

HELPDESK

WLANs zu Unrecht verteufelt

Jede Woche beantworten Sicherheits-
experten Leserfragen und geben
Ratschläge, wie sich die Sicherheit in
einem Unternehmen erhöhen lässt.

Frage: Was gilt es bei der Inbetriebnahme eines WLANs aus Security-Sicht zu beachten?

Manche Unternehmen verbieten den Einsatz von WLAN (Wireless Local Area Network) mit den Argumenten, dass kabellose im Vergleich zu kabelbasierten Netzwerken per se unsicherer sind, da sie quasi einen virtuellen Netzwerkstecker ausserhalb des Gebäudes bieten und der Aufwand, eine sichere Lösung zu implementieren sehr aufwändig sei. Doch das zweite Argument stimmt nur bedingt.

Generelle Überlegungen: Am Anfang stellt sich die Frage ob, vor wem und wie lange die mit dem WLAN in Verbindung stehenden Ressourcen geschützt werden müssen oder sollen – typische Aspekte jeder IT Bedrohungs- und Risikoanalyse. Wenn das WLAN ausschliesslich den bequemen Internetzugang in Sitzungszimmern ermöglichen soll, also keine physikalische Verbindung zum eigenen LAN besteht, dann sollte aus juristischer Sicht lediglich verhindert werden, dass sich Unberechtigte einloggen können, weil dies die WLAN-Betreiberin kompromittieren könnte.

Weitergehende Massnahmen sind nur hinderlich, weil der Internetverkehr von interessierten Kreisen auch an anderen Punkten abgelauscht werden könnte und Besucher bei vom Access Point geforderter Kommunikationsverschlüsselung die Konfiguration ihres Systems temporär verändern müssten – was umständlich oder teilweise auf Grund der Sicherheitseinstellungen nicht möglich ist. Falls die Betreiberin des WLANs mit schützenswerten Daten ar-

«WPA2 erfüllt sogar die strengen Sicherheitsvorschriften nach FIPS 140-2.»

beitet und via WLAN der direkte Zugriff auf das eigene LAN ermöglicht wird, dann muss die Infrastruktur mit geeigneten Massnahmen zuverlässig vor jeglichem Zugriff von Unberechtigten geschützt werden.

Massnahmen: Nur Clients mit aktivierter Firewall und Anti-Virenschutz verwenden. Kabellose Kommunikationsschnittstellen (WLAN, Bluetooth und Infrarot) nur bei Bedarf für die Dauer der unmittelbaren Nutzung aktivieren und anschliessend wieder deaktivieren. Authentifizierungsme-



ILLUSTRATION: COWTHU

chanismen und Kommunikationsverschlüsselung erschweren unerlaubten Zugriff und Sniffing. WLAN, welche den direkten Zugriff auf das eigene LAN ermöglichen, sollten generell verschlüsselt werden. Allerdings bietet WEP (Wired Equivalent Privacy) auf Grund der schwachen Verschlüsselung keinen ausreichenden Schutz. WPA (Wi-Fi Protected Access) und sein Nachfolger WPA2 fordern die Verschlüsselung mit AES (Advanced Encryption Standard). WPA2 erfüllt gar die strengen Sicherheitsvorschriften für den Datenaustausch der US-Behörden nach FIPS 140-2.

Mit Access Points für den Profieinsatz lassen sich virtuelle LAN (VLAN) einrichten, deren einzelne Netzwerke voneinander getrennt sind, aber dennoch die gemeinsame Nutzung bestimmter Ressourcen ermöglichen. Wem dies noch immer zu unsicher ist, kann zusätzlich ein VPN (Virtual Private Network) einrichten. Access Points oder deren Antennen sollten nach Möglichkeit so weit wie möglich im Gebäudeinnern positioniert werden – Ausnahme: öffentlich zugänglicher oder nicht überwachbarer Bereich im Inneren.

Metallfassaden und spezielle auf Fenstern oder Wänden anzubringende Folien schirmen den Einzugsbereich um Access Points oder Antennen erfolgreich ab. Den gleichen Effekt haben Fenster mit erhöhtem Bleigehalt, wie sie beispielsweise bei Banken, im militärischen und im diplomatischen Sektor zum Einsatz kommen. Eine simple Zeitschaltuhr, welche die daran angeschlossenen Access Points nur zu den gängigen Arbeitszeiten mit Strom versorgt, verhindert Missbrauch ausserhalb der Arbeitszeit. Firmen, welche mobile Barcodeleser einsetzen, sollten die Anschaffung einer zusätzlichen Firewall prüfen, welche das LAN vor unerlaubtem Zugriff via vorgetäuschten «Barcodeleser» abschottet. ■



Der Autor
Christoph Baumgartner ist CEO und Senior Consultant bei OneConsult, Thalwil, www.oneconsult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch