

Nützliche Tools überwachen den Funkraum – Administratoren müssen Integration mit kabelbasierten Netz im Auge behalten

# WLANs brauchen breite Skalierbarkeit

Rund 60 Prozent aller Unternehmen in Nordamerika und Europa installieren in diesem Jahr ein WLAN oder bauen das Vorhandene aus, hat Forrester ermittelt. Dies muss mit der richtigen Technologie und passenden Maßnahmen erfolgen, um die Kosten im Griff zu halten.

„Mit WPA und 802.1x sind die Sicherheitsrisiken von WLANs ausgeräumt“, konstatiert Forrester-Analystin Ellen Daley. Der Security-Standard 802.11i bietet einen zuverlässigen Ansatz für Authentifizierung und Verschlüsselung. Zudem gebe es mittlerweile etliche Zusatz-Tools, welche die Security noch effizienter machen.

„Dennoch verfolgen viele Unternehmen eine konsequente Anti-Wireless-Strategie“, berichtet Martin Malina, CEO des WLAN- und Token-Ring-Anbieters Madge. Doch sogar solche Firmen zählt der Netzwerker zu seinen Kunden: Dessen WLAN Probe 2 und der Probe Monitor 2 machen alle Funkaktivitäten aus – von Geräten der Standards 802.11a, b, g sowie Bluetooth – und unterstützen so das Durchsetzen dieser Policy. „Denn viele Mitarbeiter arbeiten zu Hause mit Wireless, wollen dies auch am Arbeitsplatz und verbinden Access Points mit dem Netz.“

Natürlich spüren diese Sensoren genauso gut im Firmen-WLAN



**Ubiquitärer Access steigert die Produktivität. Beim Aufbau des Funknetzes sollten Aspekte wie Security und Architektur aber nicht unter den Tisch fallen.** Foto: HP

wird installierte Access Points (APs) auf – aber vor allem Eindringlinge. In diesem Fall ergreift der Monitor Maßnahmen: „Die Countermeasure-Software schaltet bei einem Einbruch den Sensor vom Passiv- auf Aktiv-Modus um“, erläutert Malina. „Dann stört dieser gezielt die Verbindung zwischen Hacker und AP, ohne die übrigen Nutzer zu beeinträchtigen.“ Für das Management von APs verschiedener Hersteller führt Madge seine Produktfamilie der Enterprise Access Server im Produktportfolio – die Softwareversion für Intel-Server skaliert bis zu Tausenden von APs.

Und Skalierbarkeit von WLANs entwickelt sich zur wichtigen Eigenschaft: Beim Aufbau oder der Erweiterung von Funknetzen in Unternehmen, so berichtet Forrester, hat sich die durchschnittliche Anzahl der eingesetzten APs auf 150 verdoppelt. WLANs entwickeln sich damit zu großen Netzen mit zentraler Verwaltung – obwohl diese meist noch abgekoppelt ist von der des verkabelten LANs. Zu einem Steuerungs-Tool zur rufen die Forrester-Analysten in jedem Fall – gleichzeitig sollte beobachtet werden, was Systemmanager wie CA, HP und IBM machen: Denn auf lange

Sicht werden sie das Management von WLANs und verkabelten Netzen konsolidieren.

Eng verknüpft mit der Verwaltung des Netzes ist die Frage nach der eingesetzten Architektur. Neben dem Prinzip der Fat APs, die wesentliche Funktionen wie etwa Frequenzmanagement selbst übernehmen, hat sich durch Companies wie Aruba, Airespace oder Trapeze das Konzept der Thin APs etabliert. Diese Funknetzknoten sind

mehr oder weniger bis auf die reine Antennenfunktion abgespeckt, die Intelligenz steckt im zentralen Switch. Laut Forrester haben – vor allem seit Ciscos Airespace-Übernahme – beide Ansätze ihre Berechtigung. Managementsysteme sollten daher auch beide Architekturen unterstützen.

Bruce Van Nice, Marketing-Vizepräsident bei Trapeze, steht natürlich klar hinter den Switch-basierten WLANs: „Das Thick-AP-Modell hat so gut wie ausgedient. Sicher gibt es viele Anwender, die diesen Weg gegangen sind und nicht von heute auf morgen umstellen, aber

langfristig schon.“ Mit ihrer Open Access Point Initiative (OAPI) geben sich die Kalifornier jedoch auch offen: So wurde Trapezes Software Mobility System jetzt so erweitert, dass Ciscos APs mit Trapeze-Switches kommunizieren können, ohne das IOS-Betriebssystem der Aironets zu ändern. „Mit OAPI geben wir Partnern wie etwa D-Link zudem die Möglichkeit, unsere Software in ihre Systeme zu integrieren“ erläutert Van Nice. „Wir wollen auch Software anderer Hersteller in unseren APs einsetzen, um beispielsweise eine umfassendere Security zu bieten.“

## Ausbaufähig für neue Technologien

Madge ist laut CEO Malina ein klarer Verfechter der Thick APs, da solche Systeme einfacher auszubauen wären. „Unternehmen brauchen eine Wireless-Lösung, die hinsichtlich der Nutzerzahlen skaliert, aber auch in Bezug auf neue Standards und Technologien.“ Und bei Installationen auf der grünen Wiese rät Malina sogar zu einer Wireless-only-Lösung: „Verschiedene Analystenreports zeigen, dass die Vernetzung eines neuen Gebäudes – schließt man alle Kosten wie etwa für Verkabelung ein – mit Wireless billiger zu machen ist als mit einer drahtbasierten Lösung.“ sts