3787 Cyber Security Praxis-Check

Cybercrime im Unternehmensumfeld und wie man sich gemäß der NIS 2 Richtlinie davor schützt

In diesem Seminar erlernen die Teilnehmerinnen und Teilnehmer wichtige Kompetenzen, um ihr Unternehmen vor Cyberangriffen zu schützen. Die Teilnehmenden lernen verschiedene Angriffsformen und -wege kennen und diskutieren konkrete Fallbeispiele.

Welche Schritte sind im Falle eines Angriffs zur Schadensbegrenzung erforderlich und welche Meldepflichten bestehen. Die Teilnehmenden erarbeiten gemeinsam eine Checkliste mit To-Do's.

Die Schulung umfasst diverse Maßnahmen zur präventiven Schadensbegrenzung und Minimierung der Angriffsvektoren. Dazu gehören Mitarbeiterschulungen, technisch-organisatorische Maßnahmen (TOMs), Cyber-Versicherungen und die Simulation von möglichen Angriffen durch White-Hacking, Pen-Testing und Cyber-Ranges.

Die Teilnehmenden erarbeiten ein Konzept für ihr Unternehmen, das spezifische Maßnahmen zur Vorbeugung von Cyberangriffen beinhaltet. Dabei werden individuelle Unternehmensbedürfnisse und -anforderungen berücksichtigt.

Am Ende des Seminars verfügen die Teilnehmenden über das notwendige Wissen und die praktischen Fähigkeiten, um ihr Unternehmen effektiv gegen Cyberangriffe schützen zu können und ein Präventionskonzept zu erarbeiten.

Die Inhalte:

- Sicherheitsniveau von Netz- und Informationssystemen (NIS-Richtlinie) und dessen Bedeutung
- Aktuelle Bedrohungen und neueste Entwicklungen in der Cyberkriminalität, Angriffsformen und -wege, Falldiskussionen mit Beispielen.
- Übersicht aktueller Standards und Normen
- Gefährdungsbewertung, Umgang mit Dienstleistern und Lieferanten
- Reaktion auf Cyberangriffe: Was ist bei einem Angriff zu tun? Schadensbegrenzung, Krisenmanagement, Checklisten mit To Do's, Meldepflichten
- Prävention: Maßnahmen zur präventiven Schadensbegrenzung, Minimierung der Angriffsvektoren (Mitarbeiterschulung, div. TOM's (technisch-organisatorische Maßnahmen), Versicherung ..., mögliche Angriffe üben/simulieren (white hacking, Pen-testing, Cyber-Range). Interne Prüfungshandlungen
- Erarbeitung eines Präventionskonzeptes für Cyberangriffe ausgearbeitet
- Effektivitätsbewertung der Sicherheitsmaßnahmen

Ziel:

- Ziel dieser Veranstaltung ist es, eine Übersicht zu schaffen, welche Bedrohungen Unternehmen aktuell ausgesetzt sin, wie sie auf Angriffe reagieren sollen und wie sie durch Präventivmaßnahmen die Auswirkungen auf Ihr Unternehmen reduzieren können.

Hinweis:

Dieser Kurs wurde in Abstimmung mit dem Kompetenzzentrum Sicheres Österreich (KSÖ) entwickelt.