LANCOM Systems

Leitfaden für WLAN-Sicherheit in Hotels

Die Sicherheit spielt beim WLAN im Hotel eine zentrale Rolle − für den Hotelier genauso wie für den Gast. Wir haben für Sie einen Leitfaden entwickelt, welche Sicherheitsaspekte Sie bei der Auswahl der Hardware-Komponenten für Ihr Hotel-WLAN und der Konfiguration Ihres Netzes beachten sollten.

1) Trennen Sie das Gastnetz vom übrigen Hotelnetz.

Wenn Sie Ihren Gästen einen Internetzugang zur Verfügung stellen möchten, richten Sie ein separates Gastnetz (Hotspot / Public Spot) mit webbasierter Benutzer-Authentifizierung ein. Die Authentifizierung stellt sicher, dass nur die Hotelgäste im Besitz der entsprechenden Zugangsdaten Zugriff zum Gastnetz erhalten. Dieses Netz ist durch eine eigene SSID – ein frei wählbarer „Name“ eines Funknetzes − von allen anderen Netzen getrennt. Auf den Hotelverwaltungsserver oder auf die Buchhaltung kann vom Gastnetz aus nicht zugegriffen werden.

Erlauben Sie auf der Gast-SSID nicht, dass die Clients untereinander kommunizieren dürfen. In einem Gastnetz, das nur Internet-Zugang bieten soll, besteht kein Bedarf für eine Kommunikation der Gäste-PCs untereinander. Im Gegenteil stellt dies ein Sicherheitsrisiko dar, falls Gäste versehentlich offene Freigaben auf ihren Notebooks haben.

Tipp: Die beste Wahl ist hier eine Hotspot-Option, die auf Access Points (Basis-Stationen), WLAN Controllern (zentrale Steuerungs- und Managementgeräte) oder Routern aktiviert werden kann, wie z. B. die LANCOM Public Spot-Option. So benötigen Sie keine zusätzliche Infrastruktur.

2) Verschlüsseln Sie die SSIDs mit WPA2.

Weisen Sie jedem Teilnetz innerhalb des Hotelnetzwerks eine eigene SSID zu, z. B. dem Gastnetz, dem Verwaltungsnetz, dem Restaurantnetz etc. Jedes dieser Teilnetze lässt sich zusätzlich verschlüsseln. Nach heutigem Standard sollten Sie die SSIDs mit WPA2 verschlüsseln. Zur zusätzlichen Sicherheit lässt sich jeder SSID ein eigenes WPA2-Passwort zuweisen.

In der Praxis werden Gastnetze nicht verschlüsselt, da diese nur dem Internetzugang des Gastes dienen. Eine Authentifizierung erfolgt dann über eine webbasierte Schnittstelle (Public Spot). Die Mitarbeiternetze hingegen müssen zwingend verschlüsselt werden. Bedingt durch die unterschiedlichen Sicherheitsanforderungen von Gast- und Mitarbeiternetz, müssen diese Netze voneinander getrennt werden.

Hinweis: Aktuelle Profi-Geräte unterstützen WPA2 in der Regel standardmäßig. Sollten Sie noch ältere Access Points mit WEP nutzen, empfehlen wir Ihnen dringend den Umstieg.

LANCOM Systems

3) **Trennen Sie die einzelnen Netze auf Layer 2 oder Layer 3 voneinander.**

Auf Layer 2 (= Netzwerkebene 2) steht jede SSID für ein eigenes Teilnetz, die auf einem VLAN – einem virtuell abgetrennten Netzbereich – abgebildet wird. Diese VLANs (z. B. Gastnetz, Verwaltung, Restaurant etc.) müssen auch auf den Netzwerkkomponenten voneinander getrennt werden. Dafür lassen sich z.B. die Access Points und Switches (zentrale Netzwerkverteiler) entsprechend konfigurieren.

Wichtig: Ihre Access Points müssen sowohl Multi-SSID-fähig sein als auch VLAN unterstützen. Etwaige Switches in Ihrem Netz müssen ebenfalls VLAN unterstützen.

Bei der Netztrennung auf Layer 3 (= Netzwerkebene 3) ist die aufwendige VLAN-Konfiguration nicht mehr notwendig. Hierfür benötigt Ihr Netz einen WLAN Controller, mit dem sich Ihre Access Points zentral managen lassen. Ein Layer-3-Tunnel zwischen den Access Points und dem WLAN Controller trennt das WLAN vom darunter liegenden Netzwerk.

Vorteil: Die Konfiguration eines solchen Netzes ist wesentlich einfacher, und Sie können auch günstige Switches nutzen, die kein VLAN unterstützen.

4) **Nutzen Sie einen RADIUS-Server für Ihr internes Netz.**

Verwenden Sie zur höchstmöglichen Sicherheit einen RADIUS-Server für die Authentifizierung der WLAN-Benutzer. Mit individuellem Benutzernamen und Passwort authentifiziert sich ein Client gegenüber einem Access Point bzw. dem RADIUS-Server. „Fremde“ Clients werden abgewiesen und erhalten keinen Zugriff zum Hotelnetz.

Tipp: Kaufen Sie Access Points oder WLAN Controller mit integriertem RADIUS-Server. So benötigen Sie keine zusätzliche Infrastruktur. Alternativ können Sie einen externen RADIUS-Server nutzen.

Wenn Sie all diese Empfehlungen beherzigen, sind Sie und Ihr WLAN-Netzwerk auf der sicheren Seite!