CYBER|NTELLIGENCE
.Institute

Think visionary.
Act together.
Secure tomorrow.

Informationsangriffe und Fake News gegen Unternehmen: Gefahren und Abwehr

Inhalt der Schulung:
Desinformation, Fake News, Informationsangriffe – das sind längst keine politischen Phänomene mehr! Immer mehr, immer öfter und immer heftiger werden Unternehmen und private Organisationen zur Zielscheibe im Informationskrieg. Die Angreifer können feindliche Staaten, aber auch Unternehmen oder politische Organisationen und Aktivisten im In- und Ausland sein. Neben cyber influence Operationen mit Deepfakes, Bot- und Trollarmeen, kommen hierzu auch immer öfter physische Aktionen wie inszenierte Proteste, Drohungen oder Boykott-Aufrufe. Schätzungen sprachen allein 2022 von rund 78 Milliarden US $ Schaden für Unternehmen durch Desinformation. Und die anhaltende KI-Revolution vervielfacht das Bedrohungspotential.

Die CII-Schulung über Desinformation gegen Unternehmen vermittelt anhand lebensechter Fallbeispiele einen kurzen Überblick über Angriffsvektoren von Informationsattacken gegen Unternehmen. Darauf aufbauend werden für verschiedene Unternehmensbereiche (u.a. Kommunikation und PR) strategische Abwehrkonzepte vorgestellt, Software-Lösungen besprochen und in interaktiven Übungen Lösungen selbst erarbeitet.

Zielgruppen
- Führungskräfte
- CSOs, CISOs, Mitarbeiter der Unternehmens- und Informationssicherheit und Business Intelligence
- Fachkräfte und Mitarbeiter im Bereich KI, Cybersecurity und IT
- Mitarbeiter im Bereich Krisenmanagement
- Presse, PR und Kommunikationsteams

Trainer
Dr. Christopher Nehring, cyberintelligence.institute (CII), Frankfurt am Main

Kursablauf *(in Absprache mit dem Kunden individuell gestaltbar)*

Einführung

- Was sind Desinformation und Informationsangriffe?
- Aktuelle Bedrohungslage und Schaden

Modul 1: Angriffsvektoren

- 10 Angriffsarten gegen Unternehmen
- Fallbeispiele
- China und Russland: Staatliche geförderte Informationsangriffe gegen die deutsche Wirtschaft
- Informationsangriffe & Cyber Influence als private Dienstleistung

Modul 2: Abwehr und Lösungen

- Ganzheitlicher Ansatz
- Passive und aktive Lösungen
- 3-Stufen-Modell
- Best Practice
- Übung: Strategische Kommunikation
- Software-Lösungen
- Übung: Sicherheitskonzept erarbeiten

Der Kurs wird nur remote/online angeboten.

Teilnehmer: 20 max.

Dauer: durchführbar als deep dive von 2 Stunden (nur online), interaktiver Halbtages-Workshop (4 Stunden) und interaktiver Ganztags-Workshop mit praktischen Aufgaben und Lösungskonzepten

Kontakt

cyberintelligence.institute

MesseTurm
Friedrich-Ebert-Anlage 49
D-60308 Frankfurt am Main

www.cyberintelligence.institute
info@cyberintelligence.institute
+49 69 505034602