Sabine Frömling

Die Brückenbauerin zwischen Regulierung und Werkshalle

Für Medienanfragen:
Sabine Frömling ist unabhängige Beraterin und Fachautorin für industrielle Cybersecurity. Sie erklärt, warum OT-Sicherheit nicht wie klassische IT-Sicherheit gesteuert werden kann – und wie Management, Regulierung und Produktion zusammenfinden.

Kurzprofil

Sabine Frömling ist selbstständige Beraterin für OT-Security-Governance, industrielle Informationssicherheit, ISMS und regulatorische Cybersecurity-Anforderungen. Sie verfügt über mehr als 20 Jahre Erfahrung in IT- und Cybersicherheitsprojekten und verbindet die Sprache von Management, Compliance, IT und Produktion. Ihre Arbeitsschwerpunkte liegen in kritischen Infrastrukturen, produzierender Industrie, Energie, Pharma und technologiegetriebenen Organisationen.

Themen, zu denen ich kurzfristig einordne

OT-Sicherheit & Industrie Risiken in Produktionsumgebungen, Legacy-Systeme, SCADA/IACS, Verfügbarkeit und sichere Veränderungen.	**Regulierung & Governance** NIS2, KRITIS, ISO/IEC 27001, IEC 62443, CRA und prüfbare Verantwortlichkeit.
Cyber-Resilienz Was Anlagen nach einem Angriff noch leisten müssen – und warum Papier-Compliance nicht genügt.	**KI & industrielle Sicherheit** AI Governance, Agentic AI, Abhängigkeiten und der blinde Fleck zwischen digitaler Strategie und Werkshalle.

Kernthesen

„Wer OT-Sicherheit wie IT-Sicherheit steuert, riskiert nicht nur Datenverlust, sondern den Stillstand der Produktion.“

„NIS2 wird erst dann wirksam, wenn aus abstrakten Pflichten belastbare Rollen, Entscheidungen und Nachweise im Werk werden.“

„Eine Anlage ist nicht deshalb resilient, weil ihre Richtlinie aktuell ist. Resilienz zeigt sich in der Fähigkeit, sicher weiterzuarbeiten oder kontrolliert wieder anzufahren.“

„Die größte Lücke industrieller Cybersecurity liegt häufig nicht in einem fehlenden Tool, sondern zwischen Verantwortung, Asset-Realität und Managemententscheidung.“

Kurzfakten

- Über 20 Jahre Berufserfahrung in IT- und Cybersicherheit.
- Selbstständige Beraterin seit 2017.
- Mehr als 50 komplexe IT-Projekte und 25 dedizierte Cybersicherheitsprojekte.
- Schwerpunkte: OT-Security-Governance, NIS2-Umsetzung, ISMS, ISO 27001, KRITIS und Cyber-Resilienz.
- Fachautorin für Computerwoche, CIO.de, CSO Online (USA), kes und it-daily.
- Autorin des Springer-Vieweg-Fachbuchs „ISMS für die Industrie – Der Praxisratgeber“ (618 Seiten; ISBN 978-3-658-52564-4).
- MBA; laufende akademische Weiterbildung im Bereich Management und Sicherheit.

Interview- und Erklärformate

Mögliche Fragen für Interviews, Podcasts, Radio und TV

Warum ist OT-Sicherheit grundsätzlich anders als IT-Sicherheit?

In der Produktion haben Sicherheit, Verfügbarkeit, Safety und physische Auswirkungen eine andere Priorität. Viele klassische IT-Maßnahmen lassen sich nicht ohne Weiteres auf laufende Anlagen übertragen.

Was ist bei NIS2 in der Industrie die größte praktische Herausforderung?

Nicht das Ausfüllen einer Gap-Liste, sondern die Übersetzung in standortbezogene Verantwortlichkeiten, Risikoentscheidungen, Managementberichte und nachweisbare Prozesse.

Warum bleiben Legacy-Systeme ein Problem?

Weil sie oft lange Lebenszyklen, begrenzte Patchbarkeit und hohe Abhängigkeiten haben. Das Risiko muss daher technisch, organisatorisch und wirtschaftlich gesteuert werden – nicht nur durch den Wunsch nach Modernisierung.

Woran erkennt man echte Cyber-Resilienz?

An getesteten Wiederanlauf- und Ausweichverfahren, klaren Entscheidungen und der Fähigkeit, den Betrieb unter eingeschränkten Bedingungen sicher fortzuführen.

Was verändert KI in industriellen Umgebungen?

KI kann Erkennung und Analyse verbessern, erweitert aber zugleich Abhängigkeiten, Identitätsrisiken und Angriffsflächen. Besonders autonome Systeme brauchen klare Grenzen, Überwachung und Verantwortlichkeit.

Was sollten Geschäftsführungen jetzt tun?

Die wichtigsten Anlagen und Prozesse priorisieren, Verantwortlichkeiten klären, Risiken verständlich berichten und Investitionen auf die Betriebsfähigkeit statt ausschließlich auf Compliance-Dokumente ausrichten.

Publikationen und Buch

ISMS für die Industrie – Der Praxisratgeber
Springer Vieweg, 1. Auflage 2026, 618 Seiten. Das Buch verbindet ISO/IEC 27001, NIS2 und industrielle Praxis mit Methoden, Checklisten und Umsetzungshilfen für ein wirksames ISMS in Industrieumgebungen.

Regelmäßige Fachbeiträge erscheinen unter anderem bei Computerwoche, CIO.de, CSO Online (USA), kes und it-daily. Eine englischsprachige internationale Ausgabe ist in Vorbereitung.

Zur Einordnung

Sabine Frömling arbeitet unabhängig und spricht aus der Perspektive einer Praktikerin. Sie gibt keine vertraulichen Informationen aus Kundenprojekten weiter und nennt Kundenunternehmen nur mit ausdrücklicher Freigabe. Für journalistische Anfragen sind kurze Einordnungen, Hintergrundgespräche und Interviews möglich.

Kontakt
Sabine Frömling
sabine@froemling.consulting
froemling.consulting | Mobil: +49 176 58881995
LinkedIn: sabine-froemling

Stand: August 2026. Bitte vor Veröffentlichung von Profil- oder Buchdaten mit dem aktuellen Verlags- und Website-Stand abgleichen.