BERICHT

Angriffspfade und Reaktionsplan

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Umspannwerke, 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: Versorgung vor Anlage, und bei Zweifel an der Leitstelle sofort Ortsteuerung mit Personal in den Stationen. Die Reaktion setzt in der Leitwarte und vor Ort an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Das Netz bleibt beherrschbar, wenn der Schutz eigenständig arbeitet und jede Station ohne Leitstelle bedient werden kann. Schaltberechtigte, Schlüssel und Netzpläne müssen dafür griffbereit sein.

ID	Szenario	Erster Erkennungspunkt	Playbook
U1	Massenhafte Schaltbefehle aus der Netzleitstelle	SSH-Anmeldung außerhalb der Wartung	PB-U1
U2	Ortsnetzstationen über das 450-MHz-Funknetz	Anmeldung am Router über Funk	PB-U2
U3	Gefälschte Abtastwerte im Prozessbus	Einbruchmeldung, Zutritt ohne Auftrag	PB-U3
U4	Parkregler des PV-Parks manipuliert	Einspeisung folgt nicht der Vorgabe	PB-U4
U5	Gefälschte Redispatch-Abrufe	Abruf passt nicht zur Netzsituation	PB-U5
U6	Ransomware in der Netzleitstelle	Anmeldungen außerhalb der Wartung	PB-U6

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 U1 Massenhafte Schaltbefehle aus der Netzleitstelle

Mit erbeuteten Admin-Daten gelangt der Angreifer über den Jump-Host per SSH auf das Leitsystem und bringt Schadsoftware auf das Front-End. Sie sendet über den regulären Fernwirkweg IEC-104-Doppelbefehle: 110-kV-Leitungsfelder und 20-kV-Abgänge beider Umspannwerke aus. Risiko: **KRITISCH** ohne Härtung, **HOCH** im Planungsstand, **HOCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.

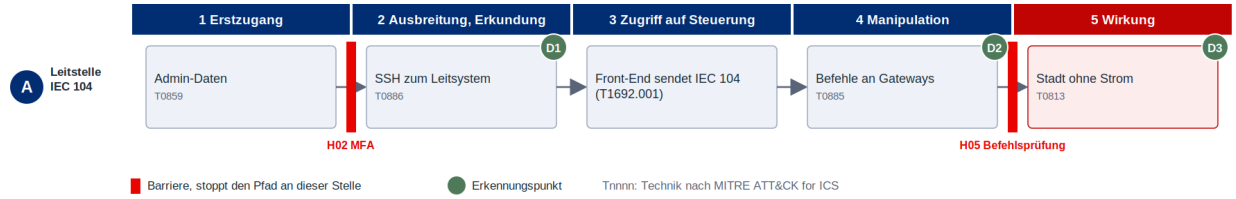


Abbildung: Angriffspfade U1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	SSH-Anmeldung außerhalb der Wartung	Jump-Host, Monitoring
D2	Fernbefehle in ungewöhnlicher Zahl	OT-Monitoring, Stationsrechner
D3	Schalter fallen ohne Bedienhandlung	Leitwarte

PLAYBOOK PB-U1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Fernwirkverbindung trennen bzw. Ortsteuerung in allen Stationen, Monteure losschicken.	Schichtleiter
Eindämmen	Konten sperren, Front-End und Server vom Netz, Ersatzleitstelle bzw. Papierlage.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Bundesnetzagentur (Versorgungsunterbrechung), ÜNB, Polizei.	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Leitsystem aus Offline-Sicherung, Befehlsprüfung im Stationsrechner beibehalten.	Netzbetrieb, Hersteller

3.2 U2 Ortsnetzstationen über das 450-MHz-Funknetz

Der Funkrouter der ONS 6 läuft mit alter Firmware und Standardkonto. Der Angreifer übernimmt ihn per Funk, gelangt in das Fernwirknetz der Ortsnetzstationen und sendet IEC-104-Befehle an andere Fernwirkstationen: Lasttrennschalter aus. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade U2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Anmeldung am Router über Funk	Kopfstelle
D2	IEC 104 zwischen Ortsnetzstationen	OT-Monitoring
D3	Lasttrennschalter fallen	Leitwarte

PLAYBOOK PB-U2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Router sperren, Monteure zur Wiederversorgung.	Schichtleiter
Eindämmen	Alle Funkrouter auf Firmware und Konten prüfen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Polizei.	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Firmware, Zertifikate je Router, Trennung der Router voneinander.	Netzbetrieb, Hersteller

3.3 U3 Gefälschte Abtastwerte im Prozessbus

Ein fremdes Gerät wird im UW Süd an einen freien Port des Prozessbus-Switches gesteckt. Es sendet Sampled Values mit der Kennung einer Merging Unit und einem eingespielten Fehlerstrom; der Trafodifferenzialschutz löst den Trafo T1 aus. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade U3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Einbruchmeldung, Zutritt ohne Auftrag	Leitwarte
D2	Doppelter SV-Strom	Schutz, OT-Monitoring
D3	Auslösung T1 ohne Netzfehler	Leitwarte, Schutztechnik

PLAYBOOK PB-U3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Versorgung über Kupplung und T2 herstellen, Station besetzen.	Schichtleiter
Eindämmen	Fremdes Gerät entfernen, Ports sperren.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Polizei (Einbruch).	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Port Security, SV-Plausibilisierung, Zutrittskontrolle prüfen.	Netzbetrieb, Hersteller

3.4 U4 Parkregler des PV-Parks manipuliert

Über die Fernwartung des PV-Betreibers übernimmt der Angreifer den Parkregler. Der ignoriert die Abregelung der Netzleitstelle und fährt die Einspeisung sprunghaft hoch; die Spannung im 20-kV-Netz steigt. Der Versuch, vom Parknetz in das Umspannwerk zu gelangen, scheitert an der SC646. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

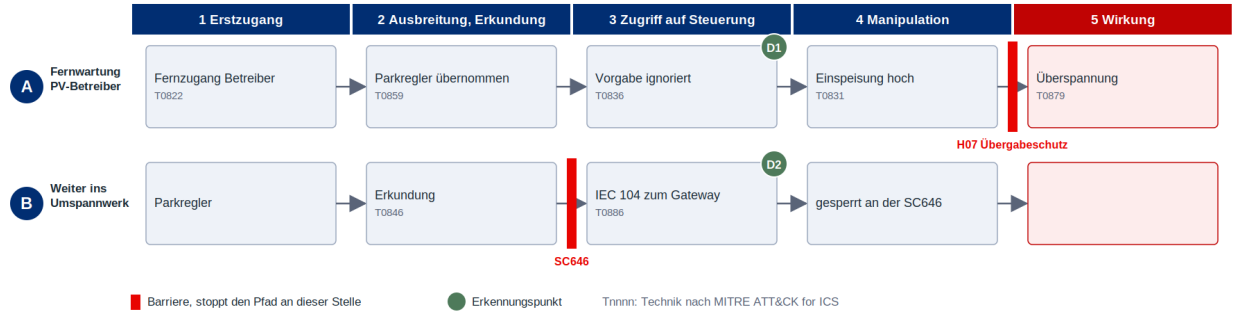


Abbildung: Angriffspfade U4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Einspeisung folgt nicht der Vorgabe	Leitwarte
D2	Verbindungsversuch aus dem Parknetz	SC646, Monitoring

PLAYBOOK PB-U4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Abgang J10 aus, PV-Betreiber informieren.	Schichtleiter
Eindämmen	Wiederzuschaltung erst nach Nachweis des Betreibers.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG; Betreiber meldet eigenständig.	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Anforderungen an Kundenanlagen im Netzanschlussvertrag, Prüfung der Fernzugänge.	Netzbetrieb, Hersteller

3.5 U5 Gefälschte Redispatch-Abrufe

Der Angreifer übernimmt das Redispatch-Gateway in der DMZ und schickt auf dem regulären Weg gefälschte Abrufe ans Leitsystem: PV-Park auf 0 %, Sollspannung 21,9 kV. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

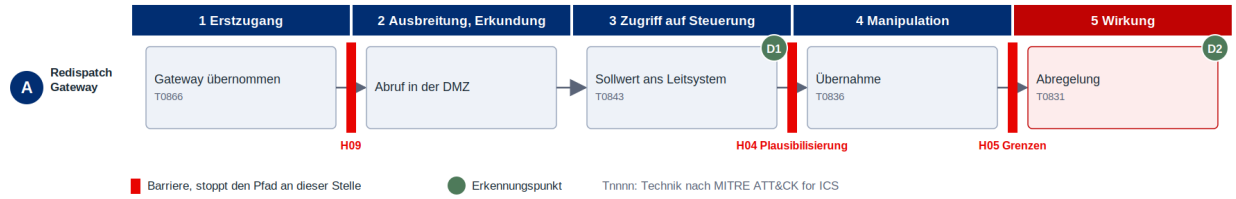


Abbildung: Angriffspfade U5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Abruf passt nicht zur Netzsituation	Leitsystem, Schichtleiter
D2	PV-Betreiber meldet Abregelung ohne Engpass	Betreiber

PLAYBOOK PB-U5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Automatische Übernahme der Abrufe aussetzen.	Schichtleiter
Eindämmen	Gateway vom Netz, Abrufe telefonisch abstimmen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, ÜNB.	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Plausibilisierung im Leitsystem, signierte Abrufe.	Netzbetrieb, Hersteller

3.6 U6 Ransomware in der Netzleitstelle

Ransomware aus der IT scheitert am direkten Weg. Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host auf Leitsystem und Engineering und verschlüsselt sie. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

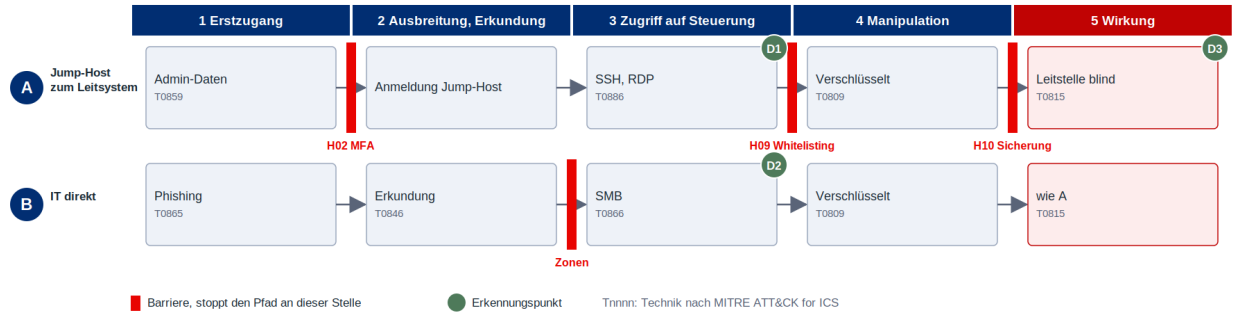


Abbildung: Angriffspfade U6

ERKENNUNGSPUNKTE

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

PLAYBOOK PB-U6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Jump-Host und IT-Verbindungen trennen, Stationen besetzen.	Schichtleiter
Eindämmen	Konten sperren, Umfang feststellen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG (24 h, 72 h, Abschluss), ÜNB, Polizei.	Leiter Netzbetrieb, Geschäftsführung
Wiederherstellen	Leitsystem aus Offline-Sicherung, schrittweise Rückkehr zur Fernsteuerung.	Netzbetrieb, Hersteller

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Menschen, Versorgung, Netzstabilität, Anlage.
- **Ortsteuerung statt blinder Fernsteuerung:** bei Zweifel Stationen besetzen und auf Ort schalten.
- **Schutz nicht verändern:** Parametersätze nur nach Vergleich mit dem freigegebenen Stand.
- **ÜNB und Nachbarnetzbetreiber informieren:** bei jeder unklaren Netzsituation.
- **Alles mit Uhrzeit festhalten:** Störschriebe und Archive sind Beweismittel.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Schutz	arbeitet in jedem Fall eigenständig
Stationen	Ortsbedienung über Station-HMI bzw. am Feld, Schaltberechtigte vor Ort
Ortsnetzstationen	manuelle Schaltung durch Monteure
PV-Park	letzter gültiger Sollwert, bei Bedarf Abschaltung am Abgang J10
Netzleitstelle	Ersatzleitstelle bzw. Papierlage mit Telefon zu den Stationen

4.3 Rollen

Rolle	Aufgabe	Besetzung
Schichtleiter Netzleitstelle	erkennt, setzt Sofortmaßnahmen, alarmiert, spricht mit dem ÜNB	[Name, Telefon]
Leiter Netzbetrieb	Netzführung, Wiederversorgung	[Name, Telefon]
Schutztechnik	Schutzgeräte, Störschriebe	[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	Schichtleiter mit OT-Security
2 Angriff bestätigt	keine Versorgungsunterbrechung	Leiter Netzbetrieb

Stufe	Merkmal	Entscheidet
3 Krise	Versorgungsunterbrechung, Störung im Verbundnetz	Geschäftsführung, Krisenstab, Behörden

4.5 Meldungen

Anlass	Stelle	Frist
erheblicher Sicherheitsvorfall (§ 5d Abs. 3 EnWG)	Meldestelle nach § 32 BSIG (BSI und BBK)	Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h, Abschlussmeldung entsprechend § 32 Abs. 2 BSIG
Versorgungsunterbrechung	Bundesnetzagentur (Störungsmeldung), Übertragungsnetzbetreiber	nach Vorgabe
Gefahr für die öffentliche Sicherheit	Polizei, Katastrophenschutz	sofort
Straftat	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarm- und Telefonliste mit ÜNB, Nachbarnetzbetreibern, Monteuren
- Schaltberechtigte und Schlüssel für Ortsbedienung jeder Station
- Offline-Sicherung von Leitsystem, Stationsprojekten und Schutzparametern
- Ersatzleitstelle oder Papierlage mit Netzplänen
- Planspiel zweimal im Jahr, eines mit dem ÜNB

5 Nächste Schritte

- Rollen besetzen, Telefonliste mit ÜNB und Monteuren.
- Playbooks mit Netzbetrieb, Schutztechnik und Hersteller abstimmen.
- Erstes Planspiel mit Szenario U1 und Ortsbedienung aller Stationen.