

Wenn jede Aussage zählt: Beim Cyberangriff souverän und rechtssicher kommunizieren

2. Industrie-Workshop-aus der Reihe 360-Grad-Cyberresilienz in der Industrie – Von der Bedrohung zur robusten Organisation

Industrieunternehmen stehen heute Cyberangriffen gegenüber, die tief in Produktion, Lieferkette und Geschäftsprozesse eingreifen. Die **Workshop-Reihe** richtet sich an Geschäftsführung und Expertinnen und Experten aus IT/OT, Recht, Risiko-, Krisen- und Kommunikationsmanagement im **produzierenden Mittelstand sowie im Anlagen- und Maschinenbau**. Die sich hieraus ergebenden Cyberrisiken werden aus verschiedenen Perspektiven mit einem 360-Grad-Ansatz beleuchtet.

Jeder Workshop verbindet einen **thematisch fokussierten Tandemvortrag** mit einer **praxisnahen Übung**, in der die technische, rechtliche und kommunikative Perspektiven zusammengeführt werden. Im interaktiven Teil stärken die Teilnehmenden ihre Krisenkompetenz, indem sie üben, Risiken realistisch einordnen, kritische Entscheidungen schnell vorzubereiten und Szenarien klar zu durchdenken. Ergänzt werden die Inhalte durch einen kurzen Impuls durch das jeweils gastgebende Unternehmen.



Quelle: Fotolia -Maksim Kabakou

Modul 2: Wenn jede Aussage zählt: Beim Cyberangriff souverän und rechtssicher kommunizieren

Ablauf:

- 1. Impuls Gastgeber: Cyberresilienz bei LAPP – Gemeinsam stark für eine sichere und stabile Organisation**
- 2. Vortrag: Zwischen Meldepflicht und Reputation**

Bei einem Cyberangriff stehen Unternehmen vor widersprüchlichen Erwartungen: Mitarbeitende und Kunden brauchen Orientierung, Behörden verlangen Informationen und Medien schnelle Antworten. Die Geschäftsführung muss entscheiden, was gesagt werden darf. Dazu braucht sie Formulierungen, die rechtssicher sind und zugleich für interne wie externe Zielgruppen verständlich. Verantwortliche stehen im Spannungsfeld zwischen gesetzlicher Absicherung und einer Krisenkommunikation, die die unternehmerische Reputation schützt. Der Vortrag zeigt auf, wie Krisenteams abgestimmt vorgehen, so dass Meldepflichten erfüllt, Gerüchte verhindert und Vertrauen gesichert werden.

3. Interaktiver Teil: Mitarbeitende fragen, Medien rufen an

- Fiktiver Vorfall mit Datenabfluss und Produktionsausfall
- Gruppenarbeit in vier Rollen: GF, Produktion, IT/OT, Kommunikation

- Entscheidungen für Meldewege, Zeitpunkt und Aussagen
- Formulierung eines rechtssicheren Statements für verschiedene Zielgruppen
- Diskussion über sich widersprechende Interessen und wie man sie auflöst

Vortragende:

Stephan Gaenss, Head of Information Security & Riskmanagement, LAPP

Thilo Kohler, Internal Auditor, LAPP

Juliane Fuchs, Business Continuity Manager, LAPP

Rebecca Weiand-Schütt, Senior Consultant mit Schwerpunkt Cyber Krisenkommunikation, Sympra GmbH

Antje Münch, Fachanwältin für Informationstechnologierecht, Partnerin Heuking Kühn Lüer Wojtek

Zielgruppe: Geschäftsführung und Expertinnen und Experten aus IT/OT, Recht, Risiko-, Krisen- und Kommunikationsmanagement im **produzierenden Mittelstand sowie im Anlagen- und Maschinenbau.**

Ort: LAPP Europazentrale, Schulze-Delitzsch-Straße 29, 70565 Stuttgart-Möhringen

Datum und Uhrzeit: 22.10.2026, 14-17 Uhr

Teilnahmebedingungen/Anmeldung:

Die Teilnahme ist kostenfrei, eine Anmeldung ist erforderlich bis zum 10.10.2026 über unser Registrierungsportal: <https://pretix.eu/wrs/cybersecurity4/> Die Teilnehmerzahl ist begrenzt, pro Unternehmen können daher nur bis zu 2 Personen berücksichtigt werden. Die Veranstaltung richtet sich ausschließlich an produzierende Unternehmen.

Weitere Module der Workshop-Reihe:

Modul 3: Cyberangriffe in der Lieferkette: Wie OT-Teams und Kommunikation gemeinsam reagieren (Ort und Termin tbd)

Veranstalter:

Wirtschaftsförderung Region Stuttgart GmbH mit fachlicher Unterstützung des Cyber Competence Centers.

Die Veranstaltung findet im Rahmen des Projekts „Cluster Automotive Region Stuttgart 2.0 – Transformationsnetzwerk für den Fahrzeug- und Maschinenbau (CARS 2.0)“ statt. CARS 2.0 wird durch die Wirtschaftsförderung Region Stuttgart GmbH koordiniert und durch das Bundesministerium für Wirtschaft und Energie gefördert.

Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages