Security Awareness Training

Schutz gegen Cyberkriminalität

mITSM
Wir verändern durch Wissen.

Dauer

Halbtägig

Location

Firmen-Inhouse (Präsenz und Online Live)
Präsenztrainings in München und Köln
Online Live

Inhalte

- Motivation und Einführung
- Grundlagen im Informationssicherheits-Management
- Grundlagen im Datenschutz
- IT-Security: Grundlagen, gängige Angriffe und Sensibilisierung
  - Schadsoftware
  - Infektion via E-Mail
  - Phishing
  - Social Engineering
  - Vishing
  - Drive-By-Download
  - Botnet
  - Fake-Gewinnspiele
  - Nicknapping
  - Dumpster Diving
  - USB-Sticks
- Sichere Passwörter
- Gegen- und Abwehrmaßnahmen

Das Security Awareness Training kann auch zum Nachweis der Mitarbeiterschulung im Rahmen von Unternehmenszertifizierungen oder von Cyber-Security-Versicherungen dienen.

Ziele und Nutzen

Unsere Security Experten sensibilisieren die Teilnehmer anhand konkreter Szenarien für den Schutz der Unternehmens-Assets vor Cyber-Attacken. Sie lernen, Bedrohungen rechtzeitig zu erkennen und in den entsprechenden Situationen richtig darauf zu reagieren.

- Wie lassen sich die von Mitarbeitern verursachten Gefahren für die Informations- und IT-Sicherheit minimieren?
- Mit welchen Arten von Sicherheitsangriffen müssen Mitarbeiter rechnen?
- Woran lassen sich Cyber-Attacken erkennen?
- Wie reagiert man richtig darauf?
- Wie ist man bei Passwörtern, E-Mails, mobilen Geräten, sozialen Netzwerken etc. auf der sicheren Seite?

Zielgruppe

- Für alle, die mit digitalen Systemen arbeiten

Mehr Information unter
www.mitsm.de/security-awareness

Optional: Social Engineering Pentest

Zur Überprüfung des Lernerfolgs und für die weitere Sensibilisierung kann das Training mit Social Engineering Pentests kombiniert werden. Hierbei sollen die Mitarbeiter beispielsweise mit E-Mails und maßgeschneiderten Websites zur Herausgabe von Passwörtern verführt werden.

Mehr Informationen unter
www.mitsm.de/social-engineering-pentest