War-Driving

So spüren Sie WLANs auf

Ein Wireless LAN (WLAN) bietet einiges an Bequemlichkeit. Der Faktor Komfort trifft für beide Seiten zu: Mitarbeiter finden es praktisch, ohne Kabelanschluss im Netz zu sein; die EDV-Abteilung profitiert davon, Gebäudebereiche ohne Kabelverlegung mit einem Netzzugang zu versorgen. Aus Sicherheitsgründen sollten jedoch alle WLAN-Zugänge autorisiert und gesichert sein. Wir zeigen, wie Sie ungenehmigte Zugänge, die ein großes Risiko für die Datensicherheit darstellen, aufspüren.

Wireless LANs sind extrem populär geworden, seitdem DSL-Anbieter neuen Kunden einen WLAN-fähigen DSL-Router schenken. Dadurch haben viele Beschäftigte bereits Erfahrungen im Umgang mit der drahtlosen Technik gewonnen. Und was daheim praktisch und bequem ist, möchten sie am Arbeitsplatz nicht missen.

Selbstgestrickte WLANs gefährden die Unternehmenssicherheit

Wenn der Arbeitgeber kein WLAN zur Verfügung stellt, installieren manche Mitarbeiter schon mal ihren privaten DSL-Router in Eigeninitiative.

Über die Auswirkungen einer solchen Aktion auf die Sicherheit des Firmennetzes machen sich diese Kollegen keine Gedanken. Auch Industriespione können natürlich WLANs installieren.

Daher gehört es heute zu den Standard-Sicherheitsmaßnahmen, die unerlaubten Access-Points zu erkennen, damit man die nicht autorisierten Geräte aus dem Verkehr ziehen kann.

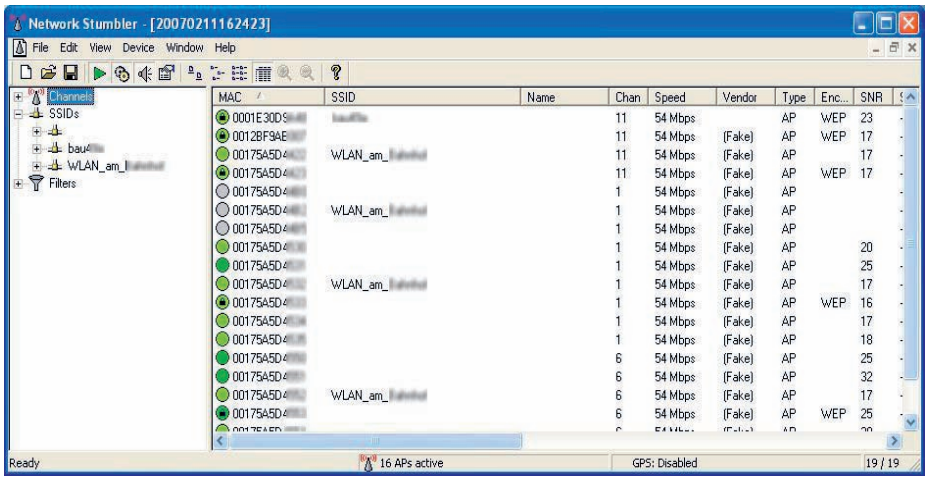
Auf der Suche nach der Funkwelle

Während Kabel wohldefiniert auf dem Firmengelände verlegt sind, stoppen Funkwellen nicht am Zaun des Firmengeländes. Hinzu kommt, dass die Ausbreitungseigenschaften der hochfrequenten Wellen nicht ganz so offensichtlich sind wie die von Licht.

Sie müssen daher ausmessen, wo überall Empfang und damit Netzzugang möglich ist.

Die systematische Netzsuche mit Notebook oder PDA

Das War-Driving per Auto oder War-Walking zu Fuß setzt nur einige einfache Werkzeuge voraus. Neben einem Notebook oder PDA mit Windows Mobile benötigen Sie lediglich eine geeignete Software.



Das Programm Network Stumbler beim Scannen auf einem Firmengelände.

Solange Sie überschaubare Bereiche untersuchen, können Sie auf einen GPS-Empfänger verzichten. Wenn es jedoch um große Gelände geht, bietet der GPS-Empfänger den Vorteil der automatischen räumlichen Zuordnung.

Alle Programme können anzeigen, ob das WLAN mit WEP, WPA oder WPA2 verschlüsselt ist oder nicht.

Die Suche nach einem WLAN an sich ist gesetzlich nicht verboten

Während die reine Suche nach einem WLAN nach derzeitiger Rechtslage straffrei ist, wäre das Knacken der Verschlüsselung nach § 202a StGB eine Straftat, da versucht wird, einen technischen Schutz zu umgehen.

Frei verfügbare Scan-Software für PDAs

Für einen Windows Mobile PDA mit WLAN-Karte gibt es drei frei verfügbare Scan-Software-Produkte:

- Pocket Warrior
- Mini-Stumbler
- WiFiFoFum

In der Grundfunktionalität unterscheiden sich die drei Programme nicht. Alle unterstützen GPS-Empfänger.

PDAs haben recht schwache Antennen. Dies ist meist ein Nachteil, aber bei der Lokalisierung eines unbekannten Funkers hilft dies, da man schon für einen guten Empfang sehr nah sein muss.

Unauffälliges War-Walking per PDA

Im Unternehmen können Sie mit einem PDA in der Jackentasche ausgesprochen unauffällig ein War-Walking durchführen. Die Auswertung der Log-Dateien kann dann später im Rechenzentrum erfolgen.

Die Netzsuche per Notebook unter Windows und Linux

Wird ein ausgewachsenes Notebook zur WLAN-Suche herangezogen, stellt

Begriffserklärungen

Access-Point: Ein einfacher Konverter, der die Netzwerkpakete aus dem Funknetz auf das Kabel und umgekehrt umsetzt.

MAC-Adresse: Eine sechs Byte lange – theoretisch weltweit eindeutige und nicht änderbare – Adresse der Netzwerkkarte. Die ersten drei Bytes kodieren den Hersteller. Die weiteren drei Bytes nummerieren die einzelnen Netzwerkkarten des Herstellers durch.

War-Driving: systematisches Suchen nach Wireless LANs mithilfe eines Fahrzeugs. Der Begriff leitet sich von War-Dialing ab, einer Methode, durch Durchprobieren vieler Telefonnummern offene Modem-Zugänge zu finden.

WLAN-Router: Ein Router, der ein funkbasiertes Netzwerksegment mit dem Kabelnetz verbindet. Diese Router beherrschen häufig auch eine Adressumsetzung und haben eine Firewall eingebaut.

sich zuerst die Frage nach dem Betriebssystem. Während kommerzielle Tools eher aus der Windows-Ecke kommen, sind die freien Tools meist unter Linux verfügbar.

Unter Linux zählen Kismet und Wellenreiter zu den gängigsten Programmen. Sie lassen sich problemlos von der Knoppix-STD-CD (STD = Security Tool Distribution) starten. Die dauerhafte Installation des Linux-Betriebssystems ist nicht erforderlich.

Unter Windows hat sich der Network Stumbler (der große Bruder des Mini-Stumblers) bewährt.

Richtantenne zur Absicherung des Firmengeländes

Für größere Aktionen, insbesondere zur Absicherung des Firmengeländes nach außen, empfiehlt sich der Einsatz einer größeren Richtantenne. Damit lassen sich auch schwächere Signale nachweisen.

Es muss immer damit gerechnet werden, dass auch ein Lauscher von außen eine entsprechende Antenne verwendet. Berühmt sind hier die Selbstbauantennen aus einer zweckentfremdeten Pringles-Dose. Bauanleitungen dazu findet man im Internet.

Access-Points mit einem Netzwerk-Scan erkennen

Jeder Access-Point oder WLAN-Router im Firmennetz, der an eine Netzwerksteckdose angeschlossen ist, lässt sich durch einen Netzwerk-Scan z.B. mit dem Portscanner nmap finden. Über die Netzwerksteckdose kann man dann den genauen Ort bestimmen.

Diese Methode versagt, wenn der heimlich angeschlossene WLAN-Router die MAC-Adresse eines zugelassenen Rechners oder Notebooks im Netz bekommt. Dann würde keine unbekannte MAC-Adresse im Firmennetz gefunden.

Auffälligkeiten verraten den Lauscher

Da diese Netzwerkscanner aber versuchen, das Betriebssystem des Rechners festzustellen, lassen sich so eventuell Auffälligkeiten finden: z.B. wurde aus dem Windows-Rechner ein Linux/Unix-Rechner, es fehlen bestimmte Dienste u.Ä.

Die Netzsuche per USB-Stick – einfach und günstig

Für Preise von rund 50 Euro bekommen Sie heute schon spezielle WLAN-USB-Adapter, die Sie auch ohne Notebook benutzen können. Gespeist von einem eingebauten Akku scannen sie nach WLANs und zeigen auf einem kleinen LCD-Display erreichbare Funknetze an. Dies ist die einfachste Möglichkeit, derartige Netze zu finden.

Aufgrund des kleinen Displays ist die angezeigte Information sehr beschränkt. Aber Feldstärke, Sicherheitseinstellung, Kanal, Funkband und SSID werden angezeigt. Allerdings lassen sich diese einfachen Geräte nicht mit einem GPS-Empfänger koppeln.

WLANs erfordern Sicherheitschecks

Wer ein WLAN im Einsatz hat, sollte sich davon überzeugen, wie die Empfangsqualität außerhalb des Firmengeländes ist, um ungebetene Lauscher zu verhindern.

Unabhängig davon sollte man regelmäßig nach unbekannten Access-Points oder WLAN-Routern suchen, um die nicht autorisierten Geräte aus dem Verkehr ziehen zu können. Je sensibler der Bereich ist, desto häufiger sollten Sie auf die Suche gehen!

Prof. Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der FH München.

Industrie-Spionage über das WLAN

Um Ressourcen eines Unternehmens auszuspionieren, versucht der Spion, auf das Netz des Unternehmens zuzugreifen. Dies lässt sich einfach realisieren, indem er einen Access-Point an eine unbenutzte Netzwerkdose, etwa in einer Putzkammer, anschließt. Er kann ihn dann von außen, z.B. aus einem geparkten Auto, auslesen. Mit der zunehmenden Verbreitung von Power-over-Ethernet ist auch die Stromversorgung kein Problem mehr.

Da viele populäre WLAN-Geräte ein Linux-basiertes Betriebssystem haben, gibt es alternative Betriebssysteme für diese Router. Am bekanntesten ist OpenWRT. Damit lassen sich relativ einfach auch eigene (Spionage-)Tools auf diesen WLAN-Geräten installieren.