Sabine Frömling

Wenn Cybersecurity physisch wird.

Unabhängige Beraterin und Fachautorin für OT-Security, industrielle Cybersecurity und KRITIS-Resilienz.

BERLIN / DEUTSCH & ENGLISCH

CSO ONLINE (USA) · COMPUTERWOCHE · IT-DAILY · SPRINGER VIEWEG

DIE PERSPEKTIVE

Die Anlage steht im Mittelpunkt.

Sabine Frömling verbindet industrielle Beratungspraxis mit internationaler Fachpublizistik. Sie macht sichtbar, wie aus digitalen Schwachstellen physische Folgen werden - und welche Entscheidungen Betreiber, Management und Dienstleister treffen müssen.

DREI POSITIONEN, DIE IHRE BEITRÄGE VERBINDEN

01 **Resilienz muss im Betrieb funktionieren.**

Entscheidend sind beherrschter Notbetrieb, vertrauenswürdige Sicherungen und ein getesteter Wiederanlauf.

CSO: Minnesota / Frankreich · it-daily: Inselbetrieb

02 **Auch eine Schutzmaßnahme kann die Anlage stoppen.**

Härtung, Patches und automatische Isolation brauchen Kenntnis der Prozessabhängigkeiten und klare Freigaben.

CSO: Siemens S7 · it-daily: CVSS / Virenschutz

03 **Ein neuer Auftrag kann das Cyberrisiko verändern.**

Geschäftsmodell, Lieferketten und Dienstleisterzugänge gehören in dieselbe Risikobetrachtung.

Computerwoche: Rüstungsproduktion / hybride Angriffe

Positionen für dieses Media-Kit verdichtet; Originalbeiträge auf den folgenden Seiten verlinkt.

Presseanfragen: sabine@froemling.consulting **+49 176 58881995**

Kritische Infrastruktur: USA & Europa

Drei Perspektiven auf eine gemeinsame Frage: Wie bleiben Versorgung und Betrieb handlungsfähig, wenn Steuerungen und Zugangswege angegriffen werden?

WIEDERHERSTELLEN / SICHER VERÄNDERN / RECHTZEITIG REAGIEREN

01

MINNESOTA: WIEDERHERSTELLBARKEIT / 04.08.2026

The Minnesota attackers may hold a better backup of your plant than you do

Angriffe auf Wasserversorger rücken aktuelle Steuerungsprojekte, unabhängige Zugänge und vorbereiteten Handbetrieb ins Zentrum.

Position: Ein Backup zählt erst, wenn damit die reale Anlage wiederhergestellt werden kann.

02

SIEMENS S7: SICHERE HÄRTUNG / 08.09.2026

CISA tells operators to harden Siemens S7 PLCs. Here’s how to do it without disrupting production

Aus einer Behördenempfehlung wird ein kontrollierter OT-Change: Abhängigkeiten prüfen, Ausgangszustand sichern, testen und den Rückweg vorbereiten.

Position: Eine geschlossene Angriffslücke ist kein Erfolg, wenn die Maßnahme zugleich den Prozess unterbricht.

03

FRANKREICH: REAKTIONSFÄHIGKEIT / 20.10.2026

When defrost becomes sabotage: 3 OT lessons from France’s supermarket attack

Manipulierte Kühlregler zeigen, wie reguläre Betriebsfunktionen zur Sabotage dienen können. Entscheidend sind kontrollierte Zugänge und eine wirksame Alarmkette.

Position: Ein Alarm schützt keine Ware, wenn niemand rechtzeitig handeln kann.

Der gemeinsame Maßstab: Bleibt der physische Prozess beherrschbar?

Für Interviews: Notbetrieb, sichere Härtung, Fernwartung und wirksame Reaktion.

Artikelreihe der Autorin, hier thematisch zusammengestellt. Titel führen zu den Originalbeiträgen.

Industrie unter Druck.

Vom europäischen Governance-Problem über den vergessenen Wartungszugang bis zur veränderten Bedrohungslage deutscher Unternehmen.

GOVERNANCE / ZUGÄNGE / GESCHÄFTSMODELL / ABHÄNGIGKEITEN

01

DIE STRUKTURELLE LÜCKE / 26.06.2026

Der blinde Fleck der europäischen Industrie

Zertifikate und Compliance schließen die Lücke zwischen dokumentierter Sicherheit und tatsächlicher industrieller Exposition nicht automatisch.

Position: OT-Risiken brauchen klare Zuständigkeiten und wirksame Entscheidungswege.

02

DER KONKRETE ANGRIFFSWEG / 20.07.2026

Der vergessene Fernwartungszugang

Alte Herstellerzugänge und verwaiste Konten verbinden technische Erreichbarkeit mit organisatorisch ungeklärter Verantwortung.

Position: Ein Wartungszugang braucht einen geregelten Anfang, laufende Kontrolle und ein Ende.

03

DIE NEUE BEDROHUNGSLAGE / 12.10.2026

Wenn die Autofabrik zum Rüstungswerk wird, steigt das Cyberrisiko

Der Wechsel in die Rüstungsproduktion kann neue Angreifer und Schutzziele mit sich bringen, während Anlagen und Dienstleister dieselben bleiben.

Position: Die Sicherheitsbewertung beginnt bei der Auftragsentscheidung.

04

DIE VERNETZTE VERWUNDBARKEIT / 26.10.2026

Wie hybride Angriffe Unternehmen unter Druck setzen

Cyberangriffe, physische Störungen und Desinformation treffen auf gemeinsame Dienste, Lieferketten und betriebliche Abhängigkeiten.

Position: Eine Ausweichlösung muss den gemeinsamen Ausfallgrund tatsächlich umgehen.

Industriesicherheit gehört in Geschäftsentscheidungen.

Für Interviews: Geopolitik, Fernwartung, Verantwortlichkeit und betriebliche Resilienz.

Artikelreihe der Autorin, hier in thematischer Lesefolge. Alle vier Titel sind direkt verlinkt.

Aus Risiko wird Entscheidung.

Die praktische Fortsetzung: Was bedeutet industrielle Cybersecurity für die nächste Schicht, das Wartungsfenster und die nächste Bestellung?

BETRIEB UNABHÄNGIG HALTEN

Kann die Produktion weiterlaufen, wenn die Konzern-IT kompromittiert ist?

Ein Netzsegment belegt noch keinen Inselbetrieb. Zugänge, Lizenzen und Wiederherstellung müssen ohne Konzern-IT funktionieren.

VERANTWORTUNG VERBINDLICH MACHEN

Zehn Maßnahmen für NIS2 in der OT

Aus Sicherheitsanforderungen werden benannte Entscheider, kontrollierte Wartungszugänge und überprüfbare Betriebsverfahren.

SCHUTZ AUF VERTRÄGLICHKEIT PRÜFEN

Wenn Virenschutz den Industrie-PC ausbremst

Auch Sicherheitssoftware braucht einen Betriebstest: Reaktionszeit, Ressourcenbedarf und Verhalten bei einem Fund zählen.

ÄNDERUNGEN NACH RISIKO PRIORISIEREN

CVSS 9,8 und trotzdem nicht zuerst patchen

Reale Zugangswege, Ausnutzung und Prozessfolgen bestimmen die Reihenfolge. Auch der Patch hat ein Betriebsrisiko.

ZUKUNFTSFÄHIGKEIT MITBESTELLEN

Niemand hat der SPS von Post-Quanten-Kryptografie erzählt

Kryptografische Nachrüstbarkeit gehört ins Lastenheft. Ein pauschales Updateversprechen genügt bei langen Anlagenlaufzeiten nicht.

Weitere Beiträge und aktuelle Themen auf it-daily.net

PRAXIS, PUBLIKATIONEN, PERSPEKTIVE

ISMS für die Industrie - Der Praxisratgeber

Springer Vieweg · 2026 · ISBN 978-3-658-52564-4

IT seit 2005 · Beratung seit 2008 · Security-Fokus seit 2020.
Selbstständig seit 2017. MBA der Wirtschaftsuniversität Wien.

Buch und weitere Veröffentlichungen

INTERVIEWS · STATEMENTS · HINTERGRUNDGESPRÄCHE

sabine@froemling.consulting

+49 176 58881995 · Deutsch & Englisch

Pressebereich