Merkblatt

Merkblatt “Sicherer Betrieb eines Wireless-LAN“

1. Zweck des Merkblattes

Der Einsatz von Funknetzen hat in den letzten Jahren verständlicherweise ständig an Bedeutung gewonnen. Die Vorteile der kabellosen Verbindung sind unbestritten: Endlich ist der langersehnte mobile Arbeitsplatz Wirklichkeit geworden.

Erschreckend ist aber noch immer das Sicherheits-Niveau: Obwohl sich viele Betreiber von Funknetzen in der Zwischenzeit der Gefahr bewusst zu sein scheinen, sind noch immer viele Funknetze offen und können problemlos gehackt werden.

Dieses Merkblatt soll aufzeigen, dass der Betrieb eines unsicheren Funknetzes grosse Risiken mit sich bringt und wie Sie ein W-LAN mit der grösstmöglichen Sicherheit konfigurieren.

2. Gefahrenquelle W-LAN

Funknetze sind häufig so eingestellt, dass sie weit über das eigentlich nötige Einsatzgebiet hinaus senden. Sogenannte „Wardriver“ haben es sich zum Sport gemacht, mit einem Notebook und laufender Sniffer-Software durch die Quartiere zu ziehen, - auf der Suche nach W-LANs. Die meisten dieser „Wardriver“ sind harmlos und amüsieren sich lediglich an der Unprofessionalität der Betreiber.

Diese Tatsache darf aber kein Grund für das Betreiben eines unsicheren Funknetzes sein. Denn Daten sind nach wie vor das Kapital vieler Unternehmen und ein erfolgreicher Angriff könnte verheerende Folgen haben. Man denke dabei nur was zu erwarten wäre, wenn geheime Daten eines Arztes veröffentlicht oder wichtige Forschungsergebnisse eines Labors in falsche Hände gelangen würden. Jeder Inhaber von Datensammlungen ist für die Sicherheit der Daten gegenüber Kunden, Lieferanten und Mitarbeiter verantwortlich.

3. Sichere Konfiguration eines W-LANs

Nachfolgend finden Sie einige wichtige Punkte für eine möglichst sichere Konfiguration eines Funknetzes aufgelistet. Es gilt dabei aber zu beachten, dass die Technik einem schnellen Wandel unterzogen ist und als sicher geltende Technologien in kurzer Zeit unsicher werden können. Die Betreiber von Funknetzwerken sind für die Sicherheit ihres W-LANs verantwortlich. Es empfiehlt sich regelmässig die neusten Berichte zu lesen und die Hard- und Software auf den neusten Stand der Technik zu bringen.

Reichweite der Signale beschränken
Die einfachste und wahrscheinlich die effektivste Massnahme ist die Beschränkung der Reichweite der Signale auf das benötigte Zielgebiet. Je kleiner die Reichweite, umso geringer ist die Gefahr, dass unerwünschte Besucher ihr Netzwerk überhaupt sehen und hacken können. In den meisten Fällen ist es gar nicht nötig, das bestehende Funknetz mit zusätzlichen Antennen und Access-Points auszubauen. Müssen dennoch zusätzliche Antennen benützt werden, so empfiehlt es sich ein Modell zu kaufen, welches die Signale punktgenau an einen anderen Ort sendet und diese nicht in alle Himmelsrichtungen streut. Ebenso wichtig ist die Position des Access-Points. Wird er direkt am Fenster positioniert, so reichen seine Signale bis auf die Strasse hinaus und können von Hackern problemlos abgefangen werden.
Viele WLAN-Router bieten heute die Möglichkeit den Access-Point (den Sender) für eine vordefinierte Zeitspanne (z.B. von 23:00 – 06:00) auszuschalten. Somit vermindern Sie die Angriffsmöglichkeit auf Ihr WLAN.

Netzwerknamen ändern
Die SSID (Service Set Identifier) bezeichnet den Namen des Funknetzes. Wer sich in ein Netz einwählen möchte, muss diesen Namen kennen. Ändern Sie den Namen des Netzwerkes und wählen Sie eine nicht zu erratende SSID. Die vorgegebenen Namen der Hersteller dürfen keinesfalls verwendet werden. Deaktivieren Sie das SSID Broadcasting.

WPA2-Verschlüsselung
WPA2 (Wi-Fi Protected Access 2) ist ein Sicherheitsstandard im W-LAN, der sowohl für die Verschlüsselung der Datenübertragung als auch für die Benutzerauthentifizierung zuständig ist.
Für WPA und WPA2 sind bis jetzt nur Passwort-Angriffe bekannt. Aus diesem Grund ist es dringend zu empfehlen, ein ausreichend langes Passwort (wenn möglich 63 Zeichen lang mit Gross- und Kleinbuchstaben sowie Sonderzeichen und Zahlen) zu verwenden. Der Passwortschlüssel kann z. B. mit einem USB-Stick einfach auf die angeschlossenen Clients übertragen werden und muss nach der einmaligen Installation nicht mehr geändert werden. Ein mit ausreichend langem Passwort geschützter Wireless-Router mit WPA2-Verschlüsselung gilt aus heutiger Sicht als praktisch unknackbar.
Aus diesem Grund muss bereits beim Kauf der W-LAN Hardware auf die Unterstützung der WPA und WPA2 Verschlüsselung geachtet werden.

Einschränkung der MAC-Adressen
Die meisten Router erlauben es, den Zugang zum Netzwerk auf vordefinierte MAC-Adressen zu beschränken. Dadurch wird ein potenzieller Eindringling mit einer unbekannten MAC-Adresse bereits an der Eingangstür abgeblockt. Auch hier gilt es zu beachten, dass mit bestehenden Hacker-Tools gültige MAC-Adressen simuliert werden können.

Einsatz von VPN
Die sicherste Methode ein W-LAN vor Hackern zu schützen, ist zurzeit der Einsatz von VPN (Virtual Private Networks). Viele ADSL-Router bieten heute bereits eine VPN-Verbindungs-Lösung an. Wenn Sie schützenswerte Daten in ihrem Netzwerk bearbeiten, so ist der Einsatz von VPN zwingend notwendig. Wir empfehlen auch sensitive Daten mit einem speziellen Programm zu verschlüsseln und diese verschlüsselt zu speichern.

Weitere wichtige Punkte für ein sicheres W-LAN
In jedem Fall ist immer eine Firewall einzusetzen, um die ein- und ausgehenden Verbindungen zu kontrollieren und diese falls nötig auf bestimmte IP-Adressen zu beschränken. Mit einer "Intrusion Detection"-Software können Attacken von Aussen erkannt und abgeblockt werden. Der Einsatz eines Virenschutz-Programms ist ebenfalls notwendig. Diese Massnahme kann zwar nicht das Eindringen von Hackern verhindern, aber die allfällig hinterlassenen Viren werden beseitigt. Zusätzlich können Sie die Dateien mit einer Verschlüsselungs-Software (z.B. PGP, Pretty Good Privacy) verschlüsseln, was für Hacker eine weitere Hürde darstellt.

4. Vorsicht mit geheimen Daten

Grundsätzlich ist aber davon auszugehen, dass kein Funknetz zu 100% sicher ist, auch wenn es mit allen Sicherheitsmechanismen ausgestattet ist. Wenn sich ein professioneller Hacker daran macht in ihn Netzwerk einzudringen, wird er es bei entsprechendem Geschick früher oder später höchstwahrscheinlich knacken können. WEP-Verschlüsselung können mit frei verfügbaren Tools gehackt werden und MAC-Adressen können abgehört und manipuliert werden. Ein W-LAN sollte entsprechend nur mit einem hohen Sicherheitsstandard betrieben werden, um einen unbefugten Zugriff zu verhindern. Jeder Betreiber sollte sich regelmässig über den aktuellen Stand der Technologie- und Sicherheitsempfehlungen informieren und diese umsetzen.

Infosurance ist ein Verein zur Förderung der Informationssicherheit in der Schweiz, welcher von grossen Unternehmungen und vom Bund gegründet wurde. Ziel ist es die Schweizer Bevölkerung im Umgang mit Informationstechnologien zu sensibilisieren.

Eine Aktion von:

InfoSurance
und Ihr Computer ist sicher.

Unterstützt durch: Industrie, Verwaltung und Bildung