Kurse zeigen Gefahren und Einsatzgebiete auf

Weiterbildung bringt Wireless näher

Soll ein WLAN im Unternehmen aufgebaut werden, müssen sich IT-Verantwortliche auf Fortbildungen mit der Technologie auseinander setzen – nicht nur wegen des Sicherheitsaspekts.

Die Funktion und das Design von Funknetzen können Interessierte in dem Seminar von Usco (www.usco.de) an einem Tag kennen lernen. Nach einer Einführung mit Vorstellung des OSI-Modells stehen die WLAN-Standards auf dem Kursprogramm. Hierbei werden nicht nur die einzelnen Normen der 802.11-Buchstabensuppe, sondern auch die eingesetzten Funkverfahren behandelt.

Mehr in die Praxis geht es dann beim Thema Design von WLAN-Netzen. Hier erfährt der Teilnehmer, was bei Installationen in Räumen beziehungsweise im Freien zu beachten ist, oder wie sich Signaldämpfung und Übertragungsgeschwindigkeit zueinander verhalten. Dies leitet über zu den Hürden, die beim Netzaufbau aus den Weg geräumt werden müssen. Die Betrachtung der Sicherheit im Funknetz sowie ein Ausblick auf künftige WLAN-Technologien schließen das Seminar ab.

Ganz auf die Security fokussiert sich der Eintageskurs, den Rhode & Schwarz auch im Anwenderunternehmen durchführt. Er richtet sich an Mitarbeiter aus allen Bereichen, die sich über die Sicherheitsproblematik informieren wollen. Neben der Erläuterung von Begriffen wie Authentifizierung, Autorisierung oder Datenintegrität werden die Gefahren aufgezeigt, die durch Spoofing, DoS-Attacken (Denial of Service) oder Abhören bestehen. Im Besonderen werden die Schwächen des WEP-Protokolls (Wired Equivalent Privacy) diskutiert. Im Weiteren wird beschrieben, welche Protokolle sicherer sind und wie sich das Netz mit zusätzlichen Maßnahmen abschotten lässt.

Einsatz in Logistik und auf dem Rollfeld

Dass WLANs ihre Vorteil auch im industriellen Umfeld ausspielen können, zeigen die WLAN Solution Days, die Netzwerker Lancom (www.lancom.de) mit dem Connectivity-Spezialisten Huber & Suhner (www.hubersuhner.de) veranstaltet. Anwendungsfelder sind–beispielsweise die Anbindungen von Service-Fahrzeugen auf einem Flughafenvorfeld oder von Maschinen und Automaten. Auch in großen Lagern lässt sich die Logistik mit WLANs deutlich vereinfachen. Die Solution Days geben deshalb Praxiseinblicke in solche Anwendungen wie auch in neue Lösungen und informieren zudem über die Grundlagen und Marktentwicklung der WLAN-Technologie. *sts*

Fehler können schnell behoben werden – Falsche Konfigurationen erkennt das System selbstständig

Zentrales Management macht das WLAN leistungsfähiger

Unterschiedliche Endgeräte und steigende Nutzerzahlen im Funknetz setzen den Administrator unter Druck. Nur eine zentrale, hardwareneutrale Managementlösung macht das WLAN-Wachstum beherrschbar.

Die Konfiguration und Verwaltung von WLANs mit hunderten Access Points (APs) kann in Zukunft gar nicht mehr manuell durchgeführt werden, weil die personellen und finanziellen Mittel nicht zur Verfügung stehen. Kosten, Performanz und Sicherheit haben nur zentrale, hardwareunabhängige Managementlösungen im Griff. Denn damit lassen sich Konfigurationseinstellungen zentral definieren und die Firmware-Version spezifizieren, die auf allen APs laufen soll. Um zu überprüfen, ob die Konfiguration tatsächlich erfolgreich war, nimmt ein zentrales Management-Tool einen regelmäßigen Abgleich der Einstellungen mit den zentral definierten vor.

Doch auch wenn alle APs korrekt konfiguriert sind, können Probleme wie fehlende Verbindung oder zu langsame Datenübertragung auftreten. Dann kommt es auf die Schnelligkeit an, mit der die Ursache des Problems ermittelt werden kann. Und die hängt wieder von den Diagnosefähigkeiten einer Managementlösung ab. Ideal wäre es, wenn dieses Tool nicht nur feststellt, dass etwa zwei benachbarte APs denselben Funkkanal benutzen, sondern auch eine E-Mail zusammen mit der Diagnose verschickt.

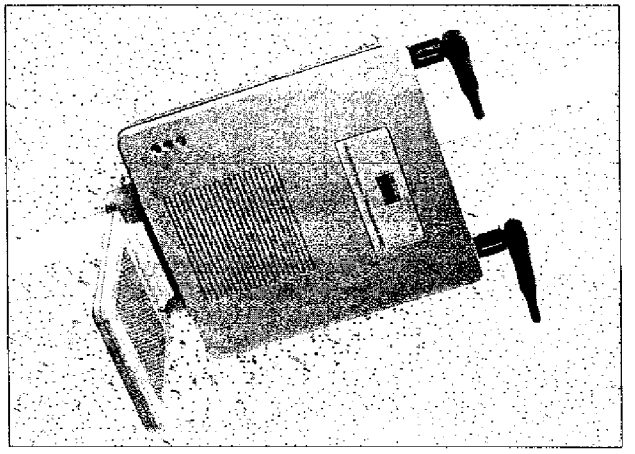
Ein zentrales Management löst zudem die klassischen Sicherheitsprobleme von WLANs: Datenverschlüsselung, Authentisierung und Zugangskontrolle sowie Schutz vor Eindringlingen. Denn gerade hier kommen die Vorteile einer solchen Lösung bei der zentralen Konfiguration der Security-Einstellungen und deren permanenter Überprüfung zum Tragen. Solite ein Gerät zum Beispiel den Standard WPA nicht korrekt übernehmen und scheitert auch die Nachkonfiguration, so wird das Problem automatisch angezeigt und kann per Fernwartung gelöst werden.

Scans und Analysen lassen alles im Lot

Abgerundet werden die Sicherheitsfunktionen einer zentralen Managementlösung durch ein Verzeichnis aller autorisierten Geräte, dem kombinierten Einsatz von Funkwellenscans und der Analyse des Datenverkehrs auch im drahtgebundenen Netz. Denn so lassen sich zuverlässig alle nicht autorisierten APs ermitteln, selbst wenn sie außerhalb der Reichweite autorisierter Geräte liegen.

Die Echtzeitüberwachung und -analyse bietet aber noch einen anderen Vorteil. Intelligente Diagnosealgorithmen zur Performance-Analyse können die Administratoren über Leistungsabfälle jedes einzelnen Gerätes informieren, die Ursache ermitteln und Ergebnisse grafisch darstellen. Dabei lassen sich die Schwellwerte, die Alarme auslösen, situationsbedingt anpassen. So würde etwa eine 95-prozentige Auslastung der APs morgens um 9 Uhr keinen Alarm auslösen, weil am Beginn des Arbeitstags alle Mitarbeiter gerade ihre E-Mails abrufen. Tritt hingegen ein ungewöhnlicher Leistungsabfall während der Mittagspause auf, wird der Administrator benachrichtigt. Möglich wird diese Schwellwertanpassung durch die Langzeitanalyse der zeitlichen Veränderungen des Anwenderverhaltens und des Datenverkehrs, die zudem Aussagen über Trends und künftige Performanzprobleme zulässt.

Jan Buis, Director, Sales & Business Development, North-Eastern Europe, AirWave/sts



Auch korrekt konfigurierte Access Points können Probleme bereiten – ein zentrales Management bringt dann schnelle Hilfe. Foto: Cisco