WLAN Protection - WPA

WPA steht für "WiFi Protected Access". Dies ist eine Verschlüsselungsmethode für Drahtlosnetzwerke. WPA ist der 2003 verabschiedete Nachfolgestandard von WEP, der zur Verschlüsselung und Authentifizierung in WLAN-Netzwerken verwendet wurde. WPA sollte die bekannt gewordenen Sicherheitslücken sowie Schwachstellen von WEP beseitigen. Außerdem sollte damit Schaden und Imageverlust der WLAN-Technik verhindert, sowie der entstehende Markt für kabellose Netzwerke nicht gefährdet werden.

Der ehemalige IEEE-Standard 802.11 (WEP) stellte sich als unsicher heraus, und die Verabschiedung des bereits geplanten, neuen Sicherheitsstandards IEEE 802.11i (heute WPA2) verzögerte sich. Da man aber dringend eine Zwischenlösung benötigte, nutze die WiFi Alliance eine Teilmenge des zukünftigen, bereits vorhandenen IEEE-Standards 802.11i in Kombination mit IEEE 802.11 und etablierte dies unter dem Namen „WPA" als Pseudostandard.

WPA enthält zwar die Architektur von WEP, doch durch dynamische Schlüssel die auf TKIP (Temporal Key Integrity Protocol) basieren, wird zusätzlicher Schutz gewährleistet. Aufgrund dessen, dass WPA auf WEP-Hardware basiert, konnte durch ein Software Update auf das neue WPA aktualisiert werden, anstatt komplett neue Geräte mit dem neuen Standard produzieren zu müssen. Es bietet zur Authentifizierung von Clients PSK (Pre-shared key) oder EAP (Extensible Authentification Protocol) über IEEE 802.1X an. EAP wird meist nur in großen Wireless-LAN-Installationen verwendet, da hierfür eine Authentifizierungsinstanz in Form eines Servers benötigt wird. PSK wird in kleineren Netzwerken verwendet, zum Beispiel in einer kleinen Firma oder beim Home Office. Damit der Sitzungsschlüssel generiert werden kann, muss der PSK also den Nutzern des WLAN bekannt sein. Im Gegensatz zu WEP wird zusätzlich zu dem 48 Bit langen Initialisierungsvektor für jedes Datenpaket ein neuer Schlüssel sowie ein MIC (Message Integrity Check / Prüfsumme) verwendet.