

...

FIREWALL & VPN

Sicherheit in ihrem Computernetz

- iloveyou
- Viren
- Trojaner
- Vandalen
- Hacker
- DoS
- Hijacking
- Snooping

Was kann man dagegen tun ?



ISBN: 3-8007-2621-1

FIREWALL & VPN

Dauer 1 Tag

Seminarziel:

- Eine detaillierte Einführung in die moderne Technik zur Absicherung von Netzwerken
- Planungsinformationen für mehr Sicherheit
- Aufzeigen von aktuellen Schutztechniken
- Übersicht der am Markt gängigen Produkte

Zielgruppe:

- Unternehmensberater
- Systemadministratoren
- Planer von Computernetzen
- Anwender, die mehr erfahren wollen

Referent:

- Dipl.-Ing. Peter Jöcker
Senior Network Consultant
Cisco Certified Network Security Specialist
- Buchautor „Computernetze“ (32,- EUR)
ISBN 3-8007-2621-1 (VDE-Verlag, 2001)

Lehrmethode:

- Vortrag, Diskussion, Handout

Inhalt:

- **Authentication (Login)**
 - Router-Strecken, RAS-Einwahl, CLI, VPN
 - Radius, Password-Server, Token-Card
- **Encryption (Verschlüsseln)**
 - Zwei gängige Verfahren: 3DES und RSA
 - Secret-Key arbeitet nur mit einem Schlüssel
 - Public-/Private-Key funktioniert mit zwei Schlüsseln
 - verschlüsselt durch Internet: SSL, HTTPS, VPN, IPsec
- **Signatur (Unterschrift)**
 - verschlüsselte und signierte E-Mails dank PGP
 - PKI-Verfahren: PGP und X.509, Certified-Authority
- **VPN (verschlüsselte Verbindungen)**
 - Tunnel mit Ipsec, IKE, ISAKMP, Pre-Shared-Key
- **Firewall (geprüft nach ISO 15408 EAL)**
 - eine Firewall ist immer ein Konzept und kein Produkt
 - Secure-Policy, Def.-Gate, Content-Proxy, URL-Blocker
 - NAT-Router, Regeln für diesen Perimeter-Router
 - DMZ mit Mail-Relay und Content-Scanner
 - Auditing (Prüfung) und Intrusion-Detection
- **TOS und Orange-Book**
 - sichere Betriebssysteme (nur auf Unix-Basis)
- **Risiken**
 - Viren, Würmer, Trojaner und Vandalen
 - gegen Hijacking und Snooping
 - Hacker mit Denial of Service