Umfassende Sicherheit für WLANs

Durch die Integration verteilter «Access Points» (APs) in leistungsfähige Multi-Threat Security-Appliances entstehen WLANs mit maximaler Sicherheit. Solche WLANs sind hoch performant und gleich sicher wie kabelgebundene LANs.

Ob Public Hot-Spot, WLAN auf dem Firmengelände oder kabelloser Netzwerkzugriff für mobile Mitarbeitende – der drahtlose Zugang ins LAN hat sich weitgehend etabliert. Dieser grundsätzlich positiven Entwicklung steht die Tatsache gegenüber, dass Funknetzwerke beziehungsweise Access Points (APs) neue Sicherheitslücken schaffen. Sind drahtlose Netzwerke nicht entsprechend geschützt, ermöglichen sie Hackern auf vergleichsweise einfache Art und Weise den unbemerkten Zugriff auf fremde Daten. Risiken wie Denial-of-Service-Attacken, MAC-Spoofing, Man-in-the-middle-Attacken oder die verdeckte Netz-Einbindung sogenannter «Rogue APs» sind ausgeprägt. Ungenügend gesicherte WLANs bieten zudem Raum für Probleme wie Datenverlust und Performanceeinbrüche durch Überlast.

Das Gefahrenpotenzial von WLANs erfordert die Integration wirksamer Schutzmechanismen. Dabei reicht es nicht, die einzelnen APs bzw. WLAN-Router mit Firewall-Funktionen zu bestücken und die Datenkommunikation mit und zu den mobilen Devices zu verschlüsseln. Vorkehrungen dieser Art führen noch nicht zu einer umfassenden Sicherheit. Denn: Verteilte APs lassen sich kaum managen, was das regelmässige Einspielen neuer Signaturen aufwendig, wenn nicht gar unmöglich macht.

Rezeptur für eine starke Security

Dieser Problematik begegnen «Secure-Wireless-LAN-Lösungen», die Access Points und UTM-Appliances zu einem integralen Ganzen verbinden. Sie vereinfachen den Aufbau hoch sicherer WLANs, offerieren ein zentrales und umfassendes Sicherheitsmanagement und gewähren in aller Regel eine hohe Skalierbarkeit.

Secure-Wireless-LAN-Lösungen machen WLANs gleich sicher wie kabelgebundene LANs.

Bildquelle: Boll/Fortinet

Dreh- und Angelpunkt entsprechender Lösungen bilden sogenannte UTM- bzw. Multi-Threat Security-Appliances. Sie beinhalten sämtliche heute denkbaren Abwehr- und Sicherheitsmechanismen in einem System. Dazu gehören Funktionen wie Firewall, Antivirus, Antispam, Intrusion Prevention, Application Control, SSL Traffic Inspection und WAN-Optimierung. UTM-Systeme bieten einen ausgewachsenen Perimeter-Schutz und werden von KMU und Grossunternehmen gleichermassen genutzt.

Durch die Verknüpfung von APs und Security-Appliance, die mit AP-Controller-Funktionen ausgerüstet sind, lassen sich einfach und schnell hochsichere WLANs realisieren. Dabei wird der Datenverkehr durch die Multi-Threat Security-Appliances geleitet. Als Folge dessen werden die übertragenen Daten mit allen verfügbaren Sicherheitsmechanismen überprüft, bevor sie ins Firmennetz gelangen. Von Bedeutung ist dabei, dass die Kommunikation zwischen AP und Controller via Tunnel erfolgt, was die Implementation ins Netzwerk vereinfacht. Ebenso wichtig ist die Erkennung sowie der automatische Ausschluss nicht autorisierter, von Unberechtigten eingeschleuster Access Points («Rogue APs»). Ein weiteres Leistungsmerkmal ist das unterbruchsfreie Mitführen einer Session von einem AP zum nächsten. Dies in Kombination mit QoS, einem Leistungsmerkmal, das namentlich bei der WLAN-basierten Telefonie eine Notwendigkeit ist.

Die Nutzung von UTM-Appliances als «AP-WLAN-Controller» führt nicht nur zu einer maximierten Sicherheit bei Funknetzwerken. Entscheidend ist auch, dass UTM-basierte Lösungen den Einsatz von «Thin Access Points» ermöglichen, was die Kosten markant reduziert. Lassen sich bereits vorhandene UTM-Appliances mit Controller-Funktionen erweitern, reduzieren sich die Investitionen weiter.

Gesamtlösungen für (Funk-)Netze

Leistungsfähige «Secure-Wireless-LAN-Lösungen» sind in der Lage, einige wenige bis mehrere Tausend APs und demzufolge bis zu mehrere Zehntausend gleichzeitige User zu verwalten. Auch hinsichtlich Datenraten sind kaum Grenzen gesetzt. So sind AP-Controller erhältlich, die WLAN-Kapazitäten von bis zu 49 Gbps unterstützen.

Auch auf Seiten der Access Points sind hinsichtlich Sicherheit und Performance kaum Grenzen auszumachen. So sind Lösungen mit Datendurchsatzraten von bis zu 600 Mbps, mit simultaner Unterstützung von zwei Frequenzen (2,4 und 5 GHz), mit mehreren integrierten Antennen sowie der Kompatibilität zur 802.11n-Norm erhältlich. Besonders erwähnenswert sind ferner auf «Power over Ethernet» (PoE) basierte Lösungen. Je nach Anwendungsbereich sind ferner Leistungsmerkmale wie PCI-DSS-Konformität (fest zugewiesene Frequenzen) oder im Gehäuseinneren versteckte Antennen zur Minimierung des Vandalismus von Relevanz. <

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

DER AUTOR

Thomas Boll,
Boll Engineering,
Wettingen