IT-Sicherheit im Home-Office Administrative & rechtliche Aspekte

Überblick

Die Gefährdungslage für die IT-Infrastrukturen von Unternehmen und Behörden hat sich in den letzten Jahren stetig weiter verschärft. Bedingt durch die Corona-Krise sahen sich zudem viele der Unternehmen und auch Institutionen gezwungen, ihre Mitarbeiter zum Schutz vor möglichen Virus-Infektionen, aber auch wegen der durch die Bundesregierung empfohlenen Ausgangsbeschränkungen von zu Hause aus arbeiten zu lassen. In der Praxis hat sich gezeigt, dass viele der Unternehmen auf die neue Herausforderung der Bereitstellung sogenannter „Home-Office“-Arbeitsplätze jedoch überhaupt nicht - oder zumindest nicht ausreichend - vorbereitet waren. Die damit verbundenen Schwachstellen in der IT-Sicherheit wurden durch potentielle Angreifer recht schnell erkannt, und für diverse, teils auch durch die tägliche Presse bekannt gewordenen Hackerangriffe auf Unternehmensdaten missbraucht. Dieser Umstand zwingt die IT-Verantwortlichen und -Administratoren zum Bereitstellen „sicherer“ Home-Office-Arbeitsplätze.

In diesem Workshop erhalten Sie einen Überblick über aktuelle Bedrohungen für die modernen IT-Infrastrukturen, sowie die Daten von Unternehmen und Behörden, die teils auch direkt von den „Home-Office“-Arbeitsplätzen ausgehen können. Dies umfasst neben den technischen Möglichkeiten auch wichtige Tipps zu den möglichen Gegenmaßnahmen, um Schäden durch Hacker-Angriffe zu vermeiden.

Dauer:
3 Tage

Preis:
1.790,00 € (2.130,10 € inkl. MwSt.)

Kursinhalt

Einführung

- Technische Trends und Entwicklungen
- Überblick über erfolgreiche Hacker-Angriffe auf deutsche Unternehmen
- Gründe für die Angriffe auf Unternehmensdaten und -infrastrukturen

- Arten und Motivation der Angreifer
- Phasen eines (geplanten) Hackerangriffs
- Opfersuche - Informationsquellen für Angreifer im Internet
- Aktuelle Angriffsmethoden

Angriffe auf Unternehmensdaten – der „indirekte Weg“ über das Home-Office

- Die verschiedenen Arten von Sicherheitsbedrohungen
- Home-Office als „Türöffner“ – der „indirekte“ Weg in das Firmennetzwerk
- Social Engineering-Angriffe – „Feinde unter uns!“
- Angriffe mittels E-Mails, Malware und Office-Makros
- Windows PowerShell unter Windows 10 – aus Sicht der Angreifer
- Infektion mit Trojaner-Programmen und Ransomware
- Angriffe auf Drahtlosnetzwerke (WLAN) im Home-Office
- Fallbeispiele für potentielle Angriffe

Home-Office ja – aber sicher!

- Überblick über Schutzmethoden und -maßnahmen
- Ausstattung im Home-Office zur Absicherung vor Angreifern
- Windows 10-Computer im KIOSK-Modus
- Möglichkeiten – und Einschränkungen im Zusammenhang mit „BYOD“
- Remote-Zugriffsmöglichkeiten mittels RDP, VPN und Co.
- Authentifizierungsmethoden – Vor- und Nachteile
- Verwendung „sicherer“ Kennwörter - sind Sie und die Unternehmensdaten wirklich „sicher“?
- Konfiguration und Einsatz von Desktop-Firewalls im Home-Office
- Sicherer Internet-Zugang vom Home-Office mittels Proxy-Server, Download- und Inhaltsfiltern
- Einsatz von Viren-, Malware- und Ransomware-Schutzfunktionen
- Verhindern von Datenverlust – Stichwort: „Data Loss Prevention“ (DLP)
- Remote-Unterstützung mittels TeamViewer, LogMeIn, AnyDesk & Co.
- Remote-Verwaltung der Home-Office-Geräte – Lösungen im Vergleich
- Vergleich verschiedener Mobile Device Management (MDM)-Lösungen
- Schutz durch Sensibilisierung und Schulung
- Rechtliche Aspekte

Voraussetzungen

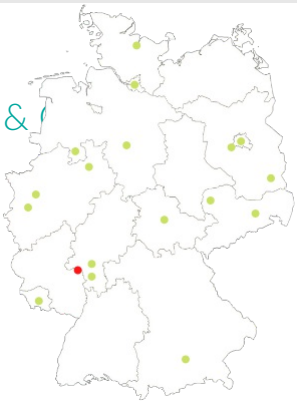
Grundlegende Kenntnisse und Fähigkeiten in der Bereitstellung und Verwaltung moderner

Computersysteme.

Zielgruppe

Dieser Workshop richtet sich sowohl an Administratoren, System- und Netzwerkverwalter, IT- und Systemverantwortliche, sowie IT-Sicherheitsbeauftragte.

Ihr Weg zu uns



Com training and services in Mainz / Wiesbaden AWMa GmbH &

Binger Straße 14 - 16

55122 Mainz

Phone: +49 6131 90705-0

Email: com@awma.de