

Security Awareness Training

Schutz gegen Cyberkriminalität



mITSM

Wir verändern durch Wissen.

Dauer

- 1/2 Tag

Format

- Firmen-Inhouse (Präsenz und 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-Attacks. 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-Attacks 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: Phishing Kampagne

Zur Überprüfung des Lernerfolgs und für die weitere Sensibilisierung empfiehlt sich eine daran anschließende Phishing-Awareness-Kampagne. Damit sollen Mitarbeitende mit Hilfe von E-Mails und maßgeschneiderten Websites dazu verführt werden, auf Links zu klicken, Anhänge zu öffnen oder Passwörter preiszugeben.



Mehr Informationen unter

www.mitsm.de/phishing

