WLAN-Sicherheit

SicherheitsmaÃŸnahmen im WLAN. Wichtig!
Allgemein Die Ãœbertragungsnormen von WLANs ist international geregelt. GrundsÃ¤tzlich kann man mit kleinen Tools (in WinXP bereits enthalten) nach Funknetzwerken suchen und sich mit diesen per Mausklick auch gleich verbinden. Mit zusÃ¤tzlicher (frei erhÃ¤ltlicher) Software ist auch ein Wardriven mÃ¶glich. Deshalb ist es heutzutage extrem wichtig, sein WLAN abzusichern!
Â Die wichtigsten MÃ¶glichkeiten, um sich davor zu schÃ¼tzen sind hier angefÃ¼hrt. 1. Man kann das "Broadca eigenen Netzwerknamen (SSID) unterbinden, so dass einÂ automatisches ErkennenÂ verhindert wird.

Es wird lediglich ein WLAN angezeigt (je nach Betriebssystem nicht einmal das), nicht jedoch die SSID.

Diese hidden-SSID ist nur eine sehr bescheidene Security-MaÃŸnahme, jedoch kostet sie keinen Mehraufwand und ist deshalb als ergÃ¤nzende MaÃŸnahme zu empfehlen.

Es gibt allerdings Linux-Tools die auch die hidden-SSID anzeigen. 2. Die Verwendung eines WEP-SchlÃ¼ssels 40 oder 104Bit

Der WEP-Key (Wireless Equivalent Privacy) basiert auf den etwas veralteten und bereits unsicheren RC4 SchlÃ¼ssel von RSA.

Der RC4 besteht aus einem 24 Bit Initialisierungsvektor und einem 40 oder 104 Bit langen SchlÃ¼sselfestlegungsalgorithmus.

Dieser Initialisierungsvektor ist unter bestimmten UmstÃ¤nden schwach, d.h. es lassen sich bei genÃ¼gend abgefangener Pakete RÃ¼ckschlÃ¼sse auf den SchlÃ¼ssel ziehen. Diesen schwachen IV (weak key) nutzen einige Tools um den SchlÃ¼ssel zu knacken.

Nach etwa 5-10Mio. empfangenen Paketen kann man den SchlÃ¼ssel in einigen Sekunden rekonstruieren. Durch geschicktes Packetinjection, kann man so eine hohe Datenmenge ohne weiteres provozieren.

Eine Brute-Force-Attacke wÃ¤re ebenfalls mÃ¶glich. Die dafÃ¼r notwendige Rechenzeit wÃ¼rde allerdings in keinem VerhÃ¤ltnis zum Aufwand stehen.

Bei einer Dictionary-Attack und einem leichten WEP-Key (z.B.: 1234567890123) wÃ¤re er in Sekundenbruchteile kompromitiert, ansonsten gestaltet sich eine solche Attacke ebenso sinnlos wie die Brute-Force-Attacke.

SchÃ¤tzungen zufolge soll das Brechen eines 40-Bit-WEP-SchlÃ¼ssels in einer Viertelstunde mÃ¶glich sein. Die etwas bessere WEP128-Variante mit 104 Bit langen SchlÃ¼sseln wÃ¼rde einen Angreifer dann auch nur etwa 40 Minuten aufhalten. Zur Zeit existieren solche Tools nur fÃ¼r Linux. 3. Manueller Eintrag aller verwendeten MAC-Adressen der Clients

Bei mehreren, wechselnden Clients ist diese MaÃŸnahme administrativ aufwendig. Der Security-Faktor ist bescheiden da sich eine MAC-Adresse (eindeutige Kennung einer Netzwerkkarte) sehr leicht fÃ¤lschen lÃ¤sst (meist reicht ein Eintrag in den Treiber-Eigenschaften). ZusÃ¤tzliche SicherheitsmaÃŸnahmen

Da diese Methoden nur einen begrenzten Schutz bieten sollte man unbedingt auf weitere Security-Features setzen!

Einige proprietÃ¤re Systeme bieten auch eineÂ Rollover-Key-VersionÂ von WEP (hier wird der SchlÃ¼ssel alle x Minuten erneuert) oderÂ WEP2/WEP+Â welcher die SchwÃ¤chen von WEP nicht mehr hat und auch erweiterbar ist.Â

Ein weiteres Beispiel wÃ¤re eineÂ Radius-Authentifizierung mittels 802.1x und zB. TLS oder PEAP.Â

Noch besser ist es den derzeit hÃ¶chsten VerschlÃ¼sselungsgrad WPA2 mit 802.1x zu kombinieren.

Eine sehr gute Security-MaÃŸnahme ist die Implementation eines VPN (Virtual Private Network) mit IPSec.

Wem das noch nicht genug ist kann auch noch ein IDS-System (Intrusion Detection System) oder noch besser IPS-System (Intrsusion Prevention System),Â zum Erkennen von Network-Scans und Angriffe, einsetzen.