Drahtlos – und trotzdem sicher

Ob firmenintern oder im öffentlichen Raum – WLANs erfreuen sich grosser Beliebtheit und sind vielerorts gar nicht mehr wegzudenken. Doch in puncto Sicherheit werden die Betreiber vor einige Herausforderungen gestellt.

Der drahtlose Netzzugang hat sich in (fast) allen Arbeits- und Lebensbereichen etabliert. Selbst im privaten Haushalt sind vermehrt WiFi Access Points anzutreffen. Was aus Benutzersicht komfortabel und in Anbetracht der erforderlichen Mobilität notwendig ist, erweist sich für die WLAN-Betreiber als anspruchsvolles Unterfangen. Gilt es doch, Aspekte wie Komfort, Sicherheit, Handling und Kosten unter einen Hut zu bringen. Namentlich dann, wenn neben der Einbindung interner Mitarbeitender auch Gästen via WLAN ein gesicherter Zugang zum Internet geboten werden soll, sind einige kritische Gesichtspunkte zwingend zu betrachten. Dazu gehört unter anderem die klare Trennung und einfache Verwaltung unterschiedlicher (virtueller) Netze. So gilt es beispielsweise sicherzustellen, dass Gäste trotz Nutzung desselben Funknetzes nicht auf firmeninterne Daten zugreifen können. Ferner ist dafür zu sorgen, dass kritische Webzugriffe, die beispielsweise Schadcodes ins Firmennetz einschleusen oder zu Reputations- und Folgeschäden führen können, verhindert werden. Wichtig ist folglich, den Datenverkehr gezielt zu überwachen und zu filtern, was sich besonders effizient und einfach mittels Application Control und Webfiltering erreichen lässt.

Um Anforderungen dieser Art zu entsprechen, stehen seit kurzem Lösungen zur Verfügung, die die einzelnen Access Points (APs) mit einer zentralen Firewall mit integriertem AP-Controller verbinden. Dabei wird der gesamte Datenverkehr des Wireless LANs über die Multi-Threat-Security-Appliances geleitet. Diese sorgen dafür, dass dem Funknetz sämtliche benötigten Abwehr- und Sicherheitsmechanismen zur Verfügung stehen – so etwa Funktionen wie Statefull Inspection Firewalling, Application Control, Webfilter, Antivirus, Intrusion Prevention und SSL Traffic Inspection.

Derart integrierte Gesamtlösungen, wie sie beispielsweise vom Security-Spezialisten Fortinet angeboten werden, ermöglichen einerseits ein zentrales und umfassendes Sicherheitsmanagement und wissen andererseits hinsichtlich Konfiguration und Skalierbarkeit zu überzeugen. So erfolgen die Einbindung und das Management sämtlicher APs zentral über den in der Security Appliance integrierten AP-Controller. Dieser ermöglicht auch das automatische und umfassende Einspielen der jeweils neusten Signaturen und der damit verbundenen Sicherheitsfunktionen. Ebenso komfortabel erweist sich die Bildung und Trennung unterschiedlicher virtueller Netze sowie die Bildung netzspezifischer Security-Policys. So ist es problemlos möglich, über die gleichen physischen APs und Controller parallel mehrere unterschiedliche Wireless-Netzwerke zu betreiben. Dazu steht eine komfortabel bedienbare Konfigurations- und Managementkonsole zur Verfügung.

Besonders attraktiv sind moderne Komplettlösungen für Firmen mit dezentralen Niederlassungen. So macht die Einbindung von Multi-Threat-Security-Appliances mit integriertem AP-Controller den Aufbau einer kabelgebundenen Netzinfrastruktur nicht zwingend notwendig. Dies reduziert die Kosten und verkürzt die für die Projektumsetzung benötigte Zeit.

«Secure-Wireless-LAN-Lösungen» verbinden Access Points sowie UTM-Appliances mit integriertem AP-Controller zu einem integralen Ganzen. Dadurch wird die Sicherheit erhöht und die Kosten werden reduziert. Bildquelle: Fortinet

Einfach nutzbare Gastzugänge

Ob im firmeninternen Sitzungszimmer, Hotel oder öffentlichen Raum: Der sicheren und trotzdem komfortablen Einbindung von Gästen ins WLAN gilt ein besonderes Augenmerk. Einerseits aus Gründen der Sicherheit für das jeweilige Unterneh-

DER AUTOR

Patrick Michel,
Boll Engineering,
Wettingen

Als Rauchmelder getarnte APs reduzieren Vandalismus und Diebstahl. Bildquelle: Fortinet

men – andererseits angesichts verschärfter Regulatorien, die eine zwingende Authentisierung der User fordern. Demnach sind Betreiber von öffentlich zugänglichen Wireless-Netzwerken verpflichtet, Benutzerinnen und Benutzer zu identifizieren. Für die Anmeldung mittels individueller Zugangsdaten lassen sich dedizierte Gästeportale beziehungsweise sogenannte «Captive Portals» einrichten. Dabei wird der Client auf eine spezielle Website umgeleitet, bevor er sich ins Internet verbinden kann, wodurch sich eine Authentifizierung und allenfalls auch die Annahme der Nutzungsbedingungen erzwingen lassen. Steht für die Authentifizierung des Gastes ein solches spezielles Gästenetz zur Verfügung, muss der WiFi-Zugriff nicht verschlüsselt erfolgen. Die mühselige Eingabe eines Keys entfällt dadurch, was die Handhabung der Log-in-Prozedur deutlich vereinfacht.

Die fürs eigentliche Log-in benötigten individuellen Zugangsdaten können im Rahmen des Gästeempfangs generiert werden. Idealerweise wird dabei auch die Mobiltelefonnummer des jeweiligen Gasts beziehungsweise die Funktion «Einmalpasswort» eingebunden, was die sichere Authentisierung der User deutlich erhöht. Das dazu benötigte «One Time Password» (OTP) wird nach Eingabe von User-Name und Passwort vom System automatisch generiert und dem jeweiligen Benutzer via SMS übermittelt.

Notwendige Schutzmechanismen

Bei der Planung und Umsetzung hoch sicherer und skalierbarer Wireless LANs lohnt es sich, ausgewählte Leistungsmerkmale besonders zu betrachten. So beispielsweise die Kommunikation zwischen APs und Controller, die via Tunnel erfolgen sollte. Ein weiteres Kriterium ist das unterbrechungsfreie, AP-übergreifende Mitführen einer Session. Ein nahtloses Roaming unterstützt die unbegrenzte Mobilität der User auf dem gesamten Campus. Dies ist namentlich dann wichtig, wenn Wireless-Geräte und -Funktionen verwendet werden, die auch dann unterbrechungsfrei funktionieren müssen, wenn sich der Benutzer aktiv bewegt – wie dies beispielsweise bei Voice over IP der Fall ist.

Von besonderer Bedeutung ist das Erkennen sowie das automatische Ausschliessen oder Stören sogenannter «Rogue APs». Dabei handelt es sich um Access Points, die durch Dritte eingeschleust und mit dem internen LAN verbunden werden. Um Rogue APs erkennen zu können, überprüfen intelligente WLAN-Lösungen das LAN kontinuierlich nach MAC-Adressen, die nicht erscheinen dürften. Zudem wird ein AP-Frequenzbereich («Radio») dazu verwendet, ständig nach unerlaubten APs zu scannen. Wird über LAN und Funk ein nicht autorisierter AP erkannt, wird einerseits eine entsprechende Alarmierung ausgelöst und die betreffende AP andererseits via LAN gestört und so ihrer Funktion beraubt.

Grenzen auflösen

Bei der Evaluation und Umsetzung von WLANs sind neben sicherheitsspezifischen Aspekten auch Fragen wie Skalierbarkeit, Vielfalt der APs, Performance sowie Unterstützung sämtlicher Standards zu betrachten. Zum erstgenannten Themenbereich darf festgehalten werden, dass nahtlos skalierbare und hoch performante Lösungen existieren, die bis zu mehreren tausend APs und folglich zehntausende gleichzeitige User unterstützen. Entsprechende Multi-Threat-Security-Appliances mit integriertem AP-Controller weisen WLAN-Kapazitäten von bis zu 49 Gbps auf. Seitens AP sind Lösungen erhältlich, die gleichzeitig zwei Frequenzen (2,4 und 5 GHz) und folglich Datenraten von bis zu 600 Mbps unterstützen. Diese «Dual Radio»-Lösungen stellen sicher, dass alle Normen (a/b/g/n) unterstützt werden und folglich sämtliche denkbaren User-Devices eingebunden werden können.

Interessant sind ferner Access Points mit PoE-Schnittstelle («Power over Ethernet»), die eine separate Zuführung der Speisespannung überflüssig machen. Um der Problematik von Vandalismus und Diebstahl zu begegnen, sind ferner Lösungen am Markt erhältlich, deren Antennen im Gehäuseinneren versteckt sind. Auch als Rauchmelder getarnte APs tragen diesem Bestreben Rechnung. Je nach Anwendungsbereich ist zudem die Verfügbarkeit von outdoortauglichen APs zu prüfen. <

KONTAKT

Boll Engineering AG, Patrick Michel
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch