Leitfaden für den sichereren Hotspot-Betrieb

Hotspot-Betreiber haben vielfältige Anforderungen an ihren Service. Der vorliegende Leitfaden gibt Ihnen eine Orientierung, wie Sie einen WLAN-Hotspot unkompliziert und sicher bereitstellen. Nutzen Sie die jahrelange Expertise von LANCOM Systems, um Ihre Bandbreite ideal zu nutzen und Ihre sowie die Daten Ihrer Kunden sicher verwaltet zu wissen.

Technische Tipps

a) Professionelle Hotspot-Lösung

Setzen Sie für den WLAN-Gastzugang eine professionelle Hotspot-Lösung ein, die über webbasierte Benutzer-Authentifizierung mit LANCOM Public Spot Option oder Cloud-managed Hotspot über die LANCOM Management Cloud verfügt. So stellen Sie sicher, dass sich nur Ihre Gäste, die im Besitz eines (zeit- oder volumenbegrenzten) Tickets / Vouchers sind, mit den entsprechenden Zugangsdaten in das Gastnetz einwählen können.

b) Trennung der Teilnetze (Gäste, Verwaltung und Service)

Weisen Sie jedem Teilnetz für Verwaltung, Gäste und Service eine eigene SSID zu, z. B. dem Gastnetz, dem Verwaltungsnetz, dem Restaurantnetz etc. Achten Sie gleichzeitig darauf, dass Sie nicht zu viele Teilnetze einrichten, da die Effizienz des Gesamtnetzwerks dadurch beeinträchtigt werden kann. Nach heutigem Standard sollten Sie alle SSIDs mit WPA2 oder WPA3 verschlüsseln, die Ausnahme bildet das Gastnetz: Dieses wird in der Praxis nicht verschlüsselt, da die Authentifizierung des Gastes über eine webbasierte Schnittstelle erfolgt. So können sich nur Gäste, die Anmeldedaten besitzen, einwählen. Wichtig ist, dass sie die Teilnetze auch auf Netzwerkebene trennen. Hierzu gibt es mehrere Möglichkeiten. Ihr zuständiges IT-Systemhaus kann Sie dazu beraten und eine solche Netztrennung für Sie realisieren (LANCOM Partner finden).

c) Keine Kommunikation der Endgeräte untereinander auf der Gast-SSID

Schließen Sie auf der Gast-SSID aus, dass die Endgeräte (Tablets, Smartphones, Laptops) miteinander kommunizieren. In einem Gastnetz, das nur Internet-Zugang bietet, besteht kein Bedarf für eine Kommunikation der Endgeräte untereinander. Im Gegenteil birgt dies ein hohes Sicherheitsrisiko, falls Gäste versehentlich offene Freigaben auf ihren Endgeräten erlauben. LANCOM Access Points ermöglichen diese Funktion.

d) Einschränkung der Web-Zugriffe

Bitte beachten Sie, dass Sie den Gast bei jeglicher Beschränkung des Internetzugriffes in den AGB darauf hinweisen sollten (siehe „Weitere Tipps“).

- Portsperren: Wir empfehlen Ports z. B. für Peer-to-Peer-Verbindungen zu sperren, über die viele illegale Tauschbörsen im Netz funktionieren. Am besten sperren Sie die Ports über die in der zentralen Netzwerkkomponente (z. B. im Router) integrierte Firewall. Hierbei empfehlen wir in der Praxis eine „Deny-All-Strategie“ zu verfolgen: Sperren Sie alle Ports und öffnen Sie nur genau die Dienste, die Sie erlauben wollen, z. B. Port 80 für das einfache Surfen, Port 53 für DNS, Port 443 für HTTPS (sichere Internetseiten), Port 110, 143, 465, 993 und 995 für E-Mail sowie Port 500 und 4500 für VPN-Anwendungen. Besuchen Sie unsere KnowledgeBase, um konkrete Hilfestellungen bei weitergehenden Fragen zu erhalten.
- Content Filter: Wir empfehlen einen Web-Content-Filter einzusetzen, mit dem Sie unangemessene Internetinhalte sperren können. Nach Belieben lassen sich mit dieser Software gezielte Webseiten-Kategorien, wie z. B. „Gewalt“ und „Pornografie“, sperren.
- Firewall: Die steigende Zahl an Cyber-Angriffen zeichnen ein bedrohliches Szenario für die Sicherheit und Verfügbarkeit Ihrer Daten und und die Ihrer Gäste. Eine passende Firewall-Lösung stellt sicher, dass Ihre sensiblen Daten gegen Angriffe sowohl aus dem Netzwerk heraus (z. B. aus dem Gastnetz) als auch von außen geschützt sind. Sichern Sie diese Daten maximal vor unerwünschten Zugriffen und Cyberattacken mit einer wirkungsvollen und vertrauenswürdigen Security-Architektur „Made in Germany“, denn: Nicht-EU-Anbietern von Sicherheitstechnologien ist es unmöglich, gleichzeitig der europäischen und der Gesetzgebung ihrer Heimatstaaten zu genügen, sodass das Risiko eines externen Zugriffs und Datenabflusses besteht.

Weitere Tipps

a) Kennzeichnung des Internet-Anschlusses

Machen Sie deutlich, dass sich Ihre Rolle als Anschlussinhaber auf eine passive Internet-Zugangsvermittlung (WLAN-Hotspot) für Dritte beschränkt: Melden Sie den Internetanschluss deshalb mit Ihrer geschäftlichen Bezeichnung beim Provider an. Bei einem Hotel wäre dies z. B. „Hotel Musterhotel, Inhaber: Max Mustermann“, statt ausschließlich Vor- und Zunamen zu nutzen.

b) AGB zur Hotspot-Nutzung

Vorab: AGB in der Anmeldemaske sind keine Pflicht! Sie stellen eine Möglichkeit dar, Ihr Unternehmen auf dem Endgerät des Gastes oder Kunden nochmals zu präsentieren und Rahmenbedingung der Hotspotnutzung festzulegen. Stellen Sie sicher, dass Ihre Gäste und Kunden vor der Hotspot-Nutzung Ihre AGB akzeptieren und dass diese mit den aktuellen DSGVO-Richtlinien konform sind.

Darin sollten Ihre Gäste insbesondere einwilligen, dass Sie keine urheberrechtlich geschützten Materialien, wie Musik, Filme und Bilder ins Netz oder aus dem Netz

laden oder anderweitig gegen geltendes Recht verstoßen werden. Dies funktioniert unkompliziert: In der Anmeldemaske zum Hotspot verpflichten Sie Ihre Gäste und Kunden per Mausklick, die AGB zu bestätigen. Sprechen Sie zur technischen Realisierung Ihr IT-Systemhaus an.

c) Keine Weitergabe der Zugangsdaten an Dritte

Weisen Sie den Gast in den AGB darauf hin, dass er die Zugangsdaten zum WLAN-Gastzugang keinesfalls an Dritte weitergeben darf. Ausgenommen hiervon sind Gruppentickets, die Sie mit der LANCOM Public Spot Option oder der LANCOM Management Cloud, z. B. für Konferenzen in Ihrem Haus, erstellen können. Hier bekommen praktischerweise alle Konferenzteilnehmer denselben Zugangscode zum Gastnetz. Stellen Sie hier sicher, dass diese Gruppentickets nur für die Dauer der Veranstaltung gelten. Die unkontrollierte Nutzung Ihres Hotspots hat direkten Einfluss für Ihre Kunden und Gäste, da deutlich mehr Bandbreite genutzt wird.

d) Datenspeicherung

Grundsätzlich sollten Sie nur die Daten Ihrer Kunden erfassen, die für die technische Abwicklung und Abrechnung des WLAN-Hotspots erforderlich sind*.

Bestandsdaten: Unter Bestandsdaten sind Angaben wie Name, Anschrift, Geburtsdatum, ggf. eine Bankverbindung sowie technische Daten des Anschlusses (feste IP-Adressen) zu verstehen. Wir empfehlen Ihnen, Bestandsdaten Ihrer Kunden für einen definierten Zeitraum zu speichern, damit Sie im Bedarfsfall Kontakt aufnehmen können. Holen Sie sich hierzu das Einverständnis des Kunden per Einwilligung in Ihre AGB ein.

Bezüglich der Diskussion zur Vorratsdatenspeicherung sind Sie als Hotspot-Betreiber nicht in der Pflicht: Das entsprechende Gesetz betrifft ausschließlich Telekommunikations-Provider, nicht den Anbieter eines WLAN-Zuganges.

e) Portsperren / Content Filter

Weisen Sie Ihren Gast in den AGB darauf hin, wenn Sie den Internetzugang in irgendeiner Weise beschränken. Wenn Sie Portsperren, z. B. für Peer-to-Peer- oder VPN-Verbindungen und / oder einen Web-Content-Filter (LANCOM Content Filter) zur Sperrung gezielter Webseiten eingerichtet haben, legen Sie dies Ihren Gästen vor der Nutzung des Hotspots ausdrücklich dar.

Wenn Sie weitere Fragen haben, sprechen Sie uns gerne dazu an:
LANCOM Systems GmbH, Vertriebsinnendienst, Tel.: +49 (0) 2405/499 36-333.

* Diese Angaben beziehen sich auf die Rechtslage in der Bundesrepublik Deutschland. Für andere Länder informieren Sie sich über die jeweils geltende Rechtslage.

LANCOM Systems GmbH
Adenauerstr. 20/B2
52146 Würselen | Germany
info@lancom.de
www.lancom-systems.de