Digitale Sicherheit für den Mittelstand eG | Markt 25 | 09648 Mittweida

Telefon: +49 3727 99 72 311
www.digitale-sicherheit-mittelstand.de

Security Awareness

Social Engineering verstehen und Hacker-Angriffe abwehren

Durch die Digitalisierung erhalten alte Angriffsmuster aus dem Bereich Social Engineering eine neue und größere Bedeutung. Cyberkriminellen wird durchzunehmende Vernetzung eine größere Angriffsfläche geboten, welcher Hacker nutzen, um in Unternehmensnetze einzudringen und an relevante Informationen zu gelangen. Hierbei kann der Angreifer oftmals auf eine Vielzahl von öffentlichen Informationen zurückgreifen und so authentische Phishing-Mails verfassen. Die Betroffenen erkennen solche Angriffe selten und öffnen dem Hacker die Tür ins Unternehmen.

Ihre Vorteile auf einen Blick

Nach dem Seminar können Sie ...
... Social Engineering Angriffe erkennen
... Angriffsvektoren analysieren und bewerten
... den Umgang mit Informationen verbessern und somit Social Hacking Angriffen vorbeugen
Das Seminar bietet Ihnen ...
... Praxisbeispiele aus der Welt des Social Engineering
... einen Überblick über Manipulationstechniken
... Übungen zur Selbstreflexion und Analyse eigener Schwachstellen

Inhalt	Session 1: Grundlagen des Social Engineering Kennenlernen der Begrifflichkeiten Überblick aktueller Angriffsvektoren Psychologische und soziale Einflussfaktoren Session 2: Social Engineering verstehen und abwehren Informationsgewinnung zur eigenen Person Maßnahmen zur Abwehr eines Angriffs im Unternehmen oder im Home-Office Schutz vor Phishing
Dauer	3 Stunden
Kurssprache	Deutsch
Lernziel	-Eine Sensibilisierung für die Gefahren durch Social Engineering -Kennenlernen von Werkzeugen zur systematischen Informationserfassung bezogen auf Einzelne und ganze Unternehmen -Verstehen der psychologischen Einflussfaktoren -Schutzmaßnahmen gegen Social Engineering-Angriffe
Zielgruppe	-öffentlich wirksame Personen -Management -Fachkräfte -Anwender -Selbstständige
Teilnahmegebühr	199,00
Voraussetzungen	Problemloser Umgang mit dem PC. Für das Webinar wird der Firefox oder Google Chrome Browser empfohlen.