



Planung, Aufbau und
Konfiguration von
sicheren
Drahtlosnetzwerken
(WLAN)

Planung, Aufbau und Konfiguration von sicheren Drahtlosnetzwerken (WLAN)

Seminarunterlage – Artikelnr. WL-010304

Autor: Carlo Westbrook

Version: Juni 2006

Alle in dieser Seminarunterlage enthaltenen Programme, Darstellungen und Informationen wurden nach bestem Wissen erstellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund ist das in der vorliegenden Seminarunterlage enthaltene Material mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Der Autor und CertPro Limited übernehmen infolgedessen keine Verantwortung und werden keine daraus folgende Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieses Materials, oder Teilen davon, oder durch Rechtsverletzungen Dritter entsteht.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in dieser Seminarunterlage berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann verwendet werden dürften.

Die in diesem Dokument aufgeführten Namen tatsächlicher Firmen und Produkte sind möglicherweise Marken der jeweiligen Eigentümer und werden ohne Gewährleistung der freien Verwendbarkeit benutzt.

Dieses Werk ist urheberrechtlich geschützt.

Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Erlaubnis für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden (auch nicht zur Unterrichtsvorbereitung), unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen, usw.).

CertPro ist eine eingetragene Marke von Carlo Westbrook.

Copyright © 2004 - 2009 CertPro Limited.
Alle Rechte vorbehalten.

Inhaltsverzeichnis

Inhalt	Seite
Voraussetzungen.....	6
Kursbeschreibung	7 – 9
Beispielszenario	10
Kapitel 1 – Grundlagen.....	11 – 18
1. Einleitung.....	13
1.1 Nutzungsmöglichkeiten von WLANs	14
1.2 Praxiszenarien für größere WLANs	15 – 16
1.3 Nachteile von WLANs	17 – 18
Kapitel 2 – Planung und Aufbau	19 – 38
2. Planung und Aufbau	21
2.1 Die Komponenten eines WLANs	22 – 23
2.2 Architekturen	24 – 27
Ad-hoc-Netzwerke (Peer-to-Peer Workgroup)	24 – 25
Infrastrukturnetzwerk	26 – 27
2.3 Der IEEE 802.11-Standard	28 – 29
IEEE 802.11b-Standard	28 – 29
IEEE 802.11g-Standard	29
IEEE 802.11a- und 802.11h-Standard.....	29
2.4 Die 802.11-Standards im Vergleich	30
2.5 Der 802.11-Standard und das ISO-OSI-Modell.....	31 – 32
2.6 Mögliche Störeinflüsse.....	33 – 34
2.7 Elektrosmog und Gesundheitseinflüsse.....	35
2.8 Vergleich von WLAN mit typischen Kabelnetzen	36
2.9 Vergleich Bluetooth – WLAN.....	37 – 38
Kapitel 3 – Grundlagen zum Aufbau von Funkzellen.....	39 – 54
3. Der Aufbau von Funkzellen	41
3.1 Anforderungen	42 – 43
3.2 Der Aufbau eines größeren WLANs.....	44 – 46
3.3 Installation der Access Points (APs)	47 – 49
3.4 Power over Ethernet (PoE).....	50
3.5 Verwendung externer Antennen	51 – 53
Antennen mit Rundumabstrahlung.....	52
Richtantennen	52 – 53
Kapitel 4 – Einrichten eines WLANs	55 – 72
4. Einrichten eines WLANs	57
4.1 Konfiguration eines Access Points.....	58 – 61
4.2 Konfiguration eines WLAN-Clients	62 – 65
4.3 Praktische Übung:	66 – 71
Konfiguration eines WLAN-Clients im Ad-hoc-Modus.....	67
Datenaustausch im Ad-hoc-Modus	68

Konfiguration eines Access Points	69 – 70
Konfiguration eines WLAN-Clients zur Anbindung an einen AP	71
Kapitel 5 – Sicherheit in WLANs.....	73 – 88
5. Sicherheit in WLANs.....	75
5.1 Wired Equivalent Privacy (WEP)	76 – 77
Verschlüsselung.....	76
Authentifizierung	77
5.2 Zugriffskontrolle (Access Control)	78
5.3 Closed Network.....	79
5.4 IEEE 802.1x/EAP.....	80 – 81
EAP-Authentifizierungsmethoden.....	81
5.5 Virtual Private Network (VPN)	82 – 83
5.6 Open User Authentication (OUA)	84
5.7 Traffic Lock.....	85
5.8 IEEE 802.11i	86 – 88
WPA.....	88
Kapitel 6 – Bekannte WLAN-Attacken	89 – 102
6. Bekannte WLAN-Attacken	91
6.1 War-Driving.....	92
6.2 Drive-by-Hacking.....	93
6.3 Klartext- und Wörterbuch-Attacken	94 – 95
6.4 Man-in-the-Middle-Attacken.....	96
6.5 Passive Attacks	97
6.6 Aktive Attacks.....	98
6.7 Praktische Übung – „Data-Sniffing“	99 – 101
Kapitel 7 – Analyse eines WLANs.....	103 – 114
7. Analyse von WLANs	105
7.1 Analyse des zu schützenden Netzwerkes	106
7.2 Grundsätzliche Überlegungen	107 – 108
Ungeschützter Access Point	107
Geschützter Access Point	108
7.3 Praktische Übung – Analyse eines ungeschützten APs.....	109 – 110
7.4 Praktische Übung – Analyse eines geschützten APs.....	111 – 112
7.5 Auswahl der Hardware	113
7.6 Netzwerk-Analyse-Tools	114
Kapitel 8 – Konfiguration eines WLANs	115 – 134
8. Konfiguration eines WLANs	117
8.1 Einstellungen des Access Points	118 – 120
Verschlüsselung.....	119
MAC-Filter	120
8.2 Einstellungen der WLAN-Karten	121 – 122
8.3 Praktische Übung –Konfiguration eines gesicherten APs.....	123 – 125
8.4 Praktische Übung –Konfiguration von gesicherten WLAN-Karten.....	126 - 127
8.5 Analyse dieser Konfiguration	128 – 132
8.6 Bewertung der Konfiguration	133
8.7 Bewertung der Wireless LAN-Technologie.....	134

Kapitel 9 – Sicherung eines WLANs mit VPN	135 – 152
9. Sicherung eines WLANs mit VPN.....	137
9.1 Grundlagen eines Virtual Private Networks (VPN).....	138 - 140
VPN-Protokolle: PPTP und L2TP	139
Integration einer Firewall.....	139
9.2 Konfiguration eines VPN-Netzwerkes / Client-Konfiguration	141
9.3 Authentifizierung im VPN.....	144
9.4 Praktische Übung – Konfiguration von WLAN-Clients für VPN.....	145
9.5 Analyse des Netzwerkverkehrs nach Implementierung des VPN.....	147
9.6 Praktische Übung – Analyse des VPN-Datenverkehrs.....	149
9.7 Fazit	152
Kapitel 10 – Implementieren der WLAN-Sicherheit nach IEEE 802.1x	153 – 206
10. Implementieren der Sicherheit nach IEEE 802.1x.....	155
10.1 Kernpunkte zur Implementierung der IEEE 802.1x-Sicherheit.....	156
10.2 IEEE 802.1x und Verschlüsselung	158
10.3 Zertifikate oder Passwörter.....	159
10.4 Voraussetzungen für die Lösung	161
10.5 Überlegungen zu WLAN-Sicherheitsrichtlinien	162
10.6 Benutzer- und/oder computerbasierte Authentifizierung.....	163
10.7 Prüfung von zertifikatsbasierten Anmeldeinformationen	164
10.8 Festlegen der Authentifizierungsanforderungen.....	166
10.9 Auswählen der Strategie zur Clientkonfiguration	168
10.10 Festlegen der Verschlüsselungsanforderungen	169
10.11 Auswählen einer Strategie für die WLAN-Migration.....	170
10.12 Design der WLAN-Netzwerkinfrastruktur	171
10.13 Überlegungen zu WLAN-Gruppenrichtlinien	172
10.14 Festlegen der für 802.1x-WLANs erforderlichen Softwareeinstellungen ...	173
10.15 Konfiguration von RAS-Richtlinien	174
10.16 Konfiguration von Verbindungsrichtlinien	176
10.17 Konfiguration von Gruppenrichtlinien für Clientcomputer.....	177
10.18 Konfiguration der 802.1x-Einstellungen auf Clientcomputern	179
10.19 Zusätzliche Überlegungen	181
10.20 Praktische Übung	182 - 204
Zusammenfassung.....	205
Anhang A – Checkliste für sicheres WLAN	209 - 210
Anhang B – Hacker- und Security-Tools	211 - 212
Anhang C – Wichtige Weblinks	213
Anhang D – Beispiele für Netzwerk-Traces	214 - 217
Anhang E – Glossar	218 - 227
Anhang F – Abkürzungen	228