CYBER|NTELLIGENCE
.Institute

Think visionary.
Act together.
Secure tomorrow.

Russische Geheimdienste gegen die deutsche Wirtschaft: Das Einmaleins der russischen Spionage in Deutschland

Inhalt der Schulung:
Hybride Angriffe gegen deutsche Unternehmen und Organisationen nehmen in den vergangenen Jahren signifikant zu. Dieses CII-Training vermittelt einen Überblick über Taktiken, Techniken und Prozeduren (TTPs) russischer Geheimdienste im Bereich Industrie- und Wirtschaftsspionage, Sabotage und hybride Bedrohungen. Es bietet einen umfassenden Überblick über operative Ansätze wie „aktive Maßnahmen“ und hybrider Taktiken, die Nutzung von Stellvertretern und Innentätern sowie grundlegende operative Taktiken bei der Anwerbung von Agenten. Besonderes Augenmerk wird auch auf die Mentalität und Organisationskultur russischer Geheimdienste gelegt, um Rückschlüsse und Einblicke in Strategien und Taktiken zu geben. Diese Inhalte werden anhand von realen und lebensechten Beispielen vorgestellt. Neben dem Vorgehen wird so ein umfassendes Risiko-Mapping erstellt. Ziel des Trainings ist es, das strategische wichtige Bewusstsein und die Resilienz gegenüber hybriden Bedrohungen zu stärken und die Teilnehmer zu befähigen, präventive und reaktive Maßnahmen zu ergreifen.

Zielgruppen
- Führungskräfte (insb. im Bereich KRITIS)
- CSOs, CISOs, Mitarbeiter der Unternehmens- und Informationssicherheit und Business Intelligence
- Fachkräfte und Mitarbeiter im Bereich KI, Cybersecurity und IT
- Mitarbeiter im Bereich Krisenmanagement

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

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

Einführung
- Warum Spionage und hybride Angriffe?
- Aktuelle Bedrohungslage und Schaden
- Russische Geheimdiensttradition: Strategische Ziele und Motive

Modul 1: Angriffsvektoren
- Überblick über Angriffsarten und Bedrohungszenarien
- Fallbeispiele für Cyberangriffe, Desinformation und Spionage
- China und Russland: Staatliche geförderte Informationsangriffe gegen die deutsche Wirtschaft
- Wie werben russische Geheimdienste Agenten an?
- Psychologische Kriegsführung
- (Alltags-)Sabotage
- Technologie und Hilfsmittel

- Modul 2: Abwehr und Lösungen
- Schutzkonzepte
- Physische Sicherheit
- Cybersicherheit
- Spionageabwehr
- Geheimnisschutz
- Technologie
- Faktor Mensch im KI-Zeitalter

Der Kurs kann remote/online oder präsent durchgeführt werden!

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