = 16)
Betroffene Systeme	Leitsystem-Server, Bedienplätze (Z04), Jump-Host (Z03)
Ort	Leitwarte, Fernwirkzentrale
Angriffsweg	1. Admin-Daten des Jump-Hosts erbeutet (T0859) 2. RDP vom Jump-Host auf Leitsystem-Server A (T0886) 3. Schadsoftware verschlüsselt die Server (T0809) 4. Leitstand blind, Alarme kommen nicht mehr an (T0815)
Folgen	Leitwarte und Bereitschaft sehen nichts mehr, auch nicht das Kanalnetz. Steuerungen und Unterstationen arbeiten autark weiter.
Planungsstand	**HOCH** (A 3 × W 4 = 12)
Ergebnis Planungsstand	gelingt, Wirkung begrenzt durch H13
Vollständige Härtung	**NIEDRIG** (A 2 × W 1 = 2)
Ergebnis vollständig	gestoppt in Schritt 1 durch H11
Restrisiko	Ransomware kann auch über andere Wege kommen (Wechseldatenträger, Lieferkette). Offline-Sicherung und geübter Wiederanlauf begrenzen die Dauer.
Schaden im Ernstfall	0,3 bis 2 Mio. €: Wiederherstellung, Handbetrieb mit Mehrpersonal über Wochen, Lösegeldforderung, Meldepflichten
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0815; IEC 62443-3-3 SR 3.2, SR 7.3, SR 7.4

3.2.6 A6 Fällmitteldosierung abgeschaltet, Phosphor steigt

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	AS-20 (Z10), Fällmittelstation T-240
Ort	Fällmittelstation, Ablauf
Angriffsweg	1. Zugang zum Leitsystem-Netz (T0859) 2. S7-Schreibzugriff auf AS-20 (T1692.001) 3. Dosierfaktor 0 (T0836) 4. P-Elimination fällt aus (T0879)
Folgen	Pges im Ablauf steigt über Stunden über 1 mg/l; Überschreitung, erhöhte Abgabe, Eutrophierung des Gewässers.
Planungsstand	**NIEDRIG** (A 3 × W 1 = 3)
Ergebnis Planungsstand	gestoppt in Schritt 2 durch H01
Vollständige Härtung	**NIEDRIG** (A 3 × W 1 = 3)
Ergebnis vollständig	gestoppt in Schritt 1 durch H07
Restrisiko	Wie A4: Sollwertgrenzen und Mindestdosierung in der SPS begrenzen auch Fehlbedienung.
Schaden im Ernstfall	0,05 bis 0,5 Mio. €: erhöhte Abwasserabgabe, Eutrophierung
Referenz	MITRE ATT&CK for ICS v20: T0859, T1692.001, T0836; IEC 62443-3-3 SR 2.1, SR 3.5

4 Maßnahmen und Wirtschaftlichkeit

Bezug zeigt, in welchen Szenarien die Maßnahme einen Schritt stoppt oder die Wirkung begrenzt. Die Priorität folgt der Risikominderung im Planungsstand. Kosten sind Schätzungen, Angebote einholen.

Nr.	Maßnahme	Bezug	Priorität	Kosten
H01	Zonen und Conduits mit Firewall zwischen Leitsystem und Zellen	A4, A6	umgesetzt	15.000 bis 40.000 €
H02	Fernwirk: 104-Verbindungen nur vom Fernwirk-Frontend (Firewall, Allowlist in der RTU)	alle	**Hoch**	2.000 bis 5.000 €
H03	Plausibilisierung von Fernbefehlen in der Unterstation (Pumpen aus bei Hochwasser abgewiesen)	A1	**Hoch**	1.000 bis 2.000 € je Station
H04	104 Ende-zu-Ende gesichert: TLS nach IEC 62351-3 und Secure Authentication nach IEC 60870-5-7, kein Klartext im Schaltschrank	A2	**Hoch**	1.500 bis 4.000 € je Station
H05	Außenstation: Türkontakt als Meldung, Port Security, abgeschlossene Schränke	A2	umgesetzt	500 bis 1.500 € je Station
H06	Zugriffsschutz der CPUs aktiv, PUT/GET aus	A4, A6	**Mittel**	1.000 bis 3.000 €
H07	Engineering nur von der Engineering-Station, Anmeldung mit MFA	A4, A6	**Mittel**	5.000 bis 15.000 €
H08	Sollwertgrenzen und Mindestdosierung in der SPS	A4, A6	umgesetzt	2.000 bis 5.000 €
H09	Modbus nur lesend: Firewall vor BHKW, Fackel und Analysatoren	A3	**Hoch**	4.000 bis 7.000 € je Stelle
H10	Fackelstart über Druckschalter hart verdrahtet, unabhängig von der SPS	A3	umgesetzt	3.000 bis 8.000 €
H11	Fernwartung der Lieferanten nur über Jump-Host mit Freigabe je Sitzung	A3, A5	**Hoch**	10.000 bis 30.000 €
H12	Offline-Sicherung von Leitsystem und Steuerungen, geübter Wiederanlauf	alle	**Hoch**	10.000 bis 30.000 €
H13	Unabhängiger Störmelder (GSM) für Prio-1-Alarme	A5	umgesetzt	2.000 bis 5.000 €
H14	Härtung und Anwendungs-Whitelisting der Windows-Systeme	A5	**Hoch**	5.000 bis 15.000 €
H15	OT-Monitoring mit Anomalieerkennung am Spiegelport	alle	**Mittel**	30.000 bis 80.000 € je Jahr
H16	Reaktionsplan, Bereitschaft geschult, Awareness	alle	**Mittel**	5.000 bis 15.000 € je Jahr

Tabelle 2: Maßnahmen, Priorität im Planungsstand, geschätzte Kosten

Die fehlenden Maßnahmen mit Priorität Hoch kosten zusammen grob 60.000 bis 150.000 € einmalig. Ein einziges Rückstauereignis in einem Wohngebiet (A1, A2) oder ein Gasaustritt (A3) liegt im Bereich von

0,3 bis 5 Mio. € und kann Menschen gefährden. Die Maßnahmen rechnen sich, wenn sie die Eintrittswahrscheinlichkeit über zehn Jahre um wenige Prozentpunkte senken.

4.1 Rechtlicher Rahmen

- **KRITIS:** Keine kritische Anlage. Die Schwelle für Kläranlagen liegt bei 500.000 EW Ausbaugröße (BSI-KritisV Anhang 2 Teil 3 Nr. 2.2.1), für Kanalisation bei 500.000 angeschlossenen Einwohnern (Nr. 2.1.1). Das KRITIS-Dachgesetz gilt seit 17.03.2026; die Verordnung zu den Anlagenkategorien steht noch aus.
- **NIS2:** Das BSIG in der NIS2-Fassung gilt seit 06.12.2025. Abwasser ist ein Sektor mit hoher Kritikalität (Anlage 1). Ein Abwasserbetrieb dieser Größe ist ab 50 Beschäftigten oder mehr als 10 Mio. € Umsatz und Bilanzsumme in der Regel wichtige Einrichtung (§ 28 BSIG), auch als Eigenbetrieb oder AöR. Für den konkreten Betreiber zu prüfen.
- **Branchenstandard:** DWA-M 1060 / DVGW W 1060 „IT-Sicherheit – Branchenstandard Wasser/Abwasser“ (09/2024) mit dem B3S WA-Sicherheitskompendium.
- **Wasserrecht:** Überwachungswerte nach Bescheid und AbwV Anhang 1; Überschreitungen erhöhen die Abwasserabgabe. Die Umsetzung der Kommunalabwasserrichtlinie (EU) 2024/3019 bis 31.07.2027 wird die Anforderungen verschärfen.
- **Explosionsschutz:** Gasanlage nach BetrSichV und GefStoffV, Explosionsschutzdokument; die Wirkung von Cyberangriffen gehört in die Gefährdungsbeurteilung. Maschinenverordnung (EU) 2023/1230 ab 20.01.2027 für neue Maschinen.

HINWEIS

Werte und Szenarien beziehen sich auf eine fiktive Anlage. Für eine reale Anlage sind Bewertung, Kosten und Fristen mit Betreiber, Behörde und Lieferanten abzustimmen.

5 Nächste Schritte

- Plausibilisierung von Fernbefehlen (H03) und Herstellerzugang über Jump-Host (H11) als erste Maßnahmen beauftragen.
- Lieferantenanforderungen für Fernwirk, BHKW und Leitsystem in die Ausschreibung aufnehmen.
- Reaktionsplan mit den Playbooks einführen und im Planspiel üben.
- Bewertung nach IEC 62443-3-2 mit dem Betreiber freigeben.