

## **Sicherheit im Wireless-LAN**

(Quelle: Computerbase.de, 19. Mai 2004)

### Drei wichtige Schritte zum "Safer Surfen"

#### Einleitung und Hintergrund

Drahtlose Netzwerke gehören nicht erst seit Intels Centrino-Feldzug und nicht zuletzt durch die zahlreichen Angebote der Internetdienstleister zur Peripherie, die sich mit beachtlicher Geschwindigkeit immer größerer Beliebtheit erfreut. Kein Wunder, ist ja auch alles so schön einfach. Der W-LAN-Router, in wenigen Minuten mit dem Internet verheiratet, kann die ganze Familie schnell und einfach ins Internet bringen, ohne lästige Kabel verlegen zu müssen. Insbesondere die Access Points mit integrierter Routerfunktion (oftmals gar rudimentärer Hardware-Firewall) bieten mittlerweile etliche nützliche Funktionen für das ungetrübte Vergnügen im heimischen Netzwerk.

Leider kommt es nicht selten vor, dass die Sicherheit dabei in Vergessenheit gerät. Doch genau sie ist bei Funkverbindungen so immens wichtig, da man von außerhalb deutlich einfacher an ein Netzwerk kommt, als es bei herkömmlichen, verkabelten Netzwerken der Fall war und ist. Ohne die nötigen Sicherheitsvorkehrungen ist es für Fremde mit dem entsprechenden Equipment in wenigen Sekunden ein Kinderspiel, sich in ein Wireless-Netzwerk einzuwählen und eventuelle Internetverbindungen mit zu nutzen. Neben finanziellen Konsequenzen, die einem so im Falle von Volumen- oder Zeittarifen anfallen, sollten auch strafrechtliche Aspekte nicht außer Acht gelassen werden. So ließe sich über ein offenes W-LAN und dessen Internet-Verbindung unbehelligt allerlei Schindluder auf Kosten des Netzbetreibers veranstalten. Begibt sich der Schmarotzer auf illegales Terrain, steht man womöglich schneller als einem lieb ist und absolut unwissend unter staatlicher Beobachtung.

Bei einem spontanen Test konnten mit Hilfe einer montierten Wireless-LAN-Antenne auf dem Autodach innerhalb von nicht einmal 30 Minuten knapp über 100 W-LAN-Netze in einem sogar eher mäßig besiedeltem Gebiet Hannovers aufgespürt werden, von denen ca. 45 % aufgrund fehlender Sicherheitsoptionen komplett zugänglich waren. Bei einigen wäre zudem eine Internetverbindung in wenigen Sekunden möglich gewesen. Darunter fielen allerdings nicht nur private Netzwerke, sondern auch viele Firmennetzwerke. In der Berliner Innenstadt zeigte sich ein ähnliches Bild.

Das Aufspüren solcher offenen W-LANs sorgte schon Anfang 2002 weltweit für Aufsehen, als sich in den hochgezüchteten Metropolen immer öfter kryptische Kreidezeichnungen an Hauswänden wiederfanden, die auf derartige Netzwerk aufmerksam machten und zum kostenlosen Surfen einluden. Im Juli 2002 widmete sich das Magazin Der Spiegel dieser auf den Namen Warchalk (engl.: „Kriegskreide“) getauften Zeichensprache in einem Artikel. Getan hat sich indes - das zeigen nicht nur unsere Ergebnisse - wenig.

Aller Unaufmerksamkeit zum Trotz bieten die aktuellen Wireless-Komponenten drei wichtige Sicherheitsoptionen, die innerhalb von rund zehn Minuten eingerichtet werden können. Namentlich sind dies die WEP-Verschlüsselung, das MAC-Filter und das unsichtbar machen der Netzwerkkennung (SSID). Wir wollen in diesem Artikel unseren Teil zum „Safer Surfen“ beitragen.

#### WEP-Verschlüsselung

##### 1. Schritt: WEP-Verschlüsselung aktivieren

Eine Grundfunktion des 802.11 Standards und der passenden Hardware ist die Verschlüsselung der Daten nach WEP (wired equivalent privacy). Hier gibt es üblicherweise zwei verschiedene Stärken, die 40 Bit (64 Bit) und die 104 Bit (128 Bit) starke Verschlüsselung. Bei der 40 Bit-Verschlüsselung setzt sich der Schlüssel aus zehn und bei der 104 Bit-Variante aus 26 Hexadezimalziffern zusammen (Eine Hexadezimalziffer = 4 Bits). Die 64 Bit respektive 128 Bit werden dadurch erreicht, dass dem Code ein 24 Bit langer Initialisierungsvektor vorausgeht, den die Hersteller bei der Angabe der Verschlüsselungsstärke mit dazu rechnen.

Generell genügt für den privaten Bereich eine Stärke von 64 Bit. 128 Bit verursachen zum einen eine leichte Dämpfung der Übertragungsrate und machen häufig Probleme - im schlimmsten Fall bis hin zu Verbindungsabbrüchen. Der WEP-Schlüssel muss sowohl dem Access Point (Router) als auch den jeweiligen Clients bekannt sein, d.h. in den Einstellungen für die WLAN-Karte muss dieser in das Profil eingetragen werden. Im Access Point kann der Schlüssel über das Webinterface (im Handbuch wird beschrieben, wie man dahin gelangt) bei den Einstellungen für die WLAN Verbindung eingegeben werden. Beim Schlüssel stehen einem also 10 Hexadezimalziffern zur Auswahl. (Hexadezimal = 0-9 und A-F) Der Schlüssel an sich sollte nicht zu einfach gestrickt sein. Ein 1234567890 oder 0123456789 ist also alles andere als sinnvoll. ;-) Der WEP-Mode muss dabei auf „HEX“ stehen. Die Konfiguration von anderen Herstellergeräten weicht von der Vorgehensweise bei dem von uns exemplarisch aufgeführten D-Link-Modells im Detail zwar ab. Die Grundzüge sind jedoch identisch und die Dokumentation sollte hier schnell Auskunft geben.

Die meisten Access Points nehmen gleich vier verschiedene Keys auf, von denen ihr Euch für einen entscheiden müsst. Kleiner Tipp am Rande: Es schadet nicht, alle Schlüssel auszufüllen und alle paar Wochen einmal zu wechseln. Das bringt zusätzliche Sicherheit auf längere Sicht. Die Clients konfiguriert ihr auf den Key, auf den der Access Point geschaltet ist. Dazu benutzt man entweder das mitgelieferte Konfigurationstool vom jeweiligen Hersteller, oder die in Windows (nur XP!) integrierte drahtlose Netzwerkkonfiguration. Bilder sagen mehr als 1000 Worte, weshalb zur Orientierung die passenden Exemplare unten mit aufgeführt sind. Die Konfigurationstools sehen von Hersteller zu Hersteller anders aus, unterscheiden sich aber häufig mehr in ihrem Aussehen als im Aufbau und Funktion. Damit wäre der erste Schritt geschehen. Alles in allem ein Zeitaufwand von wenigen Minuten.

Dabei sei angemerkt, dass WEP keine 100 %ige Sicherheit bietet, wie noch zu den Anfängen des WLANs vermutet. Allerdings ist der Zeitaufwand immens, einen solchen Key zu knacken. Für die Berechnung des Keys werden mitunter Millionen gesendete Pakete benötigt, was bei einem heimischen Netzwerk schnell einige Stunden bis Tage dauern kann. Wer übrigens die Chance hat, WPA zu nutzen, der sollte dies tun. WPA (Wireless protected Access) ist eine erweiterte Variante von WEP und bietet mit einem verstärkten Initialisierungsvektor, Re-Keying und Message-Integrity Check insgesamt eine nochmals deutlich höhere Sicherheit. Allerdings unterstützen noch nicht alle Wireless-Komponenten diesen Standard. Access Points bieten zwar auch einen "Mixed Mode" an, der den simultanen Betrieb von WEP und WPA erlaubt. Der Haken an der Sache ist jedoch, dass das Netz sicherheitstechnisch wieder auf dem Stand von WEP-only ist. WPA bringt also nur etwas, wenn ausnahmslos alle Clients dies unterstützen.

## MAC-Filterung

### 2.Schritt: Filterung der physikalischen Adressen (MAC)

Praktisch jeder W-LAN-Access Point bzw. Router bietet die Möglichkeit, nur bestimmte MAC-Adressen zuzulassen. Die MAC-Adresse (auch physikalische Adresse genannt) ist für jede Netzwerkkarte individuell und nur einmal auf der ganzen Welt vergeben (so sollte es zumindest sein). Erst über diese Adresse ist der gesamte Netzwerkverkehr möglich. Die MAC-Adresse ist bei heutigen Karten 48 Bit (12 Hexadezimalstellen) lang und nach dem Muster XX:XX:XX:XX:XX:XX aufgebaut. Die einzelnen MAC-Adressen eurer W-LAN-Karten könnt ihr in der Eingabeaufforderung mit dem Befehl „ipconfig -all“ herauslesen. Oftmals stehen die Adressen auch auf dem Typenschild der W-LAN-Karte.

Jetzt hat man die Möglichkeit, dem Router zu sagen, dass er nur eure Karten zulassen soll. Dazu bemüht man sich wieder in das Webinterface und sucht sich das entsprechende Menü. Dort kann man entweder bestimmte Adressen zulassen, oder bestimmte Adressen aussperren. Hier ist die Variante mit dem „zulassen“ in den meisten Fällen einfacher. Ihr gebt eure Adressen in die dafür vorgesehene Maske ein und fügt sie der Liste der erlaubten MAC-Adressen zu. Der Rest wird damit sozusagen

ausgeschlossen. Zwar gibt es auch hier wieder die Möglichkeit, das Verfahren zu umgehen. So langsam muss es sich aber wirklich um ein immens wichtiges W-LAN handeln - der Aufwand für einen schnellen Scherz ist entschieden zu groß. Das Handbuch des Access Points kann auch hier wieder nützlich sein.

## SSID Verstecken

### 3.Schritt: Unsichtbare SSID

Der dritte Punkt ist das verschleiern der SSID. Die SSID gibt den Namen des W-LAN-Netzes an. Sie ist Praktisch so etwas wie die Windows Arbeitsgruppen, nur eben einige Netzwerkebenen niedriger. Ordentliche Access Points bieten hier die Funktion, genau eben diesen Namen nicht zu übertragen. Der Sinn dahinter liegt ganz einfach darin, dass das Netzwerk nach außen hin in gewisser Weise unsichtbar wird. Zwar wird das Netzwerk immer noch von sämtlichen Spoofing-Tools erkannt, aber ohne die SSID geht nun einmal gar nichts. Hilfreich ist wie immer das Webinterface. Die Hersteller bezeichnen diese Funktion oft unter dem Label „Broadcast SSID“ - ja oder nein. In dem Falle auf „nein“ klicken. So haben auch wieder nur die Clienten eine Möglichkeit zur Verbindung, die die SSID kennen. Die SSID sollte man somit - ebenso wie den WEP-Schlüssel - nicht unbedingt weiter erzählen. Ein Klick und gut. Mehr ist es wirklich nicht.

### Schlussworte

Ein weiterer Punkt, der eigentlich so selbstverständlich ist, aber leider - wie wir in dem kurzen Test feststellen mussten - nicht immer gegeben war, ist die Vergabe eines neuen Passworts für den Admin-Zugang zum Access Point oder Router. Hier sollte man unbedingt ein neues Passwort definieren, da man sich sonst relativ leicht unter Kenntnis des Herstellerstandards von außen Zugriff auf das Webinterface verschaffen kann. Gerade einige Produkte der Telekom (z.B. T-Sinus 154 WLAN Router) sind davon betroffen, da dort das Standardpasswort mit „0000“ auch noch extrem simple ausfällt. Bitte unbedingt drauf achten.

Natürlich gibt es noch einige weitere Optionen wie z.B. einen RADIUS-Server, welche jedoch nur für Firmen mit dementsprechenden Server-Equipment gedacht sind. Zu Hause braucht man so etwas nicht. Dennoch sollte man sich vor Augen halten, dass über Funk nie eine 100 %ige Sicherheit gegeben ist, wie es bei normalen LANs der Fall ist. Wer die Zeit und die Technik mitbringt, der kommt auch in gut geschützte Systeme rein. Die drei aufgeführten Funktionen bieten jedoch ausreichend Schutz für den Heimgebrauch und halten nahezu alle Angreifer auf Distanz.