

Inhaltsverzeichnis

| | |
|---|------------|
| Autorenteam..... | iii |
| Einleitung | v |
| Ziele des Handbuchs | vii |
| Inhaltsverzeichnis | ix |
| 1. WLAN im Überblick | 1 |
| 1.1 Was versteht man unter WLAN?..... | 1 |
| 1.2 Anwendungsbereiche des WLAN..... | 2 |
| 1.3 Nachteile der WLAN-Technologie | 3 |
| 2. Funktionsweise eines WLAN | 5 |
| 2.1 Die wichtigsten WLAN-Komponenten..... | 5 |
| 2.1.1 Access Point..... | 5 |
| 2.1.2 WLAN Modem / Router..... | 6 |
| 2.1.3 WLAN-Adapter | 7 |
| 2.2 Betriebsarten eines Wireless LAN | 8 |
| 2.2.1 Ad-Hoc Modus..... | 8 |
| 2.2.2 Routing im Ad-Hoc Modus | 9 |
| 2.2.3 Infrastructure Modus..... | 10 |
| 2.2.4 Reichweite eines WLAN (Funkausbreitung) | 12 |
| 2.2.5 Störungen durch Hindernisse..... | 12 |
| 2.2.6 Elektrische Störungen..... | 14 |
| 2.2.7 WLAN-Antennen..... | 14 |
| 2.2.8 Extended Service Set | 16 |
| 2.2.9 Wireless Distribution System (WDS) | 17 |
| 2.2.10 Bridging Modus..... | 18 |
| 2.2.11 Repeating Modus | 18 |
| 2.2.12 Universal Repeater Mode | 20 |
| 3. WLAN-Sicherheit | 21 |
| 3.1 Einführung in die WLAN-Sicherheit..... | 21 |
| 3.2 Verschlüsselte Kommunikation mit WEP..... | 23 |
| 3.2.1 WEP-Schwachstellen | 23 |
| 3.3 Verschlüsselte Kommunikation mit WPA..... | 24 |
| 3.3.1 WPA im SOHO-Netzwerk | 25 |
| 3.3.2 WPA im Unternehmensnetzwerk | 25 |
| 3.3.3 WPA Schwachstellen..... | 27 |
| 3.4 WPA2..... | 28 |
| 3.4.1 WPS..... | 28 |
| 3.4.2 PBC – Push Button Configuration | 28 |
| 3.4.3 PIN..... | 28 |
| 3.4.4 UFD – USB Flash Drive..... | 29 |
| 3.4.5 NFC – Near Field Communication..... | 29 |
| 3.4.6 WPA2 Schwachstellen..... | 29 |
| 3.4.7 WPA2 Probleme..... | 29 |

| | | |
|-----------|---|-----------|
| 3.4.8 | Abwärtskompatibilität | 30 |
| 3.5 | VPN-Tunnel | 30 |
| 3.6 | Sichere Repeater-WLAN Verbindung bei WDS | 31 |
| 3.6.1 | WPA2 und WDS verknüpft | 31 |
| 3.6.2 | Weitere Schutzmaßnahmen | 32 |
| 3.6.3 | Änderung der Passwörter | 32 |
| 3.6.4 | Abschalten der Konfiguration des Access-Point über WLAN | 33 |
| 3.6.5 | Änderung der SSID | 33 |
| 3.6.6 | DHCP | 33 |
| 3.6.7 | MAC-Filter | 33 |
| 3.6.8 | Sichere Verschlüsselung und Schlüssel verwenden | 34 |
| 3.6.9 | Schlüsselwechsel | 34 |
| 3.6.10 | Fernwartung abschalten | 34 |
| 3.6.11 | Leistungsanpassung | 34 |
| 4. | WLAN Gefahren | 36 |
| 4.1 | Angriffstools | 36 |
| 4.2 | Angriffsmethoden | 36 |
| 4.2.1 | Hochleistungsantennen | 37 |
| 4.2.2 | Verschlüsselung entschlüsseln | 37 |
| 4.2.3 | Unberechtigte Zugangspunkte | 37 |
| 4.2.4 | MAC-Spoofing | 37 |
| 4.2.5 | „Man-in-the-middle“ Attacken | 38 |
| 4.2.6 | Denial-of-Service Attacken | 38 |
| 4.2.7 | WarWalking / WarDriving | 39 |
| 5. | Praktische Beispiele und Konfigurationsanleitungen | 41 |
| 5.1 | Vorbereitung Routerkonfiguration | 41 |
| 5.1.1 | Überprüfen der Netzwerkeinstellungen | 41 |
| 5.1.2 | Herausfinden der IP-Adresse eines Gateways | 43 |
| 5.2 | WPA-PSK Verschlüsselung | 43 |
| 5.2.1 | Beispiel WPA-PSK anhand eines Netgear Routers DG834GB | 43 |
| 5.2.2 | Verbindung mit dem drahtlosen Netz unter Windows | 44 |
| 5.3 | Router Konfiguration Firmware-Update | 45 |
| 5.3.1 | Backup und Wiederherstellung der Einstellungen | 46 |
| 5.3.2 | Herunterladen der neuen Firmware | 47 |
| 5.3.3 | Firmware-Update | 48 |
| 6. | WLAN-Tools | 51 |
| 6.1 | Tools zur Einrichtung, Konfiguration und Fehlersuche | 51 |
| 6.1.1 | RK-WLAN-Keygen | 51 |
| 6.1.2 | inSSIDer | 52 |
| 6.1.3 | NetSurveyor | 52 |
| 6.1.4 | Xirrus Wi-Fi Inspector | 53 |
| 6.1.5 | EkaHau HeatMapper | 54 |
| 6.2 | Tools für Hotspots | 55 |
| 6.2.1 | WeFi | 55 |
| 6.2.2 | Hotspot Shield | 56 |
| 6.3 | Tools zur Administration und Sicherheitsoptimierung | 56 |
| 6.3.1 | Network Share Browser | 56 |
| 6.3.2 | Advanced Port Scanner | 57 |

| | | |
|------------|--|-----------|
| 6.3.3 | WirelessKeyView | 58 |
| 7. | Überblick der gesetzlichen Regelungen | 59 |
| 7.1 | Schutz-, aber nicht rechtlos | 59 |
| 7.1.1 | Händler | 59 |
| 7.1.2 | Betreiber | 60 |
| 7.1.3 | Zivilverfahren | 60 |
| 7.1.4 | Strafverfahren | 60 |
| 7.1.5 | Zahlungsverpflichtung | 61 |
| 7.1.6 | Nutzer | 61 |
| 7.1.7 | Eindringen in ein ungeschütztes Netz | 61 |
| 7.1.8 | Eindringen in ein geschütztes Netz | 62 |
| 7.1.9 | Datenbeschaffung | 62 |
| 7.1.10 | Meldepflicht | 62 |
| 8. | Anhang | 66 |
| 8.1. | WLAN Verschlüsselungsmethoden | 66 |
| 8.1.2. | WEP-Verschlüsselung | 66 |
| 8.1.3. | WEP-Entschlüsselung | 67 |
| 8.1.4. | Neue Funktionen der WPA-Verschlüsselung | 67 |
| 8.1.5. | WPA-Verschlüsselung | 68 |
| 8.1.6. | WPA-Entschlüsselung | 68 |
| 8.1.7. | WPA2 - AES Verschlüsselung | 69 |
| 8.1.8. | WPA2-Entschlüsselung | 70 |
| 8.2. | WLAN Standard IEEE 802.11 | 70 |
| 8.2.2. | IEEE 802.11 | 70 |
| 8.2.3. | IEEE 802.11a | 71 |
| 8.2.4. | IEEE 802.11b | 71 |
| 8.2.5. | IEEE 802.11g | 71 |
| 8.2.6. | IEEE 802.11n | 71 |
| 8.2.7. | IEEE 802.11ac | 72 |
| 8.2.8. | Weitere Standards: | 72 |
| 8.3. | Allgemeiner Überblick: WLAN-Frequenzbänder | 73 |
| 9. | Abbildungsverzeichnis | 76 |
| 10. | Checkliste | 78 |
| 11. | Literaturverzeichnis | 80 |
| 12. | Weblinks | 81 |
| | Stichwortverzeichnis | 82 |
| | Glossar | 86 |