WLAN-Sicherheit

ITT-Net-IS

8. April 2025

1 Einleitung

WLANs bieten eine komfortable Möglichkeit zur Netzwerkverbindung, bringen aber auch besondere Sicherheitsrisiken mit sich. Funkbasierte Kommunikation ist per se leichter abzufangen als kabelgebundene. Daher ist der Einsatz geeigneter Verschlüsselungs- und Authentifizierungsverfahren essenziell.

2 Grundlagen der WLAN-Verschlüsselung

2.1 WEP – Wired Equivalent Privacy

WEP war der erste Verschlüsselungsstandard für WLANs, wurde aber bereits kurz nach seiner Einführung als unsicher erkannt. Er verwendet RC4 als Verschlüsselungsalgorithmus mit einem 40- oder 104-Bit-Schlüssel.

Notes

RC4 ist ein symmetrischer Stromverschlüsselungsalgorithmus. Bei WEP ist das Problem, dass Initialisierungsvektoren (IV) nur 24 Bit lang sind, sich schnell wiederholen und somit Angriffe wie das sogenannte „IV-Kollisionen“ ermöglichen.

2.2 WPA – Wi-Fi Protected Access

WPA wurde als Übergangslösung eingeführt und verbessert einige Schwächen von WEP. Es nutzt TKIP (Temporal Key Integrity Protocol), das dynamisch Schlüssel erzeugt und so die Angreifbarkeit reduziert.

2.3 WPA2

WPA2 löst WPA ab und basiert auf dem robusteren AES-Standard (Advanced Encryption Standard) in Verbindung mit CCMP (Counter Mode CBC-MAC Protocol). WPA2 ist über viele Jahre der Sicherheitsstandard in WLANs gewesen.

2.4 WPA3

WPA3 ist der aktuelle Sicherheitsstandard. Er verbessert den Schutz gegen Wörterbuchangriffe und bietet auch im öffentlichen WLAN („Open Wi-Fi“) eine gewisse Verschlüsselung durch Opportunistic Wireless Encryption (OWE).

Notes

- **TKIP**: Ein Protokoll, das dynamische Schlüsselvergabe ermöglicht, jedoch noch auf RC4 basiert.
- **CCMP**: Basiert auf AES und bietet Authentizität, Integrität und Vertraulichkeit.
- **OWE**: Verschlüsselt Datenverkehr ohne vorherige Authentifizierung – nützlich in offenen WLANs.

- Seit **Januar 2021** ist WPA3 für alle neuen Wi-Fi-zertifizierten Geräte **obligatorisch**.
- Für Geräte, die im **6-GHz-Band** („Wi-Fi 6E“) betrieben werden, ist **WPA3 zwingend vorgeschrieben**. WPA2 ist in diesem Frequenzbereich nicht mehr zulässig.

Notes

- **Wi-Fi 6E** erweitert Wi-Fi 6 um das 6-GHz-Band und ermöglicht höhere Bandbreiten und geringere Latenzen.
- Die Wi-Fi Alliance schreibt WPA3 vor, um die Sicherheit bei neuen Geräten und Frequenzbereichen zu garantieren.
- Auch bei **Wi-Fi 7** ist WPA3 im 6-GHz-Band und zusätzlich für neue Funktionen wie Multi-Link-Operation (MLO), das für stabilere Verbindungen sorgt vorgeschrieben.

3 Sicherheitsmodi: Personal vs. Enterprise

3.1 WPA2/WPA3 Personal

Verwendet ein gemeinsames Passwort (Pre-Shared Key, PSK). Einfach zu implementieren, aber nicht für größere Netzwerke geeignet.

3.2 WPA2/WPA3 Enterprise

Setzt auf eine zentrale Authentifizierungsinstanz, meist über RADIUS, und individuelle Zugangsdaten für Nutzer. Damit lassen sich Nutzer gezielt sperren und Sicherheitsrichtlinien besser durchsetzen.

Notes

- **RADIUS** (Remote Authentication Dial-In User Service): Protokoll zur Authentifizierung und Autorisierung in Netzwerken.
- **AAA**: Authentication, Authorization, Accounting – drei Säulen der Netzwerksicherheit.

4 Allgemeine Sicherheitsherausforderungen bei WLAN

- **Abhören**: Funkübertragung kann mit einfachen Mitteln abgehört werden.
- **Rogue Access Points**: Unautorisierte Geräte im Netz können als legitime Access Points erscheinen.
- **Evil Twin Angriffe**: Ein gefälschter Access Point mit identischem SSID verleitet Clients zur Verbindung.
- **Man-in-the-Middle**: Datenverkehr kann abgefangen und manipuliert werden.

5 Empfehlungen zur WLAN-Sicherheit

- Verwenden Sie WPA3, wo verfügbar, sonst mindestens WPA2.
- Nutzen Sie Enterprise-Modus mit RADIUS für größere Netzwerke.
- Deaktivieren Sie WPS (Wi-Fi Protected Setup).
- Nutzen Sie starke, individuelle Passwörter.
- Verfolgen Sie regelmäßig Firmware-Updates für Router und Access Points.

6 Beispiel: Konfiguration eines Cisco-Routers für WPA2 Enterprise

```
conf t
!
interface Dot11Radio0
 ssid WLAN_Enterprise
   authentication open
   authentication key-management wpa version 2
   dot1x authentication-server 192.168.1.10
   dot1x radius-server 192.168.1.10 auth-port 1812 acct-port 1813 key geheim
   mbssid guest-mode
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.1 255.255.255.0
!
radius-server host 192.168.1.10 auth-port 1812 acct-port 1813 key geheim
!
end
```

7 Beispiel: Konfiguration eines Cisco-Routers für WPA2 PSK

```
conf t
!
interface Dot11Radio0
 ssid WLAN_PSK
   authentication open
   authentication key-management wpa version 2
   wpa-psk ascii MeineSicherePassphrase
!
interface Dot11Radio0.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.1 255.255.255.0
!
end
```

8 Fazit

WLAN-Sicherheit ist ein vielschichtiges Thema, das mehr als nur ein starkes Passwort erfordert. Besonders in professionellen Netzwerken ist die Nutzung von WPA2/WPA3-Enterprise mit RADIUS und durchdachter Netzwerksegmentierung essenziell. Auch in privaten Netzen sollte mindestens WPA2 mit starker Passphrase und regelmäßigen Firmware-Updates Standard sein.

Notes

Der Umstieg auf WPA3 ist technisch sinnvoll, aber noch nicht flächendeckend möglich. Viele ältere Geräte unterstützen diesen Standard nicht.