ERHÖHTE SICHERHEIT IM WLAN DURCH WIRELESS SWITCHING

Wireless Local Area Networks (WLANs) haben in der Vergangenheit nicht nur durch ihre flexiblen Nutzungsmöglichkeiten von sich Reden gemacht, sondern auch durch ihre Sicherheitsrisiken. Ein Grund für viele Unternehmen auf die drahtlose Technologie zu verzichten. Die Bedrohungen durch unsichere Verschlüsselungsmechanismen sind mittlerweile durch Verfahren wie WPA und WPA2 gelöst worden. Trotzdem ist es nach wie vor sehr aufwändig mit klassischen WLAN-Access Points einen sicheren WLAN-Betrieb in komplexen Unternehmensumgebungen zu gewährleisten. Wireless Switching heißt hier die Alternative für alle mittleren bis großen Unternehmen.

Das größte Problem klassischer WLAN-Lösungen stellen die einzeln zu verwaltenden Access Points dar. Handelt es sich um ein kleines WLAN, welches nur aus wenigen Access Points besteht, so ist der Verwaltungsaufwand noch tolerabel. Spätestens jedoch bei einer Anzahl von zehn und mehr Access Points steigt er hinsichtlich Configuration Management und Monitoring überproportional an. Bei weitaus größeren Umgebungen mit über dreißig Access Points wird der Arbeitsaufwand immens und ist ohne zusätzliche Managementwerkzeuge kaum zu bewältigen. Nicht zu vergessen: Die Betriebskosten steigen exponentiell zur Anzahl der Access Points.

Unter dem Aspekt der Sicherheit betrachtet, birgt die manuelle Verwaltung von Access Points im großen Umfang vor allem die Gefahr, dass durch die sich wiederholende und somit ermüdende Tätigkeit vereinzelt menschliche Fehler bei der Konfiguration auftreten. Diese führen dann zu Schwachstellen im drahtlosen Netzwerk und lassen sich nur schwer ermitteln. Die Folgen sind absehbar: Verschlüsselungen einzelner Geräte könnten nicht korrekt aktiviert sein. Ebenfalls ist es möglich, dass Gast-Zugänge mit schwachem Zugangsschutz nicht nur Zugriff auf öffentliche Bereiche, sondern versehentlich auf das gesamte interne Netzwerk des Betreibers erhalten. Zudem erhöht fehlendes Echtzeit-Monitoring das Risiko, dass Entwendungen zunächst unentdeckt bleiben. In engmaschigen WLAN-Umgebungen ist es nicht immer möglich das Verschwinden von Access Points sofort zu bemerken. Erfahrene Eindringlinge können somit leicht Pre-Shared Keys auslesen und sich darüber unauthorisierten Zugriff in das Unternehmens-WLAN verschaffen.

Neben direkten Angriffen auf drahtlose Unternehmensnetzwerke sind klassische WLAN-Umgebungen auch durch indirekte Angriffe auf das interne Netzwerk gefährdet – nämlich durch das versteckte Einbinden zusätzlicher unautorisierter Access Points, über die ein Angreifer leicht von außerhalb des Gebäudes Zugang zum internen Netzwerk erhält. Die Lösung für Umgebungen ohne Wireless LAN gestaltet sich verhältnismäßig einfach: Der fremde unberechtigte Access Point lässt sich bei regelmäßigen Begehungen mit einem WLAN-Sniffer wie zum Beispiel Netstumbler oder Kismet aufspüren, indem er anhand seiner Funksignale identifiziert wird. Ungleich schwieriger ist dies beim Betrieb eines größeren eigenen WLANs, da bei geschickter Vorgehensweise des Angreifers ein fremder Access Point nur schwer von den eigenen zu unterscheiden ist.

Wireless Switching bietet eine Lösung zum sicheren Betrieb komplexer WLANs. Dahinter verbirgt sich die Verlagerung der Managementfunktionalität von den einzelnen Access Points in eine einzige Komponente, den Wireless Switch. Diese zentrale Verwaltung aller WLAN-Komponenten gestattet eine gebündelte Umsetzung von Sicherheitsrichtlinien – ähnlich einer Firewall, die vor einer Serverfarm positioniert wird und zentral die Security Policy für alle zur Verfügung gestellten Dienste durchsetzt. Im Wireless Switch erfolgt einmalig die Definition der Access Point Profile. Anschließend werden diese beim Booten automatisch authentifiziert und durch den Wireless Switch mit den vorgehaltenen Konfigurationsdaten versorgt. Im Idealfall erfolgt dabei keine lokale Speicherung der Daten im Flashspeicher des Access Points – Anhaltspunkte für Angreifer auf das WLAN entfallen.

Des Weiteren geht die Authentifizierung der Endgeräte und Benutzer zentral am Wireless Switch von statten und wird damit den Anforderungen an sichere Infrastrukturen gerecht. Demzufolge können Pre-Shared Keys an einer einzigen Stelle verwaltet werden. Weiterer Vorteil: Bei der Nutzung von RADIUS als Authentifizierungsprotokoll greift nur noch eine Komponente auf den zentralen RADIUS-Server zu. Der Wegfall der Reauthentifizierung bildet die Voraussetzung der Fast Roaming-Funktionalität der Wireless Switch Lösung. Neue Applikationen wie beispielsweise Voice over IP mittels WLAN-Telefonen werden dadurch ermöglicht. WLAN-Telefone können somit schnell von einer Funkzelle in die nächste wechseln: Ein Telefongespräch wird damit auch dann nicht beeinträchtigt, wenn der Benutzer sich während des Telefonats im Gebäude bewegt.

Keine Chance für Rogue Access Points

Ein entscheidender Vorteil einer Wireless Switch Lösung gegenüber einer klassischen WLAN-Implementierung mit dezentral verwalteten Access Points liegt in der gebündelten Vorlage aller Informationen über die Umgebung. Ein Wireless Switch ist in der Lage automatisch nicht-autorisierte, so genannte Rogue Access Points, sowie Ad-hoc Netzwerke aufzuspüren und zu lokalisieren – zum einen durch die ständige Umgebungsübersicht, zum anderen durch das regelmäßige Absuchen des gesamten Frequenzbereiches nach Funkquellen. Auf diese Weise trägt der Switch zur Durchsetzung organisatorischer Sicherheitsrichtlinien bei und erschwert Angriffe mittels versteckter fremder Access Points. Zur schnellen und unkomplizierten Lokalisierung sollte ein visuelles Management Bestandteil der Lösung sein.

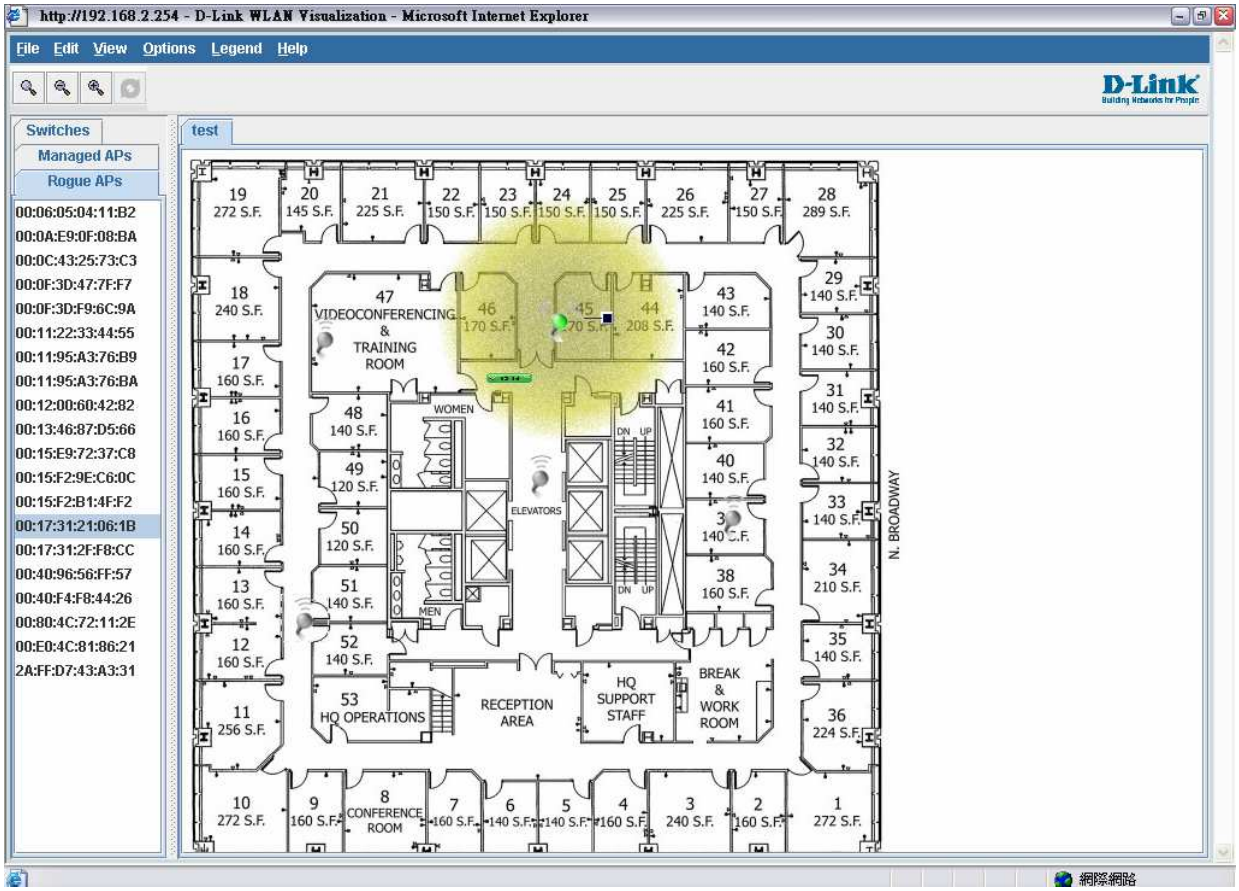

Abbildung 1: Visuelles Aufspüren von Rogue Access Points

Ein flächendeckendes drahtloses Unternehmensnetzwerk stellt nach der Inbetriebnahme schnell zusätzliche Sicherheitsanforderungen, die es umzusetzen gilt. Zu den Klassikern zählt dabei die Implementierung unterschiedlicher WLAN-Dienste für verschiedene Benutzergruppen und Endgeräte. Ein Gastzugang beispielsweise für externe Mitarbeiter wie Berater oder Wirtschaftsprüfer sollte zwar den Zugriff auf das Internet und öffentliche Unternehmensressourcen gestatten, Einblicke in das interne Netzwerk und auf Server jedoch verhindern. Ein Wireless Switch wird solchen Anforderungen mittels Virtualisierung der Access Points mit geringem Aufwand gerecht: Die Geräte erhalten zunächst mehrere SSIDs (Service Set Identifier), über die sie angesprochen werden. Für jede SSID ist ein eigener Satz von Sicherheitsrichtlinien hinterlegt, welcher den Einsatz unterschiedlicher Authentifizierungs- und Verschlüsselungsverfahren ermöglicht. Zusätzlich steuert dieser über VLAN-Zuordnungen (Virtual Local Area Network) und ACLs (Access Control List) den Zugriff auf die jeweils erlaubten Netzwerksegmente. Auf diese Art und Weise können auch entsprechende QoS-Parameter für die unterschiedlichen Dienste definiert werden.

Mit integrierten Switch-Lösungen – sogenannten Unified Switches – gestaltet sich die Implementierung unterschiedlicher Dienste besonders leicht und komfortabel. Das Management der Access Points wird nicht wie bei anderen Controller-basierten Lösungen über eine Appliance realisiert, sondern ist direkt in einen Layer2 oder Layer3 Switch integriert. So erfolgt das Sicherheitsmanagement bei Unified Lösungen sowohl WLAN- als auch LAN-seitig auf einem Gerät. Typischerweise stellen diese Managed Switches auch die für Access Points benötigten Power over Ethernet Ports zur Verfügung. Um eine Investitionssicherheit für die Access Points der neuen Generation zu gewährleisten, sollte der Unified Switch bereits mit Gigabit Ethernet Ports ausgestattet sein. Denn die neuen Geräte unterstützen den Funkstandard 802.11n und erreichen Netto-Datendurchsätze von deutlich über 100 Mbit/s.

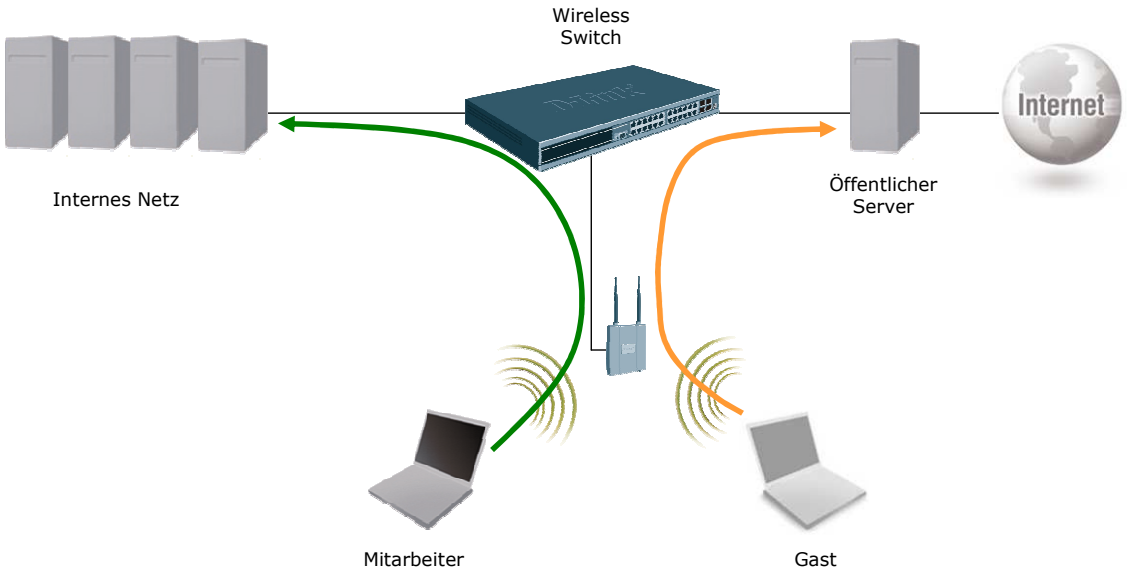

Abbildung 2: Implementierung eines Gast-Zugangsdienstes mit einem Unified Switch

Zusammenfassend ist eine Wireless Switch Lösung nahezu unerlässlich, um eine komplexe WLAN-Umgebung eines mittleren bis großen Unternehmens sicher betreiben zu können. Dafür sprechen das zentrale Management aller Sicherheitseinstellungen, das mögliche Aufspüren unerlaubter Funkquellen sowie die Definition voneinander abgeschotteter WLAN-Dienste. Die Vereinigung aller Komponenten garantiert einen rundum sicheren und gleichzeitig kostengünstigen Betrieb drahtloser Netzwerke.