von Mel Beckman

Frage: Wir entwickeln derzeit eine unternehmensweite Wireless-Lösung und meine Aufgabe in diesem Projekt ist die Evaluierung von Produkten. Ich erinnere mich an einen Ihrer Artikel zu diesem Thema aus dem Jahre 2005, in dem angemerkt wurde, dass IPSec VPN Tunnels zur Sicherung aller Wi-Fi Verbindungen eingesetzt werden sollten. Ist dies immer noch der Fall? Muss ich mir noch Gedanken darüber machen, ob ein Anbieter VPN Authentifizierung unterstützt oder nicht?

Antwort: Ich fühle mich geschmeichelt, dass Ihre Erinnerung bis zu Artikeln aus den dunklen Tagen des Jahres 2005 zurückreicht. Das war wahrlich eine schmerzvolle Periode für die Wi-Fi Sicherheit. Es stimmt, dass zu der damaligen Zeit IPSec VPN Tunnels die einzige Möglichkeit darstellten, Wi-Fi Verbindungen wirklich zu sichern. Die Wi-Fi Verschlüsselungsstandards dieser Ära (WEP – Wired Equivalent Protection und WPA – Wi-Fi Protected Access) waren bereits weitgehend von Hackern geknackt und wurden in Sachen Sicherheit als mehr oder minder unbrauchbar erachtet.

Künstler Burgy Zapp

Die Zeiten haben sich aber gewandelt und die Situation sieht heute weit erfreulicher aus. Die Wi-Fi Verschlüsselung hat sich in der Zwischenzeit beträchtlich verbessert. Der hauptsächliche Fortschritt ist in der breiten Verfügbarkeit von WPA2 (Teil des 802.11i Standards), einem Nachfolger von WPA zu sehen. WPA2 verwendet den wesentlich stärkeren Verschlüsselungs-Algorithmus AES (Advanced Encryption Standard) und einen sicheren Mechanismus für die Verteilung temporärer Schlüssel. WPA2 verwendet zwei Authentifizierungsmodelle, die beide von den meisten Client-Betriebssystemen (Windows XP, Mac OSX und Linux) unterstützt werden.