

IT-Security und der Risikofaktor Mensch

(Seminar-Beschreibung)

Inhaltlicher Ansatz

Die Zahl der Viren, Würmer und Trojaner steigt täglich. Gegen diese Form eines Angriffs schützen sich Unternehmen mit verschiedenen technischen Mitteln. Doch das alles ist nur Makulatur, wenn der Angriff auf die Firmeninterna von den eigenen Mitarbeitern (unfreiwillig) unterstützt wird.

Eine der effektivsten Angriffsvarianten auf vertrauliche Informationen wird von freundlichen und höflichen Menschen durchgeführt. Getarnt als Kollege, Führungskraft aus einer anderen Abteilung oder Mitarbeiter einer anderen Filiale gelangt der „Social Engineer“ oft problemlos an Interna: Von der Telefonliste, über Protokolle bis hin zum Quellcode. Im Seminar werden verschiedene Angriffsvarianten auf unterschiedlichen Ebenen vorgestellt.

Das Trainingsangebot gliedert sich in zwei Bereiche:

Modul 1: Computer Based Social Engineering

Hier geht es sowohl um die technischen Ebenen eines Angriffs, als auch um die kommunikativen Angriffsvarianten. Im Seminar werden verschiedene technische Varianten vorgestellt. z.B. Phishing-Mails, Pop-up-Fenster, falsche Links, Homepagekopien, Passwörter entschlüsseln, Keylogger, etc. Eingebunden werden diese Beispiele in Kommunikationssituationen aus dem Alltag.

Zielgruppe:

Diese Kombination von Technik (mit Praxisanteil) und Kommunikation wendet sich an Geschäftsführung, Abteilungsleiter und IT-Beauftragte.

Dauer: 1 Tag

Modul 2: Human Based Social Engineering

Hier geht es vor allem um die Kommunikationstechniken eines SE-Angriffs: Vorbereitung eines Angriffs, Szenario-Aufbau, Fragetechniken, Umfrage und Auswertung, etc. Die Technikebene wird nur in Form eines bebilderten Kurzvortrages vorgestellt. Eine praktische Demonstration eines Angriffs findet nicht statt.

Zielgruppe:

Der zweite Teil des Seminars ist für alle Mitarbeiter eines Unternehmens von Bedeutung, da hier die Akzeptanz für Kommunikations/ Security-Spielregeln aufgebaut wird.

Dauer: 1 Tag

In beiden Seminar-Modulen werden die Vorgehensweise und Mittel des Social Engineering mit unterschiedlichen Schwerpunkten vorgestellt. In einfachen Rollenspielen werden verschiedene Angriffs-Szenarien durchgespielt. Am Ende des Seminars werden mögliche Sicherheitsrichtlinien vorgestellt und diskutiert.

IT-Security und der Risikofaktor Mensch

(Seminar-Beschreibung)

Ablaufelemente: (gilt für beide Module)

- Einführung ins Thema
- Was ist Social Engineering?
- Erfolgreiche Angriffe
- Ein Angriff im Detail
 - Der Kommunikations-Part
 - Technische Umsetzung (Bei Modul 1 mit Demonstration)
- weitere Angriffs-Varianten
- Sicherheitshinweise

Bemerkungen:

Jeder Teilnehmer lernt die Techniken und Methoden des Social Engineering kennen. In verschiedenen Situationen wird der Umgang mit diesen Angriffen auf vertrauliche Informationen trainiert und die Angst abgebaut, etwas falsch zu machen. Tipps und Tricks für den Notfall runden das Seminar ab.

Das Seminar eignet sich zur Einführung in das Thema und zur Sensibilisierung der Mitarbeiter. Zielgruppen sind letztlich alle Mitarbeiter eines Unternehmens: von der Empfangsdame bis zum Vorstand. Für neue Mitarbeiter oder als Auffrischung bietet sich als Variante ein Vortrag zum Thema an.