SEM538

Netzwerke und Sicherheit

Sicherheit in Netzwerken analysieren und umsetzen

Ihr Nutzen aus diesem Kurs:

In diesem **herstellerneutralen Intensiv-Kurs** erhalten Sie einen Überblick über die wesentlichen Aspekte der Sicherheit in Netzwerken und lernen die IT-Sicherheit von Netzwerken aus der Sicht unterschiedlicher Gruppen, wie Management, Administratoren und Benutzer, zu betrachten. Außerdem zeigen wir Ihnen warum eine **Analyse der möglichen Gefahren und des Bedarfs für Sicherheit** nötig ist und wie Sie bei einer Abschätzung des Risikos und beim Planungsablauf von IT-Sicherheitsmaßnahmen vorgehen müssen. Danach sind Sie mit den wesentlichen technischen und organisatorischen Maßnahmen vertraut, mit denen bestimmte Sicherheitsbedrohungen bekämpft werden können.

Seminarprogramm:

Ethernet-Netze

- IP-Adressen, Subnetze, Routing, IPv4 vs. IPv6, Protokolle

Was ist Sicherheit?

- Grundforderungen, rechtliche Aspekte
- Sicherheitsziel Vertraulichkeit, Integrität und Verfügbarkeit

Risikolage für Unternehmen

- Schadensmöglichkeiten, Abhängigkeit

Angriffsvorbereitung

- Hacker, Cracker und Script-Kids
- "Staatliche" Hacker, elektronische Kriegsführung
- Netzwerkscans, Wardriving, Social Engineering

Angriffe auf Serverdienste

- Exploits, Rootkits, DoS/DDoS/DRDoS
- Sniffer, Replay-Attacken, TCP/IP Session-Hijacking

Sicherheitsprobleme durch Mitarbeiter

- Ausfall/Krankheit, mangelnde Kompetenz
- Unrechtmäßige Systemzugänge, Spionage

Virenarten und ihre Verbreitung

- Grundkonzepte, Virenarten, Tarnmechanismen
- Würmer, Trojaner, Hoaxes

Spyware, Phishing und Browser Hijacking

Standalone-Virenschutz

IT-Sicherheitsstandard

- Standards, IT-Grundschutz-Katalog, Security Policy

Symmetrische Kryptografie

- Das Problem von Alice und Bob
- Verschlüsselungsmethoden

Asymmetrische Kryptografie

- Nachteile symmetrischer Verfahren
- Diffie-Hellman, El-Gamal
- RSA, Digitale Signatur, Hashfunktionen, PKI

Kryptografische Protokolle und ihre Anwendung

- SSL/TLS, SSH, IPsec, SET/HBCI

Sichere E-Mail-Verfahren

- Schlüssel generieren, Schlüsselexport und -import
- Signieren von Schlüsseln, E-Mails und Dateien

Firewalls

- Paketfilter- und Stateful Inspection Firewall
- Proxy Level/Application Level Firewall
- NAT, Personal Firewall

Intrusion-Detection-Systeme

- Notwendigkeit und Arbeitsweise
- Intrusion-Prevention-Systeme (IPS)
- Snort, Honeypot-Netzwerke

Virtual Private Network

- PPTP, L2TP/IPsec, OpenVPN
- Abgrenzung zu anderen VPN-Arten

WLAN und Sicherheit

- Arbeitsweise, Access-Points, WEP, WPA, WPA2
- Weitere Authentifizierung und Verschlüsselung

Alternative Software

Authentifizierungssysteme

- Kerberos, PAP, CHAP, EAP und RADIUS
- Smartcards und Tokensysteme, Biometrie

Proaktive Sicherheit

- Gehärtete Betriebssysteme, Patches
- Vulnerability Assessment
- Aktive Sicherheit von Netzwerkkomponenten

Praktische Übungen:

Die gesamte Thematik wird in vielen praktischen Übungen gemeinsam bearbeitet.

Kursdetails:

Dauer: 5 Tage

Termine:

- 

  

  08.10.-12.10.2018
  Basel
  Anmelden Reservieren

-

05.11.-09.11.2018
Bonn
Anmelden Reservieren

- 

14.01.-18.01.2019
Bern
Anmelden Reservieren

- 

28.01.-01.02.2019
München
Anmelden Reservieren

- 

08.04.-12.04.2019
Hamburg
Anmelden Reservieren

Durchführung:

- Garantiert ab 3 Teilnehmern
- Maximal 8 Teilnehmer

Enthaltene Leistungen:

- Schulungsunterlagen
- Teilnahmebescheinigung
- reichhaltiges Mittagessen
- 2 Kaffeepausen
- Erfrischungsgetränke

Teilnahmegebühr:

- 2.995,- EUR / 3.595,- CHF
  (zzgl. gesetzl. MwSt)

Weitere Optionen:

- Weitere Termine
- Individuelle Firmenschulung
- Einzelcoaching

Haben Sie Fragen?

Gerne beraten wir Sie persönlich per Telefon oder per E-Mail.

IFTT Service-Line:
+49 (0)69 - 78 910 810

E-Mail:
info@IFTT.de