

Wireless LAN – Hotspots & Security

„WLAN übernimmt die Herrschaft“ – Insbesondere angesichts der nachlassenden 3G-Euphorie scheinen zahlreiche Akteure dem Charme von Wireless LAN und öffentlichen Hotspots zu erliegen.

Dieser Kurs gibt zunächst eine Einführung in die Technik von Wireless LAN. Die verschiedenen Konfigurationsmöglichkeiten werden ebenso aufgezeigt, wie die physikalische Funktionsweise und die unterschiedlichen Zugriffsverfahren auf das Übertragungsmedium Luft.

Ein Schwerpunkt dieses Kurses liegt auf dem Thema Sicherheit. Die Teilnehmer erhalten einen Überblick über die Sicherheitsmechanismen bei WLAN und die aktuellen Möglichkeiten, wie sie sich als Betreiber vor unerlaubten Zugriffen und ihre Kunden vor Attacken auf persönliche Daten schützen können.

Schließlich werden auch die Herausforderungen bei der Vergebührung (Billing) besprochen. Einige Billing-Lösungen sowie die Einbindung in UMTS werden vorgestellt.

Zielgruppe / Voraussetzungen

Der Kurs wendet sich an Netzwerk-Verantwortliche und Interessierte, die ein grundsätzliches Verständnis der Technologie WLAN anstreben und sich mit den vielschichtigen Sicherheitsaspekten auseinandersetzen möchten. Grundkenntnisse aus dem Bereich Datennetze sind Voraussetzung für den Kurs.

Kursinhalt

Einführung

- Grundbegriffe
- Abdeckung, Reichweite, Durchsatz
- Typische Anwendungsbeispiele
- WLAN-Standards und -Enhancements

WLAN-Architektur

- WLAN-Grundkonfigurationen: BSS, IBSS, ESS
- Network Identifiers (SSID, BSSID)

Physical und MAC Layer

- Physikalische Übertragungsmethoden (IrDA, FHSS, DSSS, OFDM)
- MAC-Zugriff (DCF, RTS/CTS, PCF)
- Managementfunktionen (Synchronisation, Power Management, Roaming)

Grundsätzliche Sicherheitsmängel

- Wired Equivalent Privacy (WEP)
- Funktionsweise und Schwächen von WEP
- SSID Broadcast

Kursdauer:

2 Tage

Kursnummer:

ND1353

Voraussetzungen:

Grundkenntnisse aus dem Bereich Datennetze

Herausforderungen und Bedrohungen

- War Driving
- Sniffing, Spoofing
- Man-in-the-Middle-Attack, Denial of Service (DOS)

Schutzstrategien

- Grundabsicherung (WEP, SSID, Access Control List)
- Erweiterte Absicherung, IEEE 802.11i und WPA
- Virtual Private Network (VPN) und Secure Socket Layer (SSL)

Praktische Übungen

- Sniffing
- Spoofing
- etc.

WLAN-Billing

- Billing-Problematik
- Verschiedene Lösungsansätze

WLAN und die Anderen

- Vergleich mit Bluetooth und 3G
- WiMAX (IEEE 802.16)

Kursanmeldung:

Bitte kontaktieren Sie uns

- per Telefon: +49 89 1894354-0
- per eMail: training@tfk.de oder
- über das Anfrageformular auf unserer Internet-Seite www.tfk.de/training
Dort finden Sie auch ein Fax-Formular.

Sie erhalten von uns umgehend eine Bestätigung Ihrer Anmeldung oder können sich bei der Zusammenstellung der Kursinhalte beraten lassen.

Gern erstellen wir gemeinsam mit Ihnen ein Kurskonzept, das sich speziell an Ihren Anforderungen orientiert. Sie können verschiedene Themengebiete aus unseren Standard-Kursinhalten kombinieren und an Ihre firmenspezifischen Gegebenheiten anpassen lassen.