

# Internetzugang für Gäste im Hotel

## Risiken - rechtliche Bewertung - Maßnahmen - Angebot

Der moderne Hotelgast von heute erwartet, dass er sich mit seinem Notebook, Handy, iPod oder PDA bequem per WLAN mit dem HotSpot eines Hotels verbindet und surft, mailt oder eine Firmenverbindung nutzt. Viele Hotel-HotSpots entsprechen nicht den gesetzlichen Anforderungen und bringen die Geschäftsführer in große Gefahr!

### Thema: Um was geht es?

Hotelgäste wollen heute preiswerten und einfachen Internetzugang in Hotels. Am beliebtesten ist der kostenlose, unbeschränkte, einfache unverschlüsselte Zugang. Damit ist die Kundenbindung am größten und es gibt die wenigsten Probleme, auch mit immer exotischer werdenden Geräten wie iPhones, PDAs, iPods und Handys.

Der hoteleigene Internetzugang wird den Gästen zur Verfügung gestellt. Das ist die günstigste Lösung, weil praktisch keine anlaufenden Kosten entstehen. Aber alle Aktivitäten im Internet fallen damit auf den Hotelier zurück, weil seine IP-Adresse mit seinem Vertrag beim Provider gespeichert ist.

Bei der Internetnutzung könnten auch Straftaten begangen werden. Das schlimmste Beispiel ist sicher die Kinderpornographie, aber das Feld der Möglichkeiten ist weit.

Der Gast selbst kann durch den Internetzugang geschädigt werden. Sein Computer kann durch Schadsoftware (Viren) beeinträchtigt werden. Auch sind dadurch erhebliche Folgeschäden möglich, für die der Gast das Hotel verantwortlich machen kann, zum Beispiel, weil das Hotel keine Schutzmaßnahmen getroffen hat

### Risiken: Welche?

Schadensersatzforderungen vom Gast wegen Schäden, die auf die Nutzung des Internetzugangs zurückzuführen sind. Die denkbaren Szenarien sind vielfältig. Viren oder andere Schadsoftware können den Gastcomputer kompromittieren, was wiederum zu hohen Folgeschäden führen kann (entgangener Auftrag, ...). Der Gast muss informiert sein, dass das Hotel keine aufwändigen Abwehrmechanismen installiert hat, sondern einen ungefilterten Internetzugriff bereitstellt, und er selbst alle entsprechenden Schutzmaßnahmen treffen muss.

Schäden können auch durch gegenseitiges Abhören der Gäste entstehen. Egal, ob das WLAN verschlüsselt oder unverschlüsselt betrieben wird, die Gäste können sich immer gegenseitig abhören, weil sie alle das gleiche Passwort kennen. Über diese Gefahr muss der Gast informiert werden. Er kann nur durch Nutzung eines VPNs sicher vor solchen Angriffen sein. Bei einer Messe oder dem Abgabetermin einer Ausschreibung ist die Wahrscheinlichkeit hoch, dass direkte Konkurrenten im gleichen Hotel wohnen. Zudem sind auf fast allen Computern die Firewallregeln für das interne Netz weniger restriktiv eingestellt, als für das Internet. Im Hotel-WLAN sind aber alle Gäste im gleichen internen Netzwerk.

Durch die Bereitstellung des Internetzugangs entstehen auch Haftungsrisiken. Der Gast muss darüber informiert werden, dass er keinerlei Rechtsanspruch auf die 100%-ige Verfügbarkeit der Leistung hat. Sonst drohen im Falle eines Ausfalls wiederum Schadensersatzklagen.

Die Verantwortung für die aus dem Internet durch den Gast bezogenen Inhalte muss im Vorfeld abgelehnt werden, weil sie fremde Inhalte im Sinne des §5 Abs.3 Teledienstgesetz sind. Auch hier droht sonst das Schadensersatzrisiko.

### Aufgabe: Was ist zu tun?

Die einfachste Methode, alle Risiken mit einem Schlag loszuwerden, ist sicher die Fremdvergabe des WLAN-Zugangs an einen der großen Provider, wie zum Beispiel T-Mobile. Der gravierende Nachteil ist aber, dass dann für den Gast nicht unerhebliche Kosten für die Internetnutzung entstehen. Das macht natürlich das Hotel unattraktiver. Viele Hotels mit kostenlosem WLAN verzeichnen einen erhöhten Stammgästeanteil.

Die Einrichtung eines exklusiven Internetanschlusses nur für Gäste ist die wichtigste aller Maßnahmen, weil dadurch alle Internetaktivitäten der Gäste von denen des Hotels getrennt werden. Wenn das Hotel selbst für die Internetnutzung einen anderen Anschluß

benutzt, und das bereits im Vorfeld schriftlich dokumentiert, können fast alle Risiken entschärft werden. Im Falle einer Ermittlung ist die gesamte hoteleigene Ausrüstung dadurch nicht betroffen. Alle Beschuldigungen können nicht mehr direkt dem Hotel oder seinem Personal angelastet werden, sondern es ist klar, dass nur ein Gast den Verstoß begangen haben kann. In vielen Fällen ist dazu nicht einmal ein separater DSL-Anschluss notwendig, zum Beispiel bietet HostEurope eine Internetflatrate unter 7 Euro monatlich an, die problemlos gleichzeitig zum selbst genutzten Zugang mit dem gleichen DSL-Anschluss betreibbar ist.

Von einem Anwalt erstellte Nutzungsbedingungen in deutsch und englisch müssen nachweisbar durch den Gast anerkannt werden. Dadurch sind viele Risiken ausgeschlossen oder werden sehr stark abgemildert. Der Gast kann nicht Schadenersatz für Virenbefall, Ausspähung oder Fehlinformationen aus dem Internet oder Intranet einfordern, weil er umfassend darüber informiert wurde, dass er selbst mit geeigneten Mitteln für Schutz sorgen muss. Auch wird er über die gesetzlich notwendige Aufzeichnung des Internetzugangs informiert, was sicher einen hohen Abschreckungseffekt hat. Den größten Nutzen haben alle Massnahmen dann, wenn überhaupt keine Rechtsverstöße getätigt werden.

Durch Einsatz eines "Captive Portal" zur Zugangskontrolle anstatt der Verschlüsselung ergeben sich viele Vorteile. Im Gegensatz zur Verschlüsselung arbeitet dieses Verfahren mit einer Anmeldeseite, die den kompletten Zugang zum Internet solange sperrt, bis der Gast die auf der Seite angezeigten Nutzungsbedingungen akzeptiert hat, und sich angemeldet hat. Danach ist der Zugriff auf das Internet für den Gast offen. Diese Technik hat auch organisatorische Vorteile weil die komplizierte Verschlüsselung entfällt. Diese ist oft genug auch inkompatibel mit dem Gerät des Gastes oder sogar selbst unsicher. So ist zum Beispiel die oft angewandte, weil mit vielen Geräten kompatible, WEP-Verschlüsselung seit vielen Jahren bereits mit einfachen Mitteln zu umgehen. Wird diese Umgehung dann sogar von Aussenstehenden benutzt, sind dem nicht kontrollierbaren Missbrauch Tür und Tor geöffnet. Auch wird beim Einsatz eines „Captive Portals“ keine schriftliche Nutzungsbedingung benötigt, weil diese automatisch auf der Anmeldeseite akzeptiert werden muss. Solche System sind auch als lizenzfreie OpenSource-Lösungen unter Linux verfügbar.

Durch den Betrieb der Vorratsdatenspeicherung mit sechsmonatiger Speicherung der in § 113a TKG geforderten Angaben interne IP-Adresse, Anschlusskennung und Beginn und Ende der Nutzung erfüllt man die gesetzlichen Anforderungen. Die Gefahr eines Bußgeld ist nicht mehr gegeben. Realisieren lässt sich das mit einem zentralen Radius-Dienst. Das hat aber den Nachteil, dass dann das Funktionieren des WLAN von einem zusätzlichen Dienst im Internet abhängig ist, der zudem nicht immer kostenlos ist. Die Firma Lancom Systems hat dazu auch ein fundiertes White-Paper erstellt, dass auch noch einmal detailliert auf die gesamte Problematik einght.

Durch individuelle Zugangskennungen für jedes Zimmer fühlt sich der Gast nicht mehr anonym und

wird wesentlich zurückhaltender beim Nutzen von fragwürdigen Angeboten. Auch hier ist der große Vorteil die Verhinderung des Rechtsverstoßes. Das Zimmer als Zugangskennung ist für Hotels ideal geeignet, weil die namentliche Anmeldepflicht leicht eine direkte Zuordnung zur Person ermöglicht.

Leider ist das 100%-ige Blocken von Filesharing nicht möglich, aber es gibt durchaus sehr gute Lösungen, die die Nutzung der illegalen Tauschbörsen sehr erschwert ohne andere Internetdienste zu blockieren. Die Installation eines solchen Filters ist sehr ratsam, weil so der größte Risikoteil eliminiert wird. Zum Beispiel IPP2P blockiert eDonkey, eMule, Kademia, KaZaA, FastTrack, Gnutella, Direct Connect, BitTorrent, extended BT, AppleJuice, WinMX, SoulSeek, Ares und AresLite mit sehr guten Erkennungsraten.

### Angebot: Wir helfen

Individuelle Beratung - 80 Euro (\*1) Jedes Netzwerk ist individuell. Vom Internet-Provider bis zum WLAN-Aufbau. Welche von den Massnahmen im Einzelfall notwendig und sinnvoll sind, und wie sie technisch umgesetzt werden sollten, muss geplant werden. Als Ergebnis gibt es einen Vorschlag, wie mit oder ohne fremde Hilfe vorgegangen werden sollte.

Wir liefern ein vorinstalliertes „Captive Portal“ mit Installation ab 400 Euro plus Fahrtkosten - je nach Größe des Hotels. Darin beinhaltet ist eine anwaltlich ausgearbeitete Anmeldeseite in deutsch und englisch.

Passend zu unserem „Captive Portal“ können wir wöchentlich automatisch Individualpasswörter für jedes Zimmer generieren und einstellen, sowie die tägliche Vorratsdatenspeicherung übernehmen - ab 10 Euro/Monat - je nach Zimmeranzahl. Dabei arbeitet das System offline, der Internetzugang ist unabhängig von der zentralen Erfassungsstelle. Das „Captive Portal“ speichert die Daten bis zu 48 Stunden selbst. Der IPP2P-Filter ist auch integriert. In den Quelleangaben ist ein Beispiel für das tägliche Zugriffprotokoll.

Mit dieser Lösung bleibt die Internetnutzung für den Gast kostenlos, trotz sehr geringer zusätzlicher Kosten für den Betrieb. Unser Portal mit dem Passwort/Vorratsdatenspeicherdienst deckt alle Aspekte ab, die unter dem Punkt "Was ist zu tun?" angesprochen wurden.

### Kontakt:

SchimonSoft&Coach (SSC)  
Dr.-Dietlein-Strasse 16 - 95028 Hof Saale  
Telefon: ++49 (0) 9281 50 96 76  
Email: uwe@schimon.de  
Bearbeitungsstand: 23.08.08



### Quellen und weitere Informationen zum Thema:

unsere Website: <http://hotel.wpack.de/>  
Protokoll: <http://hotel.wpack.de/assets/pdfs/daily.pdf>  
lpp2p: <http://www.ipp2p.org/>  
Whitepaper: [http://hotel.wpack.de/assets/pdfs/TP\\_Public\\_Spot\\_Legal-Notice-DE.pdf](http://hotel.wpack.de/assets/pdfs/TP_Public_Spot_Legal-Notice-DE.pdf)  
Lancom-Systems: <http://www.lancom-systems.de/>  
OpenSource-Lösungen: <http://nocat.net/>  
Captive Portal: [http://en.wikipedia.org/wiki/Captive\\_portal](http://en.wikipedia.org/wiki/Captive_portal)  
HostEurope: <http://www.hosteurope.de/produkte/DSL-VoIP-DSL-Flatrate>  
Branchenbericht: <http://hotel.wpack.de/assets/pdfs/betreiber-offener-wlans.pdf>  
Gastgewerbe 05/2008: <http://hotel.wpack.de/assets/pdfs/kribo.pdf>  
Diskussion: <http://www.medien-gerecht.de/2008/01/05/betreiber-offener-wlans-muessen-vorratsdaten-speichern/>  
Dr. Gerrit Hornung von der Universität Kassel: [http://hotel.wpack.de/pdfs/2007\\_12\\_mmr\\_hornung.pdf](http://hotel.wpack.de/pdfs/2007_12_mmr_hornung.pdf)  
§ 113a TKG: <http://www.dejure.org/gesetze/TKG/113a.html>  
IT-Rechtsleitfaden der Kanzlei esb in Stuttgart: [http://hotel.wpack.de/assets/pdfs/whitepaper\\_legal\\_guide\\_de.pdf](http://hotel.wpack.de/assets/pdfs/whitepaper_legal_guide_de.pdf)