Wirksamer Schutz

Einsatz und Risiken von Wireless LAN

Die Anzahl von Wireless LAN Access Points nimmt ständig zu. Nicht nur in privaten Haushalten, sondern immer mehr auch in kleinen und mittleren Unternehmen kann man die kleinen Geräte entdecken. Sie ermöglichen schnell eine Verbindung ins eigene Netzwerk aufzubauen, ohne viele Kabel installieren zu müssen.

Autor: Andreas Wisler

Auf der anderen Seite wird es immer schwieriger, wenn nicht gar unmöglich ein mobiles Gerät ohne Wireless zu finden. Praktisch alle Anbieter rüsten ihre Geräte mit diesem Kommunikationsmedium aus. Doch die schnelle Installation birgt auch Ihre Risiken. Nur wenige Firmen setzen sich mit den Problemen von Wireless LAN Access Points oder den Wireless Endgeräten auseinander.

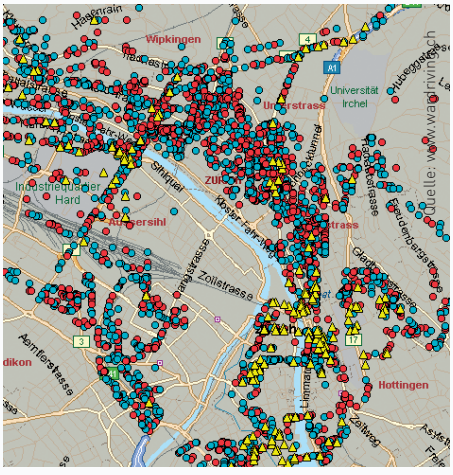
So öffnet man ohne es zu Wissen eine Möglichkeit von Aussen ins eigene Netzwerk zu gelangen.Die Gefahren der neuen Technik sind mannigfaltig:

- So kann z.B. ein Mitarbeiter einfach einen Access Point unter seinem Pult betreiben, um sich so seine Arbeit zu erleichtern, ohne ständig ein Kabel mit sich herum führen zu müssen – und damit einen ungeschützten Zugang zum Firmennetzwerk öffnen.
- Da viele Geräte mit aktiviertem Wireless LAN ausgeliefert werden, ist es auch ohne Access Point möglich, eine Verbindung aufzubauen. Man nennt diese Technik Peer-to-Peer (P2P). Auch dies lässt den Zugriff von aussen auf das Netzwerk zu.
- Die Strahlung von Access Points hört oft nicht an den Aussenwänden eines Büros auf, sondern geht durch die Wände auf die Strasse. Auch wenn der Sender zentral positioniert wird, können die Strahlen mit speziellen Empfängern und entsprechenden Antennen sowie Vorverstärkern noch in hundert Metern (!) empfangen werden.

Beihilfe zur Spam-Verbreitung

Oft hört man auf diese Risiken der Wireless LAN Technik den Einwand, dass eh niemand an den eigenen Daten Interesse hat. In den meisten Fällen hat diese Person auch Recht. Aber schon die Mitbenutzung des Internetzuganges für illegale Methoden (sei dies nun für die Spam-Verbreitung, Tauschbörsen oder weit schmutzigere Dinge), bringt das Unternehmen in grosse Schwierigkeiten. Wie kann man der Untersuchungsbehörde beweisen, dass nicht das Unternehmen oder seine Mitarbeiter für diese Umstände verantwortlich sind, sondern ein Fremder? Praktisch nicht möglich.

Es ist erstaunlich, wie viele Netzwerke von Privaten, und auch sehr vielen Firmen, ungeschützt verfügbar sind. Wardriver haben es sich zum Hobby gemacht, diese aufzuspüren, um auf diese Gefahren aufmerksam zu machen. In Gruppen sind diese in ihrem Auto unterwegs und versuchen mit allerlei Technik, diese zu finden, zu kartographieren (GPS sei Dank) und im Internet zur Schau zu stellen. Eine Schweizer Seite findet man z.B. unter www.wardriving.ch. Die Ergebnisse sind erschreckend:



Die hellblauen Punkte in der Grafik zeigen ungeschützte Access Points. Ein eigener ADSL Zugang ist praktisch nicht nötig, garantiert gibt es jemanden in der Nachbarschaft, der einem sein Netzwerk kostenlos zur Verfügung stellt.
Mit der Einführung der Wireless Technik 802.11 wurde diesem erhöhten Schutzbedarf mit der Verschlüsselung WEP (Wired Equiva-

lent Privacy) Rechnung getragen. Wie sich leider schon kurz darauf herausstellte, wurde bei dessen Implementierung ein folgeschwerer Fehler gemacht. Es ist egal, ob man einen Schlüssel mit der Länge 40 oder 512 Bit verwendet oder gar ein anderes Kryptographieverfahren einsetzt, es wird immer nur ein einziger Schlüssel verwendet.

Schon nach relativ kurzem Abhören des Funkverkehrs lässt sich die Verschlüsselung knacken. Dafür sind diverse, kostenlos verfügbare Tools im Internet zu finden. Auch das Ändern der SSID (Service Set Identifier) bringt hier absolut keinen Vorteil. Auch dafür sind Programme verfügbar, die auch bei verschlüsseltem Datenverkehr diese Kennung in sekundenschnelle „ausspucken". Alle diese Gründe haben dazu geführt, dass viele (grössere) Firmen den Einsatz von Wireless LAN strikt verbieten. Doch es gibt Möglichkeiten, ein Wireless Netzwerk sicher und komfortabel zu betreiben.

Es ist erstaunlich, wie viele Netzwerke von Privaten, und auch sehr vielen Firmen, ungeschützt verfügbar sind.

WPA – Sicherheit dank wechselnder Schlüssel

Um die Risiken von WEP zu eliminieren, wurde WPA (WiFi Protected Access) als Nachfolger eingeführt. Die Vorteile liegen in der dynamischen Schlüsselverwaltung (TKIP - Temporal Key Integrity Protocol) sowie der gegenseitigen Authentifizierung.

1. **Dynamische Schlüsselverwaltung**
   Für den Datenaustausch wird nicht mehr ständig der gleiche Schlüssel verwendet, sondern nach dem Aufbau wird für die aktuelle Verbindung ein temporärer Schlüssel gewählt. So kann garantiert werden, dass für jede neue Verbindung ein anderer Schlüssel zum Einsatz kommt. Die Verwaltung dieser Schlüssel kann wahlweise durch einen RADIUS-Server oder durch Pre-Shared-Keys erfolgen. Der Pre-Shared-Key, d.h. ein selber definiertes Kennwort, ist jedoch anfällig auf so genannte Brute-Force Attacken. Hier wird durch spezielle Tools versucht, mit ständig wechselnden Passworten an das korrekte Geheimnis zu gelangen.

   Da ein schwaches Passwort (Namen, Zahlen, etc.) sehr schnell gefunden wird, sollten immer genügend lange und zusammengesetzte Passworte verwendet werden. Dies ist aber ganz klar keine Schwachstelle von WPA, sondern abhängig vom Benutzer.

Zum Autor

Andreas Wisler
(052 320 91 20) ist Geschäftsführer der GO OUT Production GmbH mit Sitz in Wiesendangen, welche sich mit IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt.
Er unterrichtet in der Klubschule Migros den Lehrgang „IT-Security Manager", darüber hinaus veröffentlicht er regelmässig die Infonews zu aktuellen Sicherheitsthemen. Dieser informative Newsletter kann kostenlos und unverbindlich auf www.goSecurity.ch bestellt werden. (Ausgabe 4/04 beschäftigte sich ausführlich mit dem Thema WLAN-Sicherheit.)

2. Gegenseitige Authentifizierung
Durch die gegenseitige Authentifizierung können beide Stationen sicher sein, dass sie sich mit dem richtigen Gesprächspartner verbunden haben. Es genügt nicht mehr, nur das gemeinsame Passwort zu kennen, sondern man muss sich eindeutig zu erkennen geben. Dies geschieht mittels dem Protokoll EAP, auf welches an dieser Stelle nicht weiter eingegangen wird. Eine Man-in-the-Middle Attacke, bei welcher ein potentieller Angreifer den Verkehr über den eigenen Rechner weiterleitet, ist somit ausgeschlossen.

Die meisten heute verfügbaren Geräte unterstützen WPA. Ältere Geräte müssen durch ein neues Firmware (d.h. eine neue Basissoftware, eine Art Betriebssystem) aktualisiert werden. Die Homepage des Herstellers gibt darüber Auskunft, ob dies bei Ihrem Access Point möglich ist.
Auch Windows XP unterstützt seit dem Patch Q815485 (in Service Pack 2 integriert) WPA. Somit ist es möglich, den neuen Standard auch in bestehenden Windows-Netzwerken zu nutzen.

IPsec – Verschlüsselung ohne WPA

In vielen bestehenden Wireless-Netzwerken wird der Einsatz von WPA nicht möglich sein. Doch auch mit „alten" Access Points ist ein Schutz möglich. Dieser ist jedoch nicht mehr so einfach realisierbar, wie die integrierte Lösung WPA. Der Einsatz von IPsec ermöglicht trotz ungeschütztem Wireless Netzwerk die übertragenen Daten zu verschlüsseln.
Dabei werden auf dem Sender wie auf dem Empfänger die notwendigen Angaben für Verbindungsaufbau und Verschlüsselung hinterlegt. Der Verwaltungsaufwand ist dabei nicht unerheblich.

Schutz der mobilen Geräte

Wie eingangs erwähnt, bieten immer mehr mobile Endgeräte (Notebooks, PDAs, Handys, etc) die Möglichkeit, Funkverbindungen aufzubauen. Auch ohne Access Points können diese Geräte untereinander kommunizieren. Damit das Gerät auch gefunden wird, senden diese in regelmässigen Abständen ein „Hallo"-Signal an die Umwelt. Gerade jetzt, wo die Tage wieder länger werden, genügt es z.B. am Bellevue in Zürich, etwas zu warten und man findet einen mobilen Gesprächspartner.
Dabei wäre es so einfach, das eigene Gerät vor fremden Augen zu schützen. Die meisten Hersteller statten das mobile Arbeitsinstrument mit einem Knopf oder Schalter aus, mit welchem die Netzwerkkarte deaktiviert wird. Einen besseren Schutz gibt es nicht.

Viele Untersuchungen zeigen jedoch, dass trotz vorhandenen Möglichkeiten viele Wireless LAN Netzwerke nicht oder nur ungenügend geschützt sind. Die Gefahr vor Missbrauch oder gar Manipulation, Zerstörung oder Diebstahl von Daten ist dabei nicht unerheblich. Oft ist es den Betreibern gar nicht bewusst, dass es sehr einfach möglich ist, dies auszunutzen. Der Schutz des eigenen Netzwerkes ist dabei aus vielen Perspektiven ein absolutes Muss.

Kontrollieren Sie daher in regelmässigen Abständen, ob Ihr Netzwerk (noch) sicher ist. ◆