

Network Security (NES)

Die Datensicherheit im Unternehmensnetz ist von entscheidender Bedeutung für geschäftskritische Prozesse. Jeder Netzverantwortliche muss in der Lage sein, möglichen Gefährdungen schon bei der Planung vorzubeugen.

Das gilt für die Netzanbindung in der Office- wie auch in der Industriewelt, wo der Einzug der IP-Technologie bislang getrennte Bereiche zunehmend verbindet.

Zielgruppe

Planer, Nutzer und Betreuer von IT-Systemen sowie alle am Netzaufbau beteiligten Entscheider.

Voraussetzungen

Grundkenntnisse im Bereich der Netzwerktechnik sind wünschenswert, aber nicht zwingend erforderlich.

Zielsetzung

Die Teilnehmer dieser Einführung erfahren, welchen Gefahren und Bedrohungen IT-Systeme ausgesetzt sind, und lernen so, bei der Netzplanung und späteren -betreuung Schwachpunkte rechtzeitig zu erkennen.

Darüber hinaus wird aufgezeigt, welche Maßnahmen und Verfahren sinnvoll eingesetzt werden können, um die IT-Sicherheit nachhaltig zu erhöhen.

Inhalt des Seminars

Security-Grundlagen

- Bedrohungsanalyse
- Kosten-Nutzen-Überlegungen
- Schutzmaßnahmen
- Sicherheitsprozess
- Zertifizierungen
- Besondere Randbedingungen in Produktionsnetzen

Netzwerk-Grundlagen

- Netzwerkkomponenten
- TCP/IP-Grundlagen
- Subnetting
- ICMP, UDP, TCP
- IP-Routing

Protokolle

- HTTP/HTTPS
- Telnet
- SSH
- DNS
- TFTP, FTP
- POP3, SMTP, SNMP

Angriffsszenarien

- Phasen eines Angriffs
- Footprinting
- Würmer, Viren und Trojaner
- Spoofing
- DoS/DdoS-Attacken

Sicherheitslösungen

- VLAN
- Accesslisten (ACL)
- Network Address Translation (NAT)
- Firewall
- Intrusion Detection
- Content Security
- Planungsbeispiel einer Firewallumgebung

Einführung Kryptografie

- Ziele und Methoden
- Kryptoanalyse, Kryptografie und Steganografie

Symmetrische Verschlüsselungs-Algorithmen

- ECB/CBC
- DES, 3DES, IDEA, AES, RC5, Blowfish
- Schlüsselmanagement

Asymmetrische Verschlüsselung

- Public/Private Key
- RSA
- Diffie-Hellman
- ECC

Hash-Funktion

- MD5, SHA-1, RIPEMD
- MAC

Sicherheit und Anwendung von Algorithmen

- Sichere Schlüssellänge und Algorithmen
- Hybride Verschlüsselung
- Key Recovery Verfahren
- Key Encapsulation, Key Escrow, Key Backup
- Digitale Signatur

Authentifizierungsverfahren

- RADIUS
- PAP/CHAP
- Kerberos
- SecurID
- LDAP
- PKI
- X.509

Verschlüsselungsprotokolle und VPN

- SSL und TLS
- VPN-Verbindungen
- Site-to-Site, Site-to-Client
- Layer-2- und Layer-3-VPN
- IPSec, IKE

Sprachversionen:

NESd deutsch

Dauer:

2 Tage
je 9.00 – 17.00 Uhr

Preis:

1.100 € zzgl. MwSt.

Termine / Ort:

siehe beiliegende Übersicht oder
www.hicomcenter.com