**WLAN-Sicherheit**

Es gibt 3 verschiedene Verschlüsselungs- und Authentifizierungsmethoden von WLAN, die heißen WEP, WPA und WPA2, dabei ist WPA2 das sicherste und es wird empfohlen Geräte, die WEP unterstützen aufzurüsten auf WPA2, weil WEP nicht mehr als sicher gilt, außerdem gibt es 10 Maßnahmen zur WLAN-Sicherheit, nämlich 1. eine eigene SSID zu vergeben, 2. ein eigenes Admin-Passwort für den Access Point zu vergeben, 3. den SSID-Broadcast abzustellen, 4. WPA2-Verschlüsselungen einzuschalten, 5. MAC-Adressfilter einzusetzen, 6. VPN einzusetzen, 7. WLANs von anderen Netzwerk-Segmenten logisch zu trennen, 8. eine Firewall zwischen WLAN und LAN installieren, 9. IDS im WLAN aufzustellen und 10. regelmäßige Audits mit aktuellen Hacker-Tools zu machen.

WEP ist technisch veraltet und nicht mehr zeitgemäß, sollte ausgetauscht werden mit WPA2, weil es strafbar ist, wenn das WLAN nicht verschlüsselt ist und Hacker sich ziemlich leicht in ein WEP-gesichertes-WLAN-Netz hacken können.

WPA nutzt TKIP (Temporal Key Integrity Protocol) als Verschlüsselungsmethode, während WPA2 AES (Advanced Encryption Standard) verwendet.