Inhalt – IT-Sicherheitsarchitekturen

- Grundlegende Begriffe der IT-Sicherheit
- Exkurs: Kryptografische Grundlagen
- Sichern vom Kommunikationsverbindungen, Protokolle
- Firewalltechnologie
  - Ziele und Aufgaben
  - Packetfilter, Filterregeln auf Layer 3 und 4
  - Proxy Server
  - Application Level Gateway
  - Strukturelle Verknüpfungen (DMZ)
- Public Key Infrastrukturen
  - Digitale Zertifikate
  - Digitale Signatur
  - Funktionale Elemente einer PKI (RA, CA, Verzeichnisdienst)
  - Vertrauensmodelle
  - ID-Zertifikate und Erweiterungen, Revocation Lists
  - OSCP- und SCVP-Protokolle

Inhalt – IT-Sicherheitsarchitekturen

- Zugriffskontroll-Strategien
  - Discretionary Access Control
  - Mandatory Access Control (Bell-LaPadula-Modell)
  - Role Based Access Control
- Priviledge Management Infrastructure
  - Zertifikate und Vertrauensmodell
- Sniffer und Malware
  - Sniffer Angriffe
  - Attacken über Protokolle
  - Distributed Denial-of-Service Attacken
  - ARP-Spoofing
  - Viren, Würmer, Trojaner
  - Mobiler Code
- Aspekte des Datenschutzes

Inhalt – IT-Sicherheitsarchitekturen

- Praktikum (Debian GNU/Linux 6.0 („Squeeze“))
  - Konfiguration von interner und externer Firewall für eine DMZ (Linux)
  - Sicherer E-Mail Verkehr mit Zertifikaten (Postfix-MTA)
    - Verschlüsselte Mail, digital signierte Mails
  - Sicherer Webserver (Apache)
    - http-, https-Verbindungen
    - Application Security
  - Konfiguration von VPN-Verbindungen (OpenVPN)
    - LAN-to-LAN
    - Road Warrior