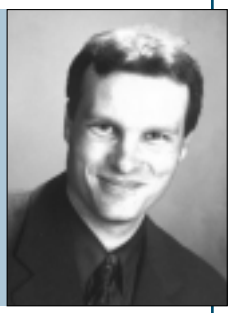
Alle Sicherheitslücken beseitigt?



von Kai-Oliver Detken

Ein Wireless LAN (WLAN) basiert auf dem definierten Standard der IEEE 802.11 und bietet die Möglichkeit, mit geringem Aufwand und auf sehr flexibler Basis drahtlose lokale Netze aufzubauen. In den meisten Fällen wird es als Erweiterung des bestehenden Festnetzes angesehen, kann aber auch als Alternative zu einer Kabelinstallation eingesetzt werden. In den letzten Jahren sind WLANs immer populärer geworden. Allerdings geriet ihre Sicherheit immer mehr in Verruf, als findige Studenten der Universität Berkeley im letzten Jahr den WEP-Algorithmus von WLANs hackten. Da aber WLANs auch in sehr sensiblen Umgebungen eingesetzt werden, sollte gerade die Security kontinuierlich nachgefragt werden.

Folgende Sicherheitsschwächen lassen sich auflisten:

- Grundeinstellungen: keine Aktivierung von Sicherheitsmechanismen in der Standardkonfigurationen;
- MAC-Adressen: relativ einfaches Abhören und Manipulieren der MAC-Adressen (Medium Access Control) eines WLAN, dadurch werden Access-Filter unbrauchbar;
- Wired Equivalent Privacy (WEP): WEP verwendet den RC4-Algorithmus zur Verschlüsselung. Er besteht aus 40 oder 128 bit und muß vorab den Clients und Access Points zur Verfügung stehen. 40 bit sind aber viel zu kurz, was ebenfalls auf die Länge von 24 bit des Initialisierungsvektors zutrifft, wodurch auch der 128-bit-Schlüssel angreifbar wird.

Die Schwächen des WEP-Protokolls sind bereits ein ausreichender Grund, keine sensiblen Daten über WLANs zu übertragen. Nach dem Hacken der Verbindung können auch Datenpakete gefälscht und die Authentisierung gebrochen werden. Neben den direkten Angriffen auf WEP gibt es noch passive Angriffsmöglichkeiten mittels RC4. Inzwischen sind sogar Tools im Internet erhältlich, die es auch weniger visierten Angreifern ermöglichen, das WEP-Protokoll zu hacken. Dafür müssen allerdings immer noch ungefähr 4 bis 6 Mio. Pakete erfolgreich abgehört werden.

Obwohl bereits bei mäßiger Auslastung des WLAN der Schlüssel relativ schnell ermittelt werden kann, sollte ein regelmäßiger Schlüsselwechsel automatisch initiiert werden, damit ein Angreifer gezwungen ist, immer wieder neu den Schlüssel zu ermitteln. Allerdings ist eine automatische Verteilung problematisch, da WEP kein Schlüsselmanagement kennt. So muß auf jedem Access Point der Schlüssel statisch eingetragen werden. Aus diesem Grund werden in der Praxis die Schlüssel selten oder gar nicht gewechselt. Hinzu kommt, daß der geheime Schlüssel oftmals auf der Festplatte oder bei Windows-Betriebssystemen direkt in die Registry-Datei eingetragen wird.

Zudem breiten sich die Funkwellen unkontrolliert in Reichweiten von 30 bis 150 m aus, so daß über die Nutzreichweite der WLANs hinaus eine Abhörgefahr besteht. Durch den ungeschützten Frequenzbereich kommt es außerdem zu Störungen mit anderen Systemen, z.B. Mikrowellenöfen, die auch als Denial-of-Service-Angriff (DoS) gezielt genutzt werden könnte.

Zur Erhöhung der Sicherheit sind verschiedene Maßnahmen möglich:

- Konfiguration und Administration der WLAN-Komponenten: Basisschutzmaßnahmen, die sich durch den Standard einstellen lassen;
- standardübergreifende Maßnahmen;
- organisatorische Maßnahmen: Einbeziehung der WLAN-Komponenten in die Security Policy des Unternehmens.

Als Basisschutzmaßnahmen sind die SSID (Service Set Identifier) und das Paßwort der Access Points so einzustellen, daß keine Rückschlüsse auf die Firma oder das Netz erhältlich sind. Der SSID Broadcast ist abzuschalten, die MAC-Adreßfilterung einzurichten und die WEP-Verschlüsselung ist auf 128 bit zu stellen. Weiterhin sollte man DHCP (Dynamic Host Configuration Protocol) im WLAN-Bereich deaktivieren bzw. die IP-Adressen statisch vergeben. Proprietäre Erweiterungen wie WEPplus, Fast Packet Keying oder LEAP sollten ggf. eingesetzt werden. Zum Schutz sensibler Daten reicht dies allerdings nicht aus. Dazu sind weitere, über den Standard hinausgehende Maßnahmen zu ergreifen:

- zusätzliche Authentisierung: hier könnte man auf 802.1X zurückgreifen, das auf dem Extensible Authentication Protocol (EAP) basiert;
- zusätzliche Verschlüsselung: Einsatz eines VPN auf IPsec-Basis, das Verschlüsselung, Authentifizierung und Schlüsselmanagement bietet;
- Abschotten des Festnetzes durch eine Firewall: Abgrenzung durch ein Intrusion Detection System (IDS) vom LAN;
- Absichern der Clients: Einrichten von Personal Firewalls und Virenschutz sowie Zugriffsschutz und Benutzerauthentifizierung.

Man sieht also, daß die Sicherheitsmaßnahmen des Standards nicht ausreichen, um ein WLAN abzusichern. Jüngste Erweiterungen, die die Wireless Fidelity Alliance (www.wi-fi.com) für WLANs verabschiedet hat, sind Wi-Fi Protected Access (WPA), Advanced Encryption Standard (AES) und Temporal Key Integrity Protocol (TKIP). Allerdings ist TKIP nicht optimal, und man muß auch bei den anderen Verfahren abwarten, welche Schwächen sie ggf. im Einsatz offenbaren. Durch VPNs hingegen kann bereits heute eine sichere Abschottung herstellerneutral gewährleistet werden.

Kai-Oliver Detken ist Senior IT Consultant der Detken Consultancy & Internet Technologies e.K. sowie Dozent und freier Autor in Grasberg