Krisenstab

Was würdest du tun?

Ein Workshop zum Cyberangriff auf kritische Infrastruktur aus Legal Sicht

Antje Dirlam · Senior Legal Counsel, SBB Infrastruktur ,
Mitglieder der Rechtskommission SwissICT

Das Szenario – «Operation Blackout»*

Montag, 06:47 Uhr

Die Betriebszentrale Olten fällt aus.

> *«Eure Systeme sind verschlüsselt. 8 Stunden. CHF 12 Mio. in Bitcoin.*
> *Andernfalls bleibt Bahnbetrieb blockiert und Daten werden veröffentlicht.»*

40 Züge im Notbetrieb	OT-Leitsystem + HR-Daten verschlüsselt	Medien fragen ab 07:15 Uhr an

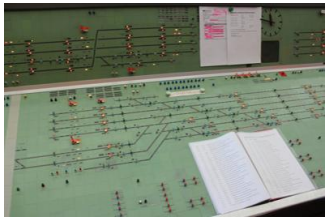
Eingeschleust via IT-Lieferant (Supply-Chain) → OT-Leitsystem | Angelehnt an: DSB / Supeo, DK (2022)

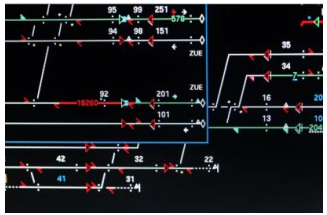
> **Du bist im Krisenstab. Was tust du jetzt?**

**Ein fiktiver Fall, konstruiert zur Veranschaulichung rechtlicher Themen*

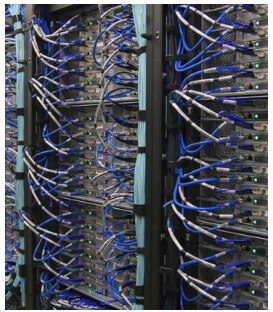
Wenn IT und OT Welt verschmelzen

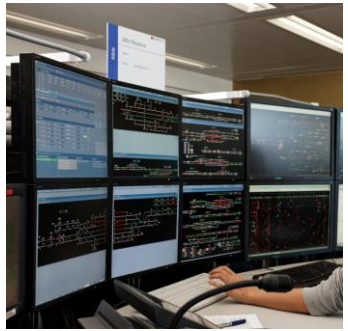
Operational Technology (OT)





Informational Technology (IT)





Warum ist das kein “normaler” Hackerangriff?

OT und IT folgen verschiedenen Regeln – und wachsen immer mehr zusammen.

OT – Operational Technology

Leitsysteme · Stellwerke · Sensoren · Zugsicherung

– Ausfall = physische Konsequenz (Züge stehen)

– Lebenszyklen 20–40 Jahre

– Kein Patching ohne Betriebsunterbruch

– Ursprünglich air-gapped – kein Internet

– Heute: zunehmend vernetzt mit IT

→

IT – Information Technology

· HR-Systeme · E-Mail · Cloud

– Ausfall = Betriebsunterbruch, Datenverlust

– Lebenszyklen 3–7 Jahre

– Regelmässige Updates eingeplant

– Immer netzwerkverbunden

– Klassisches Angriffsziel

Im Szenario: IT-Lieferant ist Einfallstor → Angriff trifft OT-Leitsystem. Konvergenz = neue Rechtsfragen.

Wer sitzt am Tisch?

CEO / GL

Will wissen ob der Betrieb läuft.
Will ein Communiqué für den VR und die Öffentlichkeit.

CISO

Hat nur Fragmentinfos.
Kämpft an der technischen Front.

Legal Counsel

Du – im Raum.
Meldepflichten, Haftung, Strategie.

IT-Lieferant

Sein System war das Einfallstor.
Wartet auf Anweisungen.

Ihr spielt heute alle die Rolle der Legal Counsel – und denkt mit den Augen aller anderen mit.

So läuft es ab

1

3 Runden

Jede Runde = eine neue Etappe. 8 Minuten Diskussion.

2

Eure Entscheide zählen

Was melden wir? Wann? An wen? Bezahlen? Keine Musterlösung – nur gute Argumente.

3

Presentation der Gruppen am Ende jeder Runde 2 Minuten

Wir sehen, wo im Raum Einigkeit herrscht – und wo nicht.

Runde 1 – Montag, 6:48 Uhr | Minute 1 nach der Meldung

8 Min.

Der CISO ruft dich an. Ransomware bestätigt. OT-Leitsystem BLZ Olten teilweise ausgefallen. Weitere Systeme unklar.

8 Minuten

01

Was ist deine erste Handlung als Legal Counsel?

02

Muss die SBB heute Morgen noch jemanden informieren?

03

Was sagst du dem CEO, der jetzt anruft?

2 Min

Kurze Präsentation pro Gruppe

Runde 2 – Montag, 09:00 Uhr | Das Dilemma

8 Min.

CEO: «Die Leute wollen, dass der Betrieb läuft. Können wir nicht einfach bezahlen?»

8 Minuten

04

Bezahlen oder nicht bezahlen?
Deine rechtliche Einschätzung?

05

Wie verändert die Zahlung Haftung und Versicherung?

06

Dein Rat an den CEO – in einem Satz.

2 Min

Kurze Präsentation pro Gruppe

Runde 3 – Montag, 18:00 Uhr | ~ 11h nach dem Ereignis

8 Min.

Der CISO ruft dich an. Ransomware bestätigt. OT-Leitsystem BZ Olten teilweise ausgefallen. Weitere Systeme unklar.

8 Minuten

07

Welche Meldungen müssen jetzt raus? An wen, bis wann?

08

Was schuldet ihr dem IT-Lieferanten – und was schuldet er euch?

09

Medien wollen eine Stellungnahme. Was sagt ihr?

2 Min

Kurze Präsentation pro Gruppe

Rechtsrahmen Schweiz auf einen Blick

Die Antworten – nach eurer Diskussion.

BACS-Meldepflicht

ISG, in Kraft ab April 2025

24h nach Entdeckung · Bei krit. Infrastruktur zwingend · Bussen bis CHF 100'000 (Art. 74g–74h) seit Okt. 2025

DSG Art. 24

Verletzung der Datensicherheit

So rasch als möglich → EDÖB · Hohes Risiko: auch Betroffene informieren · HR-Daten = klarer Anwendungsfall

Strafrecht IT + OT

Art. 143bis / 144bis / 237 StGB

Unbefugter Zugriff, Datenbeschädigung · Art. 237: Störung öffentlicher Verkehr = Gemeingefährdungsdelikt · Beweise sofort sichern

Haftung & Lösegeld

OR / Cyber-Versicherung

Regress gegen IT-Lieferanten prüfen · Lösegeld nicht verboten, aber BACS + Versicherung einbeziehen

Polizei & Strafverfolgung

Kantonspolizei / fedpol / BACS

Strafanzeige bei kantonaler Polizei · fedpol bei internationaler Täterschaft · Koordination mit BACS parallel

Supply-Chain-Haftung

ISG / NIS2-Druck

IT-Lieferanten Teil des Risikomanagements · Cybersecurity-Klauseln und Auditrechte in Verträgen sind Pflicht

3 Dinge zum Mitnehmen

1

Ein Cyberangriff ist ab Minute 1 ein Rechtsfall – nicht erst wenn die Anwälte kommen.

2

OT und IT wachsen zusammen. Die Rechtspflichten gelten für beide – und für alle Lieferanten dazwischen.

3

Das Dilemma «bezahlen oder nicht» ist keine Rechtsfrage, sondern eine Governance-Entscheidung, die ihr vorbereiten müsst.