SGAM.Informatics – Tip des Monats

Heinz Bhend
Leiter der Arbeitsgruppe «SGAM.Informatics»

Wireless LAN richtig konfigurieren

Die Vorteile des mobilen Einsatzes und der Flexibilität sind bestechend. Immer häufiger werden daher Intranetverbindungen, zumindest teilweise, als drahtloses sogenanntes Wireless LAN (WLAN) eingerichtet.
Mit wenigen Einstellungen lässt sich aus den unsicheren Standardkonfigurationen ein sicheres WLAN machen. Das ist keine grosse Hexerei und kann von jedem durchschnittlich versierten User vorgenommen werden.
Die meisten Konsolen (oft Standardbrowser) zur Verwaltung des Access Points bieten eine graphische Oberfläche. Damit kann mit wenigen Anpassungen das WLAN so konfiguriert werden, dass Spione und Trittbrettsurfer keine Chance haben.
Es gibt verschiedene Optionen, die einen möglichst hohen Grad an Sicherheit gewährleisten, den hundertprozentigen Schutz erreicht man aber nie. Das ist wie bei einem Haus: Man kann alle Läden, Türen und Fenster verriegeln, sämtliche Schränke abschliessen und eine Alarmanlage einbauen, trotzdem wird es einem Einbrecher immer irgendwie möglich sein, zum Beispiel durch einen unterirdischen Tunnel, ins Gebäude zu gelangen.

Abbildung 1
Wichtig: SSID Broadcast ausschalten.

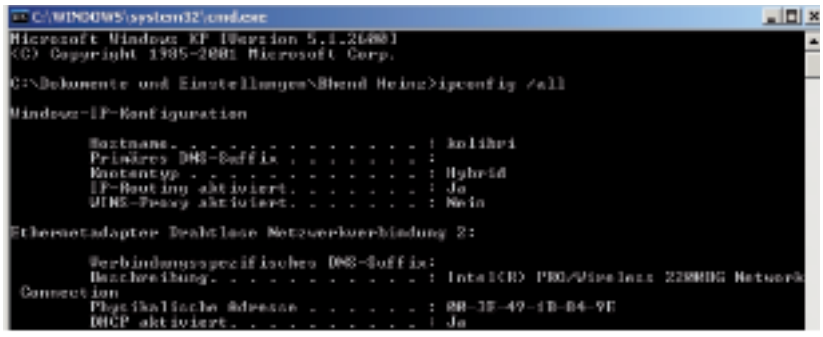

Abbildung 2
Übersicht über die Netzwerkkonfiguration des Computers.

Die folgenden fünf Punkte lassen sich mit geringem Aufwand bewerkstelligen und können so das Funknetz optimal absichern:

1. Administratorpasswort ändern

Der standardmässig eingestellte Benutzername und das vorgegebene Passwort sind für die entsprechenden Produkte jeweils im Internet abrufbar. Somit ist die erste und zwingende Massnahme, dieses Passwort zu ändern.

2. SSID ändern

Alle WLAN-Geräte tragen einen Netzwerknamen, die sogenannte SSID oder Service Set Identifier. Nur Geräte mit derselben SSID können miteinander kommunizieren. Ab Werk besitzen alle Access Points einen voreingestellten Netzwerknamen, der nicht individuell ist. Häufig sind es Namen wie «Default», «WLAN», «Wireless» oder auch einfach der jeweilige Produktename. Deshalb ist es wichtig, eine neue, eindeutige Bezeichnung einzugeben.

3. SSID Broadcast ausschalten

Die WLAN Access Points senden standardmässig ungefähr 100mal pro Sekunde ihren Netzwerknamen in den Empfangsbereich. Somit kommen Datenspione leicht in den Besitz der nötigen Anmeldeinformationen. Wird dieser Broadcast, also das Aussenden des Netzwerksignals, unterdrückt, weiss die Umgebung gar nicht, dass hier ein Access Point vorhanden ist. Es ist möglich, die SSID ganz auszuschalten, sie zu verbergen oder unsichtbar zu machen (Abb. 1).

4. MAC-Adressen filtern

Alle Netzwerkprodukte (Netzwerkkarten, Access Points usw.) tragen eine weltweit eindeutige Hardwarenummer, die sogenannte MAC-Adresse oder Media Access Control Address, in Form eines zwölfstelligen hexadezimalen Codes (z.B. 00–3E–49–1B–84–9E). Bei neueren Access Points oder Routern können die MAC-Adressen der Nutzer, die auf das Funknetz zugreifen dürfen, eingegeben werden. Konkret muss man jeden einzelnen User aufnehmen.
Um die MAC-Adresse eines PCs oder Notebooks zu erfahren, gibt man im Eingabefenster von «Start/Ausführen» den Befehl «cmd» ein, worauf ein DOS-Eingabefenster (schwarzweiss) auf dem Bildschirm erscheint. Nun gibt man den Befehl «ipconfig/all»

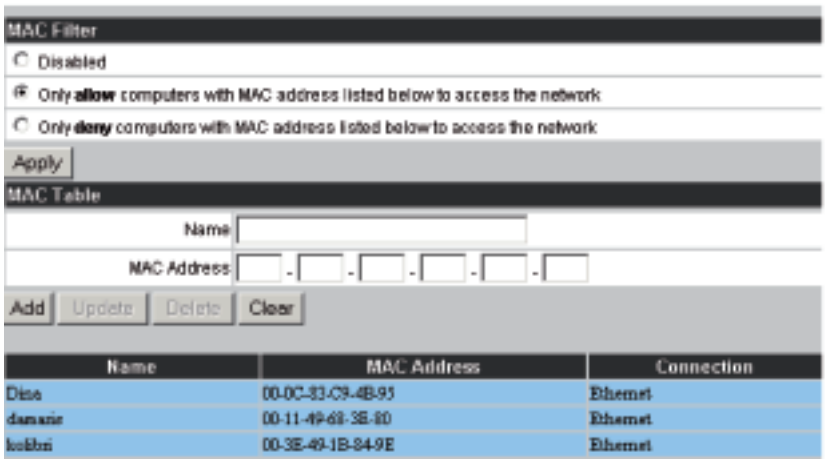

Abbildung 3
Der MAC-Filter regelt den Netzwerkzugang.

ein, und es wird eine Übersicht über die Netzwerkkonfiguration des Computers angezeigt (Abb. 2). Die «Physikalische Adresse» ist die gesuchte MAC-Adresse. Dieser zwölfstellige Code muss nun im Access Point registriert werden. Sobald der MAC-Filter aktiviert ist, können nur noch Geräte Verbindung aufnehmen, die in dieser Liste aufgeführt sind (Abb. 3).

5. Verschlüsselung einschalten

Jedes Datenpaket, das über das Funknetz verbreitet wird, ist normalerweise, das heisst ab Werk, unverschlüsselt. Wireless Router bieten die Möglichkeit, die Daten zu verschlüsseln, und zwar entweder via WEP (Wired Equivalent Privacy) oder WPA (Wi-Fi Protected Access).

Der Verschlüsselungsalgorithmus von WPA ist deutlich besser und konnte bisher nicht geknackt werden. Der WEP-Schlüssel bietet trotz eines 128-Bit-Verfahrens keinen hundertprozentigen Schutz. Daher sollte wenn immer möglich das WPA-Verfahren gewählt werden, wobei eine Verschlüsselung mit WEP immer noch besser ist als gar keine.

Fazit

Um Angreifer abzuwehren, muss man wissen, welche Angriffsstrategien es gibt:

- Wer sich in ein Funknetz einloggen will, muss zuerst wissen, dass eines vorhanden ist. Also wird er Router bzw. Access Points suchen, die ihr SSID-Signal aussenden. – Konsequenz: SSID Broadcast ausschalten.
- Wer sich als Hacker bei einem WLAN mit eingeschaltetem MAC-Filter einloggen will, muss viele Datenpakete abfangen, diese analysieren und aus diesen die entsprechenden MAC-Adressen extrahieren. Dieses Verfahren ist mit einem gewaltigen Aufwand verbunden. – Konsequenz: MAC-Filter einschalten.
- Grundsätzlich kann beim Datentransfer jedes Paket in einem Wireless-Netz abgefangen und die Information verarbeitet werden. Wenn die Pakete verschlüsselt sind, ergibt der Inhalt keinen Sinn und macht es einem Angreifer sehr schwer. Bei den heutigen Verschlüsselungsalgorithmen dauert das Hakken eines verschlüsselten Zugangs teilweise Monate bis Jahre, ein entsprechend kontinuierlicher Datentransfer vorausgesetzt. Dies ist sicherlich jenseits jeder Vorstellungsmöglichkeit und somit äusserst unwahrscheinlich. – Konsequenz: Verschlüsselung aktivieren.