IT Security Basics

Was ist Sicherheit
- Grundforderungen an Sicherheit
- Sicherheitsziel Vertraulichkeit
- Sicherheitsziel Integrität
- Sicherheitsziel Verfügbarkeit

Risikolage für Unternehmen
- Warum ist das Internet nicht „sicher
- Schadensmöglichkeiten
- Wie abhängig sind Firmen vom IT-Einsatz

Angriffe auf Serverdienste
- Exploits
- Rootkits
- DoS/DDoS/DRDoS
- Sniffer
- Replay-Attacken
- TCP/IP Session-Hijacking
- Sicherheitsprobleme durch Mitarbeiter
- Ausfall/Krankheit
- Unrechtmäßige Systemzugänge
- Spionage
- Mangelnde Kompetenz

Angriffsvorbereitung
- Hacker und Cracker
- Staatliche“ Hacker
- Elektronische Kriegsführung
- Netzwerkscans
- Wardriving
- Social Engineering

Proaktive Sicherheit
- Defensive Programmierung
- Gehärtete Betriebssysteme
- Patches
- Vulnerability Assessment

Sichere E-Mail-Verfahren
- Grundlagen der E-Mail-Verschlüsselung
- Schlüssel generieren
- Schlüsselexport und -import
- Signieren von Schlüsseln
- E-Mail signieren und verschlüsseln
- Dateien signieren und verschlüsseln

Virtual Private Network
- Zielsetzung
- PPTP
- LTP/IPsec
- OpenVPN
- Abgrenzung zu anderen VPN-Arten

WLAN und Sicherheit
- WLAN-Arbeitsweise
- Access-Points
- WEP – Wired Equivalency Protocol
- WPA – Wi-Fi Protected Access
- Weitere Authentifizierung und Verschlüsselung im WLAN
- Funkausleuchtung

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

Asymmetrische Kryptografie
- Nachteile symmetrischer Verfahren
- Einwegfunktion
- Diffie-Hellman-Schlüsseltausch
- El-Gamal
- RSA
- Digitale Signatur
- Hashfunktionen
- Schwachstellen in RSA
- Public Key Infrastructure

Symmetrische Kryptografie
- Das Problem von Alice und Bob
- Einfache Verschlüsselungsmethoden
- Symmetrische Verfahren

Kryptografische Protokolle und ihre Anwendung
- SSL/TLS
- SSH
- IPsec

Virenarten und ihre Verbreitung
- Grundkonzepte von Viren
- Virenarten
- Tarnmechanismen von Viren
- Würmer
- Trojaner
- Adware und PUA
- Tendenzen und Ausblick

Alternative Software
- Warum Nicht-Standard-Software sinnvoll sein kann
- Alternative Webbrowser
- Alternative E-Mail-Clients

Firewalls
- Wie Firewalls arbeiten
- NAT
- Paketfilter-Firewall
- Stateful Inspection Firewall
- Proxy Level/Application Level Firewall
- Personal Firewall
- Sicherheitskonzept Firewall
- Erweiterte Funktionen der Firewall

Intrusion-Detection/Prevention-Systeme
- Notwendigkeit von Intrusion-Detection-Systemen
- Arbeitsweise eines IDS
- Auf erkannte Angriffe reagieren
- Intrusion-Prevention-Systeme (IPS)
- Snort
- Honeypot-Netzwerke

Spyware, Phishing und Browser Hijacking
- Geld verdienen im Internet
- Spyware
- Browser Hijacking
- Was ist Phishing
- Anti-Spyware einsetzen

Stand-Alone-Virenschutz
- Einfache Virenprävention
- Gängige Antivirensoftware
- Computer scannen
- Viren entfernen

IT-Sicherheitsstandard
- Standards im Bereich Informationssicherheit
- IT-Grundschutz-Kompendium
- Weitere Kriterienwerke zur IT-Sicherheit
- DIN EN
- Security Policy
- Aufgaben eines IT-Sicherheitsbeauftragten