Drahtlos, na und ...

Neue WLAN-Standards für eine sichere Kommunikation

Kai-Oliver Detken

Obwohl sich Wireless LANs (WLAN) zunehmender Beliebtheit erfreuen, wurde immer ihre Sicherheit in Frage gestellt, da die Daten vom Sender zum Empfänger frei über den Äther übertragen werden und somit theoretisch von jedem Angreifer, der über die entsprechenden Mittel verfügt, abgefangen und gelesen werden können. Spätestens mit der Einführung des 802.11i-Standards hat sich das geändert. Neben der Zugriffssicherheit sind allerdings noch weitere Dinge beim Aufbau von WLANs mit ins Kalkül zu ziehen.

Eine Auflistung der verschiedensten WLAN-Standards steht Ihnen im Internet zum Download bereit unter www.NET-im-web.de/pdf/WLAN-Standards.pdf

Dr. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Das bei Funknetzen nach 802.11 gebräuchliche Verschlüsselungsverfahren WEP (Wired Equivalent Privacy) stellte sich in der Vergangenheit als anfällig heraus. Daher stellte im Sommer 2003 die WiFi-Alliance WPA vor, das eine bessere Verschlüsselung ermöglicht, da es das sog. Temporal Key Integrity Protocol (TKIP) benutzt. Ferner werden Preshared Keys verwendet sowie das RADIUS-basierte 802.1X, mit dem man Benutzer eindeutig identifizieren kann.

Neue Standards

WiFi Protected Access (WPA) ist vom IEEE-Projekt 802.11i abgeleitet und aufwärtskompatibel. Es ausgewählte Bestandteile von 802.11i wie z.B. einen erweiterten Initialization-Vector, Re-Keying oder Message-Integrity-Check. Zudem sieht WPA eine Authentifizierung mittels IEEE 802.1x und EAP (Extensible Authentication Protocol) vor, die auf einen vorhandenen RADIUS-Server für die Nutzerverwaltung zurückgreifen. Nicht dazu gehören 802.11i-Merkmale wie sicheres Hand-off, sichere De-Authentifizierung oder verbesserte Verschlüsselungsverfahren (AES-CCMP). WiFi-zertifizierte WLAN-Geräte lassen sich per Softwareaktualisierung mit WPA ausrüsten.

Der Wireless-Standard 802.11i ist seit Juni 2004 vom IEEE ratifiziert. Er enthält die seit längerem erwarteten Sicherheitsspezifikationen für Funknetze, insbesondere die Verschlüsselung betreffend. 802.11i ersetzt WEP durch WPA. Darüber hinaus schreibt der Standard vor, wie der Advanced Encryption Standard (AES) zur Verschlüsselung von Daten zu verwenden ist. Damit genügt er den Vorschriften des Federal Information Standards (FIPS) und ist somit auch behördentauglich. Allerdings erfordert die AES-Umsetzung kompatible Hardware.

Inzwischen wurden einige ergänzende Standards wie der 802.11c festgelegt, der die Verfahren für Wireless Bridging behandelt, also die drahtlose Kopplung verschiedener Netztopologien. Als World Mode regelt der Standard 802.11d regionalspezifische technische Unterschiede, z.B. wie viele und welche Kanäle die Basistechniken a/h/b/g in welchem Land verwenden dürfen. Der Anwender muß lediglich das Land angeben, in dem er seine WLAN-Karte gerade benutzt. IEEE 802.11e definiert QoS- und Streaming-Erweiterungen, um die 54 Mbit/s schnellen Netze für Multimedia-Applikationen und vor allem für Voice over IP (VoIP) vorzubereiten. Um dazu notwendige Merkmale wie garantierte Datenraten oder minimale Laufzeitschwankungen zu garantieren, muß aber noch am MAC-Layer nachgearbeitet werden. Mit standardisierten Verfahren zum Roaming mobiler Clients zwischen Access Points (AP) vor allem verschiedener Hersteller beschäftigt sich 802.11f. Die Abstimmung der Übergabe erfolgt dabei über das Inter Access Point Protocol (IAPP).

Auswahlkriterien

Bei der Auswahl der geeigneten Komponenten ist es nicht mehr ausreichend, nur die vom Hersteller zur Verfügung gestellten Funktionen oder den Anschaffungspreis der Produkte als Kriterium heranzuziehen. Heutzutage hat sich im IT-Bereich als Grundlage für Investitionsentscheidungen der Begriff Total Costs of Ownership (TCO) etabliert, der zu den oben genannten Aspekten folgende Kriterien hinzufügt:

- Kosten für Betrieb und Support;
- Ausbau- und Erweiterungsfähigkeit;
- Integrationsfähigkeit in bestehende und zukünftige IT-Landschaften.

Beim Aufbau von WLAN-APs sind insbesondere die Ausleuchtung sowie

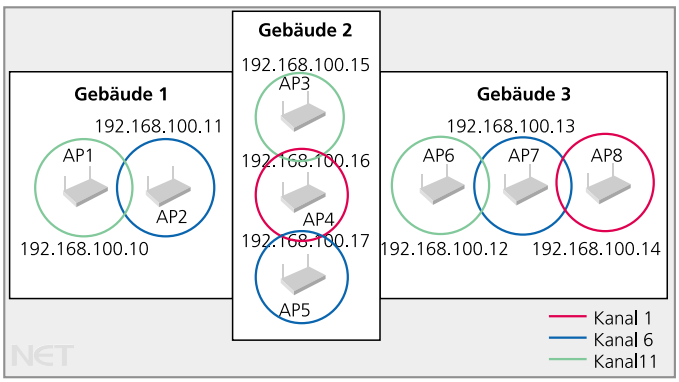

Bild 1: Ausleuchtung von WLAN-APs in verschiedenen Gebäuden

das Überlappen gleicher Kanäle zu beachten. Um Störungen zu vermeiden, sollte jeder AP nur mit einem Kanal senden und einen anderen als seine direkten Nachbarn besitzen. Im Beispiel in *Bild 1* ist dabei immer ein optimaler Abstand von fünf Kanälen eingehalten worden, was in der Praxis allerdings nicht immer möglich ist. Zudem können manche APs noch durch zusätzliche Bridging-Funktionalität direkt miteinander verbunden werden, um den Endgeräten ein unterbrechungsfreies Roaming zwischen ihnen zu ermöglichen. Auch kann bei hochwertigen Komponenten die Sendeleistung eingestellt werden, um so bestimmte Räume effektiver ausstrahlen zu können.

Viel wichtiger als die Leistungsmerkmale ist aber die Berücksichtigung der aktuellen Sicherheitsstandards. Diese sind meist den teureren Geräten vorbehalten. Weitere Anforderungen bei Umsetzung und Implementierung sind:

- Ausarbeiten eines WLAN-Konzepts (Ausleuchtung, Frequenzen usw.);
- Vermessen des Funknetzes vor Ort;
- Dokumentieren der optimalen bzw. möglichen AP-Standorte;
- Konfiguration der Basiseinstellungen (SSID und MAC-Zugriffsschutz);
- Konfiguration der Sicherheitseinstellungen (WPA, RADIUS, AES);
- Durchführen von Sicherheitschecks zum Überprüfen der Einstellungen.

Referenzprojekt Uni Bremen

Als Referenzprojekt sei an dieser Stelle die Universität Bremen genannt. Sie betreibt seit ein paar Jahren ein flächendeckendes drahtloses Datennetz in 802.11b-Technik mit über 400 Access Points. Das WLAN erweitert das bestehende Festnetz und stellt so IP-Konnektivität auf dem gesamten Campus bereit.

Zuerst wurde ein technisches Konzept für das Campus-WLAN der Universität Bremen zuzüglich der begleitenden Evaluierung von Standards und Produkten ausgearbeitet. Ein Schwerpunkt lag dabei auf den Sicherheitsanforderungen an die drahtlose Infrastruktur. So wurde ein Virtual Private Network (VPN) für die Sicherheitsinfrastruktur geplant, da zum Konzeptzeitpunkt keine ausreichenden Sicherheitsmechanismen für die 802.11-Spezifikation vorhanden waren. Das als unsicher eingestufte WLAN-Zugangsnetz, in dem sich die Endgeräte befinden, wurde daher vom übrigen Campus-Netz getrennt (*Bild 2*); der Übergang ist nur über VPN-Gateways möglich. Diese gewährleisten einerseits eine nutzerbasierte Authentifizierung und andererseits eine sichere Verschlüsselung der Kommunikation. Eingesetzt werden das Point-to-Point Tunneling Protocol (PPTP) und IPsec, letzteres mit AES-Verschlüsselung. Durch diesen Ansatz konnte die Universität auf proprietäre Ergänzungen zu 802.11 verzichten, was angesichts der heterogen

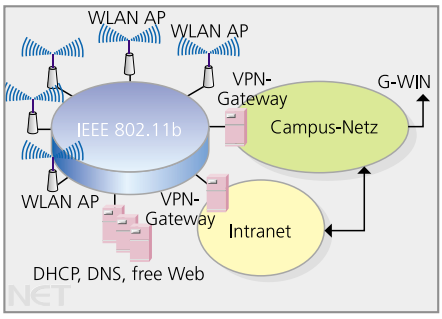

Bild 2: WLAN der Universität Bremen

ausgestatteten Nutzergruppe unabdingbar war. Zusätzlich sparte man signifikante Kosten durch den Einsatz preiswerter Linux-Rechner, die als VPN-Gateways eingesetzt wurden.

Nach der Implementierung wurden die Sicherheitseinstellungen komplett überprüft, indem ein sog. War Driving durchgeführt wurde. ZU diesem Zweck bewegten sich Mitarbeiter mit entsprechender Hard- und Software über den Campus und versuchten, Sicherheitslücken aufzudecken. Dabei kamen teilweise Fremdnetze, die auf dem Campus von Firmen betrieben werden, offen zum Vorschein.

Zusätzlich wurden gesundheitliche Aspekte untersucht. Dazu wurde ein Gutachten in Auftrag gegeben, das mögliche schadhafte Wirkungen aufdecken sollte. Funk-LAN-Geräte arbeiten im Mikrowellenbereich und haben eine Sendeleistung von max. 100 mW. Im Vergleich dazu entwickeln die gebräuchlichen Mobilfunktelefone im deutschen D-Netz mit 5000 mW die 142fache Leistung. Ein handelsübliches Mikrowellengerät kann sogar bis zu 1000 mW abstrahlen, ohne den gesetzlichen Rahmen zu überschreiten. Durch das Verteilen der Sendeleistung auf mehrere Frequenzen (Spread-Spectrum-Verfahren) wird die Wirkung bei Funk-LANs noch weiter abgeschwächt. So wurde auch im Campus-Netz keine Unverträglichkeit durch das EMVU-Gutachten festgestellt.

Durch den Einsatz von PPTP konnte bereits auf Layer-2-Ebene ein Zugang zum VPN geschaffen werden. Dadurch entfiel die Ausrüstung sämtlicher Laptops mit einer zusätzlichen IPsec-Software. Hinzu kam, daß man sich dadurch nicht mit unterschiedlichen Betriebssystemen und Treibern beschäftigen mußte. IPsec-Software-Clients der Hersteller haben oftmals Kompatibilitätsprobleme mit bestehender Software oder lassen zumindest kein weiteres IPsec-Tool zu. Hinzu kommt, daß die Software meistens nicht auf unterschiedlichen Betriebssystemen lauffähig ist.

Durch den Einsatz von RADIUS konnten Benutzerprofile vergeben werden, die die Authentifizierung und Autorisierung über die VPN-Gateways vornehmen und die jeweiligen Dienste zur Verfügung stellen. Auf diese Datenbank kann auch netzübergreifend zugegriffen werden, so daß z.B. Studenten der Hochschule in Bremerhaven sich auch am Bremer Campus-Netz anmelden können. *(bk)*