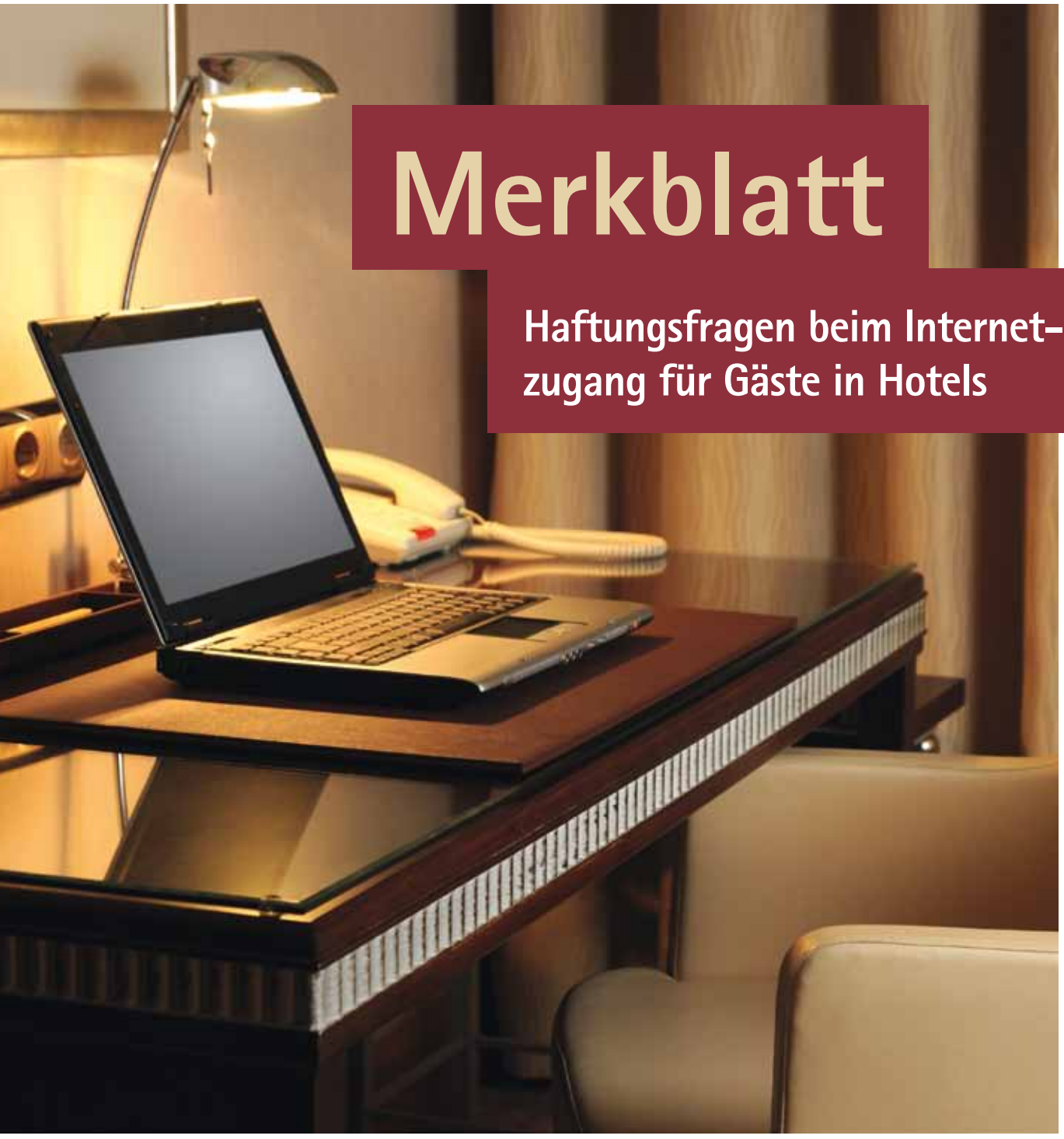

Merkblatt

Haftungsfragen beim Internet-zugang für Gäste in Hotels

Inklusive Nutzungsbedingungen
in Deutsch und Englisch

SERVICE

IMPRESSUM

HERAUSGEBER:

Hotelverband Deutschland (IHA) e.V.
Am Weidendamm 1A
10117 Berlin

Telefon	030 / 59 00 99 69-0
Telefax	030 / 59 00 99 69-9
E-Mail	office@hotelverband.de
Web	www.hotelverband.de

VERFASSER:

Stefan Dinnendahl
Geschäftsführer
Hotelverband Deutschland (IHA) e.V.
E-Mail: dinnendahl@hotellerie.de

Meinhard Kirchner
Referent / Justitiar
Hotelverband Deutschland (IHA) e.V.
E-Mail: kirchner@hotellerie.de

VERLEGER:

IHA-Service GmbH
Kronprinzenstraße 37
53173 Bonn

Telefon	0228 / 92 39 29-0
Telefax	0228 / 92 39 29-9
E-Mail	info@iha-service.de
Web	www.iha-service.de

VORWORT

Der Hotelverband Deutschland (IHA) empfiehlt seinen Mitgliedsunternehmen, die Ihren Gästen einen Internetzugang bereitstellen, die beigefügten Nutzungshinweise unverbindlich zur Verwendung im Geschäftsverkehr mit den Kunden. Den Adressaten steht es frei, der Empfehlung zu folgen oder andere Nutzungshinweise zu verwenden.

Das Merkblatt dient ausschließlich der allgemeinen Information und kann eine rechtliche Beurteilung im Einzelfall oder die Beratung durch einen Anwalt nicht ersetzen.

Auch wenn dieses Merkblatt mit größter Sorgfalt erstellt wurde und der Hotelverband Deutschland (IHA) sich stets bemüht, dieses Merkblatt an die aktuelle Rechtsprechung anzupassen, übernimmt er keine Gewähr für die Richtigkeit, Vollständigkeit und Aktualität seines Inhaltes noch haftet er für Schäden, die aus der Benutzung des Merkblattes entstehen könnten.

Der Hotelverband Deutschland (IHA) dankt seinen Preferred Partners, die an der Erstellung dieses Merkblattes beteiligt waren.

Berlin / Bonn, Januar 2012

I. EINLEITUNG

Ob drahtlos oder drahtgebunden, in der Lobby oder auf den Gästezimmern, gratis oder kostenpflichtig – ein Internetzugang im Hotel ist für den Gast inzwischen zum Standard geworden. Er wird besonders von Geschäftsreisenden erwartet und ist für den Kunden ein Auswahlkriterium. Mit der Bereitstellung des Internetzuganges ergeben sich jedoch eine Vielzahl technischer und rechtlicher Herausforderungen für den Hotelier.

So verzeichnet der Hotelverband Deutschland (IHA) bereits seit geraumer Zeit vermehrt Abmahnungen gegen Hotels wegen Urheberrechtsverletzungen, welche von Gästen begangen wurden, die über den Internetzugang des Hotels gesurft hatten. Parallel dazu hat die Rechtsprechung die Betreiber der Internet- bzw. WLAN-Anschlüsse in Fällen des illegalen Filesharings über die sogenannte „Störerhaftung" verantwortlich gemacht.

PRAXISTIPP:

Rechts- und IT-Experten raten deshalb, bei der Konzeption und der Installation von WLAN-Hotspots in Hotels Sicherheitsüberlegungen eine Schlüsselrolle zukommen zu lassen.

Um den Hotelier für die Problematik zu sensibilisieren, skizziert dieses Merkblatt die Haftungssituation des Hoteliers und wirft einen Blick auf die aktuelle Rechtsprechung auf diesem Gebiet (siehe II).

Weiterhin werden Lösungen aufgezeigt, die der Hotelverband Deutschland (IHA) mit seinen Preferred Partnern entwickelt hat, um das Haftungsrisiko für Internetzugänge in Hotels zu minimieren (siehe III). Darunter befindet sich auch eine Checkliste mit Sicherheitsaspekten für die Auswahl von Hardware-Komponenten und die Konfiguration des Hotelnetzes, die bei der Einrichtung eines WLAN-Netzes im Hotel beachtet werden sollten (siehe III.D). Diese Liste haben wir gemeinsam mit unserem Preferred Partner Lancom erarbeitet.

Abschließend sind diesem Merkblatt Hinweise zur Nutzung des Internetzugangs in Hotels beigefügt. Der Hotelier findet hier die aus Sicht des Hotelverbandes Deutschland (IHA) wichtigen Aspekte, welche der Gast bei der Benutzung eines Internetzugangs im Hotel zu beachten hat, und kann ihm diese vorlegen (siehe IV).

II. HAFTUNGSSITUATION FÜR HOTELIERS

Urheberrechtsverletzungen, die über das Internet begangen wurden, sind in den letzten Jahren vermehrt abgemahnt worden. Unter diesen Abmahnungen sind auch viele, die sich gegen Hotels richten. Ausgangspunkt sind oft sogenannte Online-Tauschbörsen, auf denen Musikdateien oder Ähnliches zum Up- und Download angeboten werden.

Illegale Up- oder Downloads erfolgen zumeist über Filesharing-Systeme im Internet. Die einschlägigen Tauschbörsen werden im Auftrag der Film- oder Musikindustrie ständig nach illegalen Dateien durchsucht, und die betroffenen Unternehmen verfolgen diese Verletzungen über ihre Anwälte sehr offensiv. Wer ertappt wird, läuft Gefahr, ein Abmahnschreiben mit Androhung einer empfindlichen Geldstrafe zu kassie-

ren und zur Abgabe einer strafbewehrten Unterlassungserklärung aufgefordert zu werden.

Werden solche Tauschbörsen von Hotelgästen genutzt, die über den hoteleigenen Internetzugang surfen, kann der Hotelier als Inhaber des Internetanschlusses über die sogenannte „Störerhaftung“ ins Visier der Abmahnindustrie geraten.

A. WAS KANN ABGEMAHNT WERDEN?

Das Urheberrecht schützt Werke vor unbefugter Nutzung. Hierzu gehört unter anderem das Bereitstellen urheberrechtlich geschützter Musiktitel, Filme, Hörbücher etc. per Upload. Dies gilt als öffentliches Zugänglichmachen der jeweiligen Bild-, Video- oder MP3-Dateien für Dritte und ist damit – wenn es unberechtigt erfolgt – illegal. Parallel dazu ist der Download solcher Dateien eine unerlaubte Verwertung von urheberrechtlich geschützten Werken und damit illegal, wenn die Vorlage offensichtlich rechtswidrig im Internet angeboten wird. Solche Fälle können unter anderem zivilrechtliche Schadensersatzforderungen nach sich ziehen.

B. WAS TUN IM FALLE EINER ABMAHNUNG?

Eine Abmahnung ist ein außergerichtliches Vergleichsangebot des Rechteinhabers. Dieser rügt darin das Verhalten des Abgemahnten als rechtswidrig und fordert ihn auf, dies zukünftig zu unterlassen. Sinn und Zweck der Abmahnung ist es, den Rechtsstreit um die Verletzung eines Rechtes schnell in einem außergerichtlichen Verfahren beizulegen.

Das Angebot des Rechteinhabers besteht in der Regel aus drei Teilen:

- Der Hotelier wird aufgefordert, die abgemahnte Datei endgültig vom Rechner zu löschen.
- Der Hotelier wird aufgefordert, einen pauschalen Betrag als Schadensersatz zu zahlen. In diesem Betrag sind die Kosten des abmahnenden Anwalts sowie teilweise auch ein Ersatz für den durch die Urheberrechtsverletzung entstandenen Schaden enthalten.
- Der Hotelier wird aufgefordert, eine Unterlassungserklärung, gerichtet auf künftige Verstöße, in einer bestimmten, sehr kurzen Frist abzugeben.

PRAXISTIPP:

Da sich aus einer Abmahnung Rechtsfolgen ergeben, die für den Hotelier nicht nur verbindlich sind, sondern ihn auch bis zu 30 Jahre verpflichten können, sollte auf ein solches Schreiben nie ohne rechtliche Beratung reagiert werden.
Auf keinen Fall kann empfohlen werden, auf eine Abmahnung gar nicht zu antworten.

C. WARUM WIRD DER HOTELIER ABGEMAHNT?

Beim Tauschvorgang in den Filesharing-Systemen werden dem Server der Tauschbörse verschiedene Daten mitgeteilt. Zum einen um welche Dateien es sich handelt und weiterhin die sogenannte IP-Adresse dessen, der die Dateien anbietet oder her-

unterlädt. Dies ist eine Art Identifikationsnummer, die der Computer für die Zeit, in der er mit dem Internet verbunden ist, zugeteilt bekommt.

Im Falle einer Urheberrechtsverletzung über solche Tauschbörsen wird zunächst bei der Staatsanwaltschaft ein Ermittlungsverfahren eingeleitet. Im Zuge dessen ist der Internetprovider dann verpflichtet, der Staatsanwaltschaft den Namen des Nutzers der jeweiligen IP-Adresse mitzuteilen. Läuft der Internetanschluss auf den Namen des Hoteliers, richtet sich das folgende Verfahren gegen ihn - auch wenn es der Gast war, der über den hoteleigenen Internetzugang surfte. Als Anschlussinhaber und Hotspotbetreiber steht er zunächst im Visier der Abmahnanwälte. Zur Abwehr dieser Ansprüche ist der Hotelier dann in der Pflicht nachzuweisen, dass er die Verletzungshandlung nicht begangen hat.

Hotelier als Störer?

Kann der Hotelier nachweisen, dass er weder Täter noch Teilnehmer der Urheberrechtsverletzung war, scheidet zwar ein Schadensersatzanspruch gegen ihn aus. Dennoch kann vom Hotelier ein Unterlassen der Urheberrechtsverletzung auch für die Zukunft verlangt werden, wenn Dritte illegal geschützte Dateien über seinen Internetanschluss aus dem oder ins Internet laden. In diesem Fall hat er auch die Kosten der Abmahnung, die oft mehrere Hundert Euro betragen können, zu zahlen. Voraussetzung hierfür ist, dass er als Störer ursächlich zur Verletzung des Urheberrechts beiträgt, ohne dabei Täter oder Teilnehmer zu sein. In diesem Sinne gilt bereits die Zurverfügungstellung eines Internetzugangs für Dritte, beispielsweise ein WLAN für Gäste in einem Hotel, als eine solche ursächliche Mitwirkung. So hat das LG Hamburg entschieden, dass derjenige Störer ist, der seinen Internetzugang Unbefugten überlässt oder seinen WLAN-Hotspot nicht ausreichend gegen Unbefugte sichert, da er so zur Verletzung der geschützten Rechte beiträgt.[1] Nach dieser sehr weitgehenden Auffassung des LG Hamburg muss ein potentieller (Mit-)Störer alles unternehmen, um eine Rechtsverletzung zu verhindern.

Welches Haftungsrisiko gibt es?

Als Störer haftet der Hotelier jedoch nicht unbeschränkt. Für ihn ist es deshalb wichtig zu wissen, inwieweit und unter welchen Umständen er für Urheberrechtsverletzungen, die über seinen WLAN-Hotspot begangen werden, verantwortlich gemacht werden kann. Aktuell gibt es hierbei einige positive Entwicklungen in der Rechtsprechung, die entsprechende Sicherheitsanforderungen konkretisieren.

Keine offenen und ungesicherten WLAN-Zugänge

Das größte Haftungsrisiko besteht bei WLAN-Hotspots, die offen und ungesichert einen Internetzugang ermöglichen. Neben den oben genannten Entscheidungen des LG Hamburg, die sich auf privat genutzte Hotspots beziehen, gibt es auch eine aktuelle Entscheidung des gleichen Gerichts für gewerblich betriebene Internetzugänge. In einem Abmahnfall gegen einen Internetcafébetreiber entschied das Gericht zu Gunsten der Urheberrechtsinhaber.[2] Nach seiner Auffassung konnte der Internetcafébetreiber nach den Grundsätzen der Störerhaftung auf Unterlassen der Rechtsverletzung herangezogen werden, da er überhaupt keine ihm möglichen und zumutbaren Maßnahmen ergriffen hatte, um solche Rechtsverletzungen zu verhindern.

[1] LG Hamburg, Urteile vom 2. August 2006, Az. 308 O 509/06 und 26. Juli 2006, Az. 308 O 407/06

[2] LG Hamburg, Beschluss vom 25. November 2010, Az. 314 O 433/10.

Maßnahmen zur Einschränkung des Haftungsrisikos

Für gewerblich betriebene Internetzugänge ist noch nicht abschließend geklärt worden, welche Maßnahmen für einen kompletten Haftungsausschluss getroffen werden müssen. In einem viel beachteten Urteil hat der BGH festgelegt, dass der Inhaber eines WLAN-Anschlusses dann als Störer für Urheberrechtsverletzungen haften soll, wenn er es unterlässt, „die im Kaufzeitpunkt des WLAN-Routers marktüblichen Sicherungen ihrem Zweck entsprechend anzuwenden.“[3] Welche konkreten Maßnahmen zumutbar sind, bestimmt sich nach den jeweiligen technischen Möglichkeiten. Das Urteil bezieht sich jedoch nur auf private Haushalte. Ob es entsprechend auf WLAN-Hotspots in Hotels angewendet werden kann, ist fraglich. Eine erste Entscheidung mit dieser Tendenz kommt vom LG Frankfurt[4]: Mit Bezug auf das BGH-Urteil ist das Gericht der Ansicht, dass der Anschlussinhaber eines im Hotel betriebenen WLAN-Hotspots dann nicht haftet, wenn er sein Funk-Netzwerk mit einer marktüblichen Verschlüsselung gegen Urheberrechtsverletzungen Dritter sichert, seine Gäste vor der Nutzung des Internetzugangs auf die Einhaltung der gesetzlichen Vorgaben hinweist und es unstreitig ist, dass weder der Hotelier als Anschlussinhaber, noch seine Angestellten die Urheberrechtsverletzung begangen haben. Ob sich diese Meinung auch bei anderen Gerichten durchsetzen wird und welche Maßstäbe künftig die Rechtsprechung an die Verschlüsselung von Netzwerken und die Aufklärungspflichten eines gewerblichen Hotspot-Betreibers anlegt, verfolgen wir aufmerksam.

Erschwerend kommt hinzu, dass bei unerlaubten Handlungen ausnahmsweise das Gericht am Begehungsort angerufen werden kann. Begehungsort bei Urheberrechtsverletzungen im Internet kann allerdings jeder Ort sein, so dass der regelmäßig klagende Rechteinhaber als Gerichtsstand voraussichtlich Hamburg wählt, weil dort die für ihn vorteilhaftere Rechtsprechung vertreten wird.

PRAXISTIPP:

Im Lichte dieser Rechtsprechung sollten Hoteliers folgende Aspekte dringend beachten:

1. Der Hotelverband Deutschland (IHA) empfiehlt zu prüfen, inwieweit es wirtschaftlich vertretbar und technisch möglich ist, seinen Gästen eine Zugangslösung (Hotspot) eines externen Internetproviders (z. B. Deutsche Telekom /Stichwort: Hotspot-Partner werden) anzubieten. Bei dieser Lösung wird im Hotel lediglich ein Internet-Hotspot aufgestellt, der Gast surft über den Internetzugang des jeweiligen Hotspot-Betreibers, während der Hotelier nur Vermittler zwischen diesen beiden Vertragsparteien ist. So kann das Haftungsrisiko für den Hotelier bei richtiger Vertragsgestaltung minimiert werden.
2. Hoteliers, die einen eigenen Internetzugang anbieten, sollten das Haftungsrisiko durch professionelle und sichere Zugangslösungen minimieren, die von verschiedenen IT-Spezialisten angeboten werden. Bei diesen Angeboten bleiben Hotel und Gast Vertrags-

[3] BGH, Urteil vom 12. Mai 2010, Az. I ZR 121/08 „Sommer unseres Lebens“.

[4] LG Frankfurt, Urteil vom 18. August 2010, Az. 2-6 S 19/09.

partner und der Hotelier ist damit in der Preisgestaltung flexibel. Eine solche hotelspezifische Internetlösung bietet ebenfalls unser Preferred Partner Deutsche Telekom an.

3. Der Internetzugang im Hotel sollte auf Gäste beschränkt werden und technisch nicht für jedermann offen sein. Hierbei haben sich die (marktübliche) Verschlüsselung des Hotspots und zeitlich begrenzte sowie ausreichend sichere Zugangstickets für Gäste bewährt, um unbefugten Dritten keinen Zugang zu gewähren. Eine entsprechende Checkliste unseres Preferred Partners LANCOM Systems mit Hinweisen zum sicheren WLAN im Hotel finden Sie im folgenden Abschnitt (siehe unten III.D). Ebenso erfüllt auch die Hotspot-Lösung unseres Preferred Partners Deutsche Telekom diese Anforderungen (siehe unten III.A)
4. Die Nutzer sollten darüber informiert werden, dass keine urheberrechtlich geschützten Werke ins Netz oder aus dem Netz geladen werden dürfen oder anderweitig gegen geltendes Recht verstoßen werden darf. Hoteliers können hierzu die unten stehenden Nutzungsbedingungen für ihre Gäste verwenden (siehe unten IV).
5. Der Hotelier könnte auch für Urheberrechtsverstöße seiner Mitarbeiter zur Haftung herangezogen werden, sofern diese einen Zugang zum Internet über das Hotel haben. Insoweit sollte bei solchen Mitarbeitern eine entsprechende Belehrung in den Arbeitsvertrag integriert werden.
6. In datenschutzrechtlicher Hinsicht dürfen nur die Daten erfasst werden, die für die Abwicklung und Abrechnung der WLAN-Nutzung durch den Gast unbedingt erforderlich sind. Werden diese nicht mehr für die Abrechnung benötigt, sind sie unverzüglich zu löschen.
7. Die Speicherung von Daten die für die Sicherstellung der Funktionsfähigkeit WLAN-Systems erforderlich sind, ist für einen Zeitraum von bis zu sieben Tagen zulässig.
8. Eine technisch mögliche und weitergehende Speicherung der Verbindungsdaten der Internetnutzung von Gästen in Hotels (sogenannte Vorratsdatenspeicherung) ist seit dem Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung unzulässig.[5] Hier besteht für den Hotelier die dringende Gefahr, dass er damit massiv gegen das Datenschutzrecht verstößt.

[5] BVerfG, Urteil vom 2. März 2010, Az. 1BvR 256/08.

III. LÖSUNGEN FÜR HOTELIERS

Gemeinsam mit seinen Preferred Partnern hat der Hotelverband präventive und reaktive Lösungen für den Bereich Internetzugang per WLAN in Hotels entwickelt, die wir hier kurz vorstellen wollen.

PRAXISTIPP

Bei technischen Fragen und allgemeinen Auskünften zum Thema WLAN und Internet empfiehlt der Hotelverband Deutschland (IHA) die Seiten des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de).

Wenn Sie weitere Beratung wünschen, hilft die IHA-Service GmbH, Herr RA Stefan Dinnendahl, (info@iha-service.de oder Tel. 0228/92 39 29-0), Ihnen bei der Auswahl des richtigen Beratungspartners gerne weiter.

A. HOTSPOT-LÖSUNG DER DEUTSCHEN TELEKOM

Die Hotspot-Lösung unseres neuen Preferred Partners Deutsche Telekom bietet zusätzlich zu einem leistungsfähigen Internetzugang vor allem den Service aus einer Hand – Beratung, Planung, Installation und Wartung – so wird aus der persönlichen Datenleitung ein professioneller Hotspot. Er trennt den geschäftlichen Datenverkehr vom öffentlichen Surfen, protokolliert Einwahl und Nutzer, erfasst Online-Zeiten und -Volumina pro User und Sitzung und hat auch schon die Anbindung an externe Abrechnungsprogramme vorgedacht.

Erleben, was verbindet.

Die Hotspot-Komplettlösung der Telekom kann so dank Datentrennung und definierten Benutzergruppen parallel von Gästen, Verwaltung und Service genutzt werden und bietet gleichzeitig: First-Class-Service – Oberste Sicherheitsstufe – Neuesten Stand der Technik.

Bei dieser Lösung entscheiden Hotels selbstverständlich selbst, ob sie den Internet-Service gratis oder kostenpflichtig anbieten. Er gilt als wichtiger Buchungs-Anreiz. Abgerechnet werden kann dabei über automatisch erstellte Benutzertickets.

Einfach: Die Bedienung erfolgt ganz einfach über Rezeptions-PC und Standarddrucker, Sie sparen Schulungs- und Hardwarekosten. In nur drei Schritten – Eingabe, Prüfung, Ausdruck – halten Sie das Benutzerticket mit den Zugangsdaten für Ihren Gast in der Hand.

Transparent: Die Abrechnung ist genau und präzise nachvollziehbar – für den Gast ebenso wie für Sie als Betreiber.

Sicher: Die Content-Filter-Option schützt sowohl die Geschäfts- als auch die Netzwerkintegrität. So sind Sie sicher vor Angriffen von außen durch Spyware und Viren sowie vor einer rechtswidrigen Internetnutzung durch Mitarbeiter oder Gäste. Ihr persönlicher Komfort: Sie erhalten Beratung, Installation, Wartung und Service aus einer kompetenten Hand.

Ebenso besteht die Möglichkeit, eigene oder die vom Hotelverband Deutschland (IHA) erarbeiteten Nutzungsbedingungen so im System zu hinterlegen, dass der Gast erst nach deren Akzeptanz den Hotspot nutzen kann.

B. Rechtliche Beratung durch die Anwaltssozietät Beiten Burkhardt

Die Kanzlei Beiten Burkhardt berät die Hotel & Leisure Branche seit Jahren erfolgreich in der Erstellung und Verhandlung von IT-Verträgen aller Art sowie in Fragen des Markenrechts und Geistigen Eigentums. Das IP/IT-Team der Kanzlei umfasst mehr als 30 spezialisierte Berufsträger und verfügt über langjährige, umfassende Erfahrung in allen für die Tourismusindustrie relevanten Rechtsbereichen rund um die Themenkreise IT/Technologie und Geistiges Eigentum.

Beiten Burkhardt steht IHA-Mitgliedern bei haftungsrechtlichen Fragen und Unterlassungsansprüchen rund um Internetzugänge zur Verfügung. Wir empfehlen in diesem Zusammenhang, das Haftungsrisiko durch unseren Preferred Partner Büchner Barella Assekuranzmakler im Vorfeld versichern zu lassen, weil so im Zweifel die Rechts- bzw. Anwaltskosten ersetzt werden.

C. Versicherung des Haftungsrisikos

Bisher konnte ein Hotel sein verbleibendes Haftungsrisiko mit den marktüblichen Versicherungslösungen nicht versichern. Es ist uns gemeinsam mit unserem Preferred Partner Büchner Barella Assekuranzmakler über den IHA-Rahmenvertrag erstmals gelungen, eine versicherungstechnische Lösung sicherzustellen und Ansprüche im Zusammenhang mit Urheberrechtsverletzungen zu versichern. Danach gilt die Haftpflicht des Hotelbetriebes aus der Bereitstellung von Internetzugängen für Hotelgäste (z. B. über WLAN oder Hotspots) auch bei Schäden wegen Verletzung von Namens- oder Urheberrechten.

Der Versicherer bezahlt vor allem die Gerichts- und Anwaltskosten im Zusammenhang mit einer einstweiligen Verfügung und Unterlassungs- oder Widerrufsklage gegen den Hotelbetrieb.

Für IHA-Mitgliedsbetriebe, die bereits eine Haftpflichtversicherungslösung von Büchner Barella haben, ist dieser verbesserte Versicherungsschutz bereits ohne Mehrkosten sichergestellt.

D. LANCOM-Checkliste zum sicheren WLAN im Hotel

Die Sicherheit spielt beim WLAN im Hotel eine zentrale Rolle − für den Hotelier genauso wie für den Gast. Gemeinsam mit unserem Preferred Partner LANCOM haben wir exklusiv für Sie eine Checkliste 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. So kann vom Gastnetz nicht auf den Hotelverwaltungsserver oder auf die Buchhaltung aus zugegriffen werden.

Erlauben Sie im Gastnetz nicht, dass die Gäste-PCs untereinander kommunizieren dürfen. Dieses Netz soll nur den Internet-Zugang bieten. Eine Kommunikation der Gäste-PCs untereinander ist nicht notwendig und stellt zudem ein Sicherheitsrisiko dar, falls Gäste versehentlich offene Freigaben auf ihren Notebooks haben.

PRAXISTIPP:

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.

PRAXISTIPP:

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

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.

PRAXISTIPP:

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

IV. HINWEISE ZUR NUTZUNG DES INTERNETZUGANGES

Nach Auffassung verschiedener Gerichte hat der Betreiber eines WLAN-Hotspots die Pflicht, Dritte vor Nutzung des Internetzuganges darauf hinzuweisen, dass diese die gesetzlichen Vorgaben einzuhalten haben. In diesem Sinne hat der Hotelverband Deutschland (IHA) die folgenden *„Hinweise zur Nutzung unseres Internetzuganges“* erstellt und empfiehlt diese seinen Mitgliedern unverbindlich zur Verwendung im Geschäftsverkehr mit Gästen. Der Internetzugang sollte Gästen nur dann ermöglicht werden, wenn sie diese Hinweise zur Kenntnis genommen haben.

HINWEISE ZUR NUTZUNG UNSERES INTERNETZUGANGES

Verehrter Gast,

um Ihnen die Nutzung unseres Internetzuganges so unkompliziert und sicher wie möglich zu machen, bitten wir Sie, folgende Grundregeln zu beachten:

1. VERWENDEN SIE MÖGLICHST EINEN BROWSER MIT 128 BIT SSL-VERSCHLÜSSELUNG

Die aktuellen Versionen der gängigen Browser (Microsoft Internet Explorer, Apple Safari, Mozilla Firefox oder Opera) sind auf diesen Standard ausgelegt.

2. SCHÜTZEN SIE IHREN PC MIT AKTUELLEN VIRENSCHUTZPROGRAMMEN UND EINER FIREWALL

Installieren Sie eine Virenschutzsoftware auf Ihrem PC und aktualisieren Sie diese regelmäßig. Stellen Sie sicher, dass Ihr Rechner frei von Viren, Würmern und Trojanern/Backdoors ist.
Wir empfehlen Ihnen, Ihren Rechner mit einer Firewall und einer Anti-Spy-Software auszustatten und diese regelmäßig zu aktualisieren.
Bitte nehmen Sie zur Kenntnis, dass wir Ihnen lediglich einen Internetzugang zur Verfügung stellen, der über keinerlei Virenschutz und keine Firewall verfügt.

3. HALTEN SIE IHR BETRIEBSSYSTEM AUF DEM AKTUELLEN STAND

Installieren Sie die entsprechenden Updates und Patches für das Betriebssystem Ihres PCs zeitnah und regelmäßig.

4. SCHÜTZEN SIE IHRE DATEN AUCH FÜR DEN FALL DES VERLUSTES IHRES RECHNERS

Ihren PC und die darauf gespeicherten wichtigen Dateien sollten Sie mit Passwörtern sichern. Diese sollten regelmäßig geändert werden. Speichern Sie die Passwörter nicht auf Ihrer Festplatte ab. Stellen Sie Ihren Rechner nur Personen Ihres Vertrauens zur Verfügung.
Wir empfehlen Ihnen, regelmäßig ein Backup Ihrer Daten anzulegen.

5. STARTEN SIE BEI VERBINDUNGSFEHLERN IHREN BROWSER ERNEUT

Bei auftretenden Verbindungsfehlern schließen Sie bitte den Browser und starten ihn erneut. Stellen Sie die korrekte Eingabe Ihrer entsprechenden Passwörter sicher. Schließen Sie bitte Ihren Browser nach Beenden der Internetsitzung.

6. SEIEN SIE VORSICHTIG BEI UNBEKANNTEN DATEIEN ODER EMAIL-ANHÄNGEN

Öffnen Sie keine Dateien unbekannter Herkunft oder Dateien, die Sie nicht angefordert haben.

7. BESUCHEN SIE KEINE WEBSEITEN MIT STRAFRECHTLICH RELEVANTEN INHALTEN

Dies gilt insbesondere für Seiten mit volksverhetzendem oder kinderpornographischem Inhalt, Seiten, die zu Straftaten anleiten oder Gewalt verherrlichen bzw. verharmlosen oder Seiten, die geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden.

8. BETEILIGEN SIE SICH NICHT AN UNSERIÖSEN ODER ILLEGALEN TAUSCHBÖRSEN

Beachten Sie beim Herunterladen oder Aufspielen von Dateien, insbesondere Musik, Filmen oder Bildern stets, dass diese urheberrechtlich geschützt sein können. Die Verletzung solcher Urheberrechte kann unter anderem erhebliche Schadensersatzansprüche gegen Sie auslösen.

9. VERFÜGBARKEIT, GEEIGNETHEIT ODER ZUVERLÄSSIGKEIT DES INTERNETZUGANGES

Wir geben keine Gewähr für die tatsächliche Verfügbarkeit, Geeignetheit oder Zuverlässigkeit des Internetzuganges.

10. HAFTUNGSBESCHRÄNKUNG

Wir übernehmen keine Verantwortung für etwaige Schäden an Ihrem PC, die durch die Internetnutzung entstehen. Hiervon ausgenommen sind Schäden, zu denen wir vorsätzlich oder grob fahrlässig beigetragen haben. Insbesondere wird keinerlei Haftung für die Inhalte aufgerufener Websites oder heruntergeladener Dateien übernommen. Ferner wird auch keinerlei Haftung für einen etwaigen Virenbefall durch Verwendung des Internetzuganges übernommen.

11. HAFTUNGSFREISTELLUNG

Wir sind von sämtlichen Ansprüchen Dritter freizustellen, wenn unser Internetzugang von Ihnen oder mit Ihrer Billigung rechtswidrig verwendet wird, insbesondere wenn Sie die oben stehenden Hinweise schuldhaft außer Acht gelassen haben. Ebenfalls sind wir von sämtlichen Ansprüchen Dritter freizustellen, die sich aus urheberrechtlichen oder sonstigen rechtlichen Streitigkeiten ergeben, die mit Nutzung des Internetzuganges durch Sie verbunden sind.

12. DATENSCHUTZ

Soweit wir Ihre Daten im Rahmen der Internetnutzung über unseren Internetzugang erheben, werden diese selbstverständlich gemäß der geltenden Datenschutzbestimmungen behandelt.

13. VERSTOSS GEGEN DIE NUTZUNGSHINWEISE

Sofern Sie gegen diese Nutzungshinweise verstoßen oder wir einen entsprechenden Verdacht haben, sehen wir uns gezwungen, Ihren Internetzugang einzuschränken oder zu sperren. Sollten Sie hierbei Daten verlieren, übernehmen wir dafür keine Haftung.

14. WEITERE HINWEISE

Die Nutzung unseres Internetzuganges ist auf die Dauer Ihrer Anwesenheit im Hotel beschränkt. Die Nutzung erfolgt durch Eingabe eines Passwortes. Dieses darf nicht an Dritte weitergegeben werden.
Bei Fragen oder Problemen mit dem Internetzugang hilft Ihnen gerne unsere Rezeption (Tel.: …) weiter.
Bei technischen Fragen und allgemeinen Auskünften zum Thema WLAN und Internet empfehlen wir die Seiten des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de).

[Ort, Datum], Unterschrift des Gastes