Wirtschaftsförderung Region Stuttgart

:

CYBER COMPETENCE Center

Wenn die Produktion still zu stehen droht: Handlungsfähig in den ersten 24 Stunden eines Hackerangriffs

Auftakt zur Workshop-Reihe *360-Grad-Cyberresilienz in der Industrie – Von der Bedrohung zur robusten Organisation*

Quelle: Fotolia -Maksim Kabakou

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, Risko-, 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.

Modul 1: Wenn die Produktion still zu stehen droht: Handlungsfähig in den ersten 24 Stunden eines Hackerangriffs

Vortrag: **Überblick statt Hektik**
In den ersten Stunden eines Cyberangriffs zählt Übersicht, nicht Aktionismus, damit Unternehmen handlungsfähig bleiben. Krisenmanagement, Incident Response und Kommunikation müssen eng zusammenarbeiten, um unter Zeitdruck ein verlässliches Lagebild zu entwickeln. Auf dieser Basis greifen die Rollen im Krisenteam ineinander – von Werksleitung und IT/OT über die Geschäftsführung bis zum Kommunikationsteam. Der Vortrag zeigt, wie ein abgestimmtes Vorgehen beider Bereiche typische Fehler der Frühphase vermeidet und die Grundlage für strukturiertes Handeln im gesamten Unternehmen legt.

:

Interaktiver Teil: Montag, 6:30 Uhr – Cyber-Angriff wird bemerkt: Abschalten oder nicht?!

- Kurzes fiktives Lagebild mit realistischen Indikatoren
- Kurze Gruppenarbeit in vier Rollen IT, GF, OT/Produktion und Kommunikation
- Gemeinsame Lagebesprechung mit allen vier Rollen zur Lagefeststellung, Lagebewertung und Beschluss von Maßnahmen.
- Ziel: Entscheidung Isolation ja oder nein, Erstellung Aufgabenliste. Erstellung einer internen Erstmeldung.

Referenten:

Dr. Moritz Huber, Geschäftsführer der smartSEC GmbH

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

Zielgruppe:

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

Ort:

Wirtschaftsförderung Region Stuttgart GmbH (Das Gutbrod), Friedrichstraße 10, 70174 Stuttgart

Datum und Uhrzeit:

9.6.2026, 14-17 Uhr

Teilnahmebedingungen/Anmeldung:

Die Teilnahme ist kostenfrei, eine Anmeldung ist erforderlich bis zu 22.5.2025 über unser Registrierungsportal: https://pretix.eu/wrs/cybersecurity3/ Die Teilnehmerzahl ist begrenzt, pro Unternehmen können daher nur bis zu 2 Personen berücksichtigt werden. Die Veranstaltung richtet sich in erster Linie an produzierende Unternehmen aus dem Anlagen- und Maschinenbau sowie der Industrieproduktion. Unternehmen aus diesen Bereichen werden bei der Anmeldung bevorzugt berücksichtigt.

In der Special Interest Group (SIG) „Digitale Werkzeuge“ tauschen sich Unternehmen der Industrieproduktion zu aktuellen Entwicklungen und Erfahrungen mit dem Einsatz digitaler Werkzeuge in der Entwicklung und Produktion aus.

Weitere Module der Workshop-Reihe:

Modul 2: Wenn jede Aussage zählt: Beim Cyberangriff souverän und rechtssicher kommunizieren (Ort und Termin tbd)

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