IT-säkerhet för chefer

KURSPLAN

Kapitel 1: Introduktion till IT-säkerhet för chefer

- ✓ Vad är IT-säkerhet? – Grundläggande begrepp och vikten av ledarskap
- ✓ Digitala hotbilder idag – aktuella trender och scenarier
- ✓ Chefers ansvar för säkerheten – strategiskt och operativt
- ✓ Förstå organisationens värde och sårbarheter
- ✓ Nyckeln till en säker verksamhet: Ledarskap, kultur och medvetenhet
- ✓ Övningsuppgifter

Kapitel 2: Kännetecken och typer av cyberhot

- ✓ Vanliga attacker och attackerarnas motiv
- ✓ Olika hottyper: Ransomware, botnet, social engineering, phishing
- ✓ Hur attacker sker: Metoder och taktiker
- ✓ Medarbetarnas roll och identitetsskydd
- ✓ Identifiera och känna igen en attack i tid
- ✓ Övningsuppgifter

Kapitel 3: Säkerhetsåtgärder och teknik för ledare

- ✓ Säkerhetsrutiner och policys för hela organisationen
- ✓ Uppdateringar, patchning och systematiskt underhåll
- ✓ Säkra lösenord och tvåfaktorsautentisering
- ✓ Molntjänster och datahantering
- ✓ Användning av sociala medier och policys för medarbetare
- ✓ Säker användning av smartphones och tablets
- ✓ Övningsuppgifter

Kapitel 4: Hantering av incidenter och krishantering

- ✓ Hur märker företaget att en attack pågår?
- ✓ Agera och återställa: Steg för att hantera incidenter
- ✓ Backupstrategier och redundans
- ✓ Kommunikation vid incidenter – intern och extern
- ✓ Förebyggande arbete mot ransomware och andra hot
- ✓ Övningsuppgifter

Kapitel 5: Strategi och framtidssäkring

- ✓ Att skapa en säkerhetskultur inom organisationen
- ✓ Utbildning och medvetenhetsfrämjande insatser
- ✓ Regelbundna riskbedömningar och tester
- ✓ Policy för distansarbete och användning av privata enheter
- ✓ Framtidens IT-säkerhet: Trender och innovationer
- ✓ Att leda digitalt och säkert i en föränderlig miljö
- ✓ Övningsuppgifter