White Paper

Datenschutz für den Betrieb von WLAN-Hotspots
Die VPN-Routing-Lösung von HOTSPLOTS

Stand: März 2010

hotsplots GmbH
Dr. Ulrich Meier, Dr. Jörg Ontrup
Rotherstr. 17
10245 Berlin
E-Mail: info@hotsplots.de
Tel.: +49 (0)30 29 77 348 0

1. Auch unterwegs online

Drahtlose Zugangspunkte zum Internet, so genannte WLAN-Hotspots, sind eine günstige und mittlerweile weit verbreitete Lösung, um auch unterwegs Zugriff aufs Internet zu erhalten. Vor zehn Jahren war „mobiles Internet“ via Laptop oder PDA sehr teuer und fast ausschließlich in großen Ballungszentren verfügbar. Seitdem hat sich die WLAN-Technik stark weiterentwickelt und ist mittlerweile auch entsprechend verbreitet. So kommen heute Urlauber oder Geschäftsreisende vielerorts zu erschwinglichen Preisen mobil ins Internet. Laut BITKOM gab es im September 2008 rund 14.200 WLAN-Hotspots[1] in Deutschland. Seitdem hat sich zumindest die Anzahl der Standorte von HOTSPLOTS mehr als verdoppelt - bis Anfang 2010 auf rund 1000.

WLAN-Hotspots als öffentlicher Weg ins Internet

Neben der privaten hat auch die kommerzielle Nutzung von WLAN-Hotspots zu deren steigender Verbreitung in den letzten Jahren beigetragen. Verschiedene Systeme zur Abrechnung und Zugangskontrolle ermöglichen Bezahlen sowie sicheres Login. Das Einloggen erfolgt dabei zumeist via Webbrowser. Nach der Eingabe der Zugangsdaten wird dann der Zugriff auf das Internet freigegeben. Die Abrechnung erfolgt danach – in der Regel ohne großen Aufwand für Betreiber oder Nutzer – über das externe Abrechnungssystem des jeweiligen Anbieters.

2. Risiko: Ermittlungen führen zum Hotspot-Betreiber

Die rasante Verbreitung der WLAN-Technologie an Flughäfen, in Hotels und Cafés oder auf Campingplätzen birgt jedoch Risiken. Nicht nur die Internetnutzer, sondern auch die Hotspot-Betreiber sorgen sich um den Schutz ihrer Daten und Privatsphäre. Eine der immer wieder von Ihnen geäußerten Ängste lautet: „Steht die Polizei vor meiner Tür, wenn ein Internetnutzer meinen Hotspot zu illegalen Zwecken missbraucht?“.

Ganz abwegig ist das nicht. Auch wenn Hausdurchsuchungen und die Beschlagnahmung von Hardware immer noch die Ausnahme sind: Im Falle eines Missbrauchs, zum Beispiel eines unberechtigten Dateitransfers, ermittelt die Polizei zuerst beim Hotspot-Betreiber – unabhängig davon, ob er etwas damit zu tun hat oder nicht. Denn seine eindeutig zuordenbare Hotspot-IP-Adresse ist im Datenverkehr stets erkennbar. Wird diese Absenderkennung vom Internet-Provider gespeichert, können Ermittler sie mit einer Person verknüpfen – und das führt sie dann direkt zum Betreiber des WLAN-Hotspots.

Jederzeit identifizierbar

Im Normalfall besteht zwischen dem WLAN-Hotspot und dem Internet eine direkte Verbindung. Der Nachteil ist die Identifizierbarkeit der Hotspot-IP-Adresse in der Öffentlichkeit. Problematisch kann das werden, sobald ein Internetnutzer den öffentlichen Zugangspunkt beispielsweise zum illegalen Herunterladen von Musik- oder Videodateien benutzt. Denn in diesem Fall ist es nicht die Nutzer-IP-Adresse, die im Datenverkehr übermittelt

[1] BITKOM Presseinfo 14.09.2008: http://www.bitkom.org/files/documents/BITKOM_Presseinfo_WLAN_14_09_2008.pdf

wird, sondern die des Hotspots. Ist hier keine Authentifizierung notwendig, hinterlässt der Internetnutzer keinerlei Spuren – die Polizei kann sich dann nur an den Hotspot-Betreiber wenden.

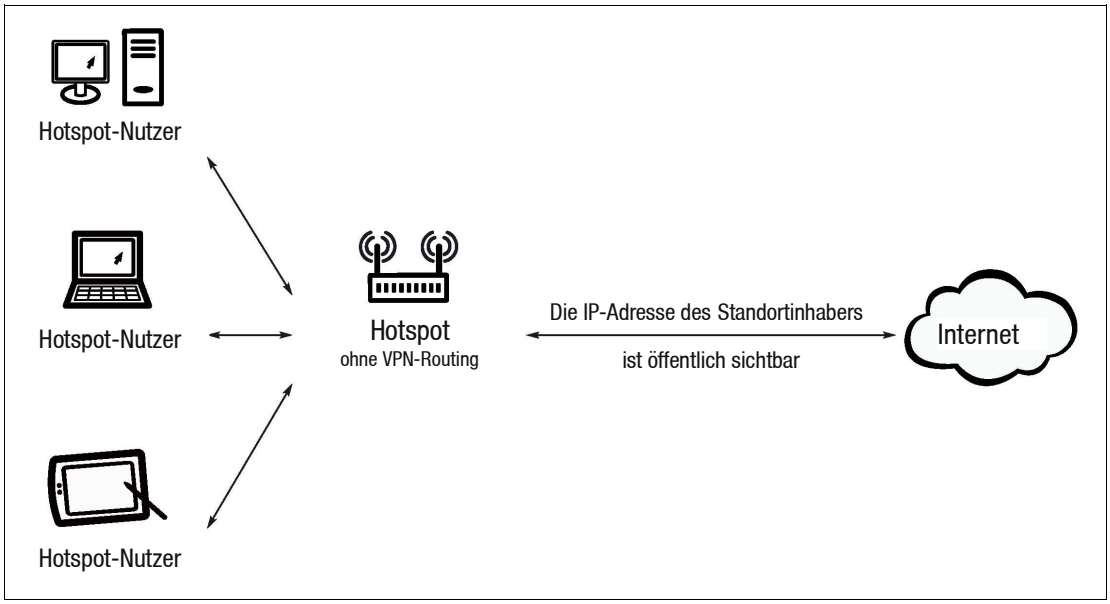

Abbildung 1: Funktionsdiagramm eines Hotspots ohne VPN-Routing

Warum aber die Ermittlungsbehörden erst zum Hotspot-Betreiber schicken? In der Regel kann dieser auch nicht weiterhelfen, denn normalerweise übernimmt ein externer Dienstleister die Zugangskontrolle und Abrechnung. Sinnvoller wäre es, die Polizei direkt zu dem Anbieter des Abrechnungssystems bzw. dem Internet Service Provider zu leiten – wenn es ermittlungsrelevante Daten gibt, dann sind sie dort zu finden.

3. Mehr Privatsphäre durch die VPN-Server von HOTSPLOTS

Die hotsplots GmbH hat eine Lösung entwickelt, die die Identität des Hotspot-Betreibers im Internet besser schützt und unnötige Besuche von Strafverfolgern vermeidet. Auf Wunsch sorgen so genannte „Virtuelle Private Netzwerke“ (VPNs) dafür, dass die Betreiber von WLAN-Hotspots im öffentlichen Datenverkehr nicht mehr zu identifizieren sind. Stattdessen werden Ermittler direkt zu HOTSPLOTS geleitet.

4. Die Funktion des VPN-Routings von HOTSPLOTS

Normalerweise hat jeder Hotspot eine direkte Verbindung zum Internet und ist dort durch seine IP-Adresse eindeutig identifizierbar. Anders sieht es aus, wenn sich der Hotspot-Betreiber für den Einsatz von VPN-Routing entscheidet. Hier wird nämlich der gesamte Hotspot-Datenverkehr zuerst über Server von HOTSPLOTS geleitet. Der Hintergrund: Durch das Tunneln der Verbindung zum Internet wird die Hotspot-IP-Adresse durch eine Kennung des VPN-Servers im Rechenzentrum ersetzt. Damit erhalten alle Hotspots, deren Datenverkehr über VPN-Server umgeleitet wird, eine andere IP-Adresse – der Hotspot-Betreiber bleibt anonym.

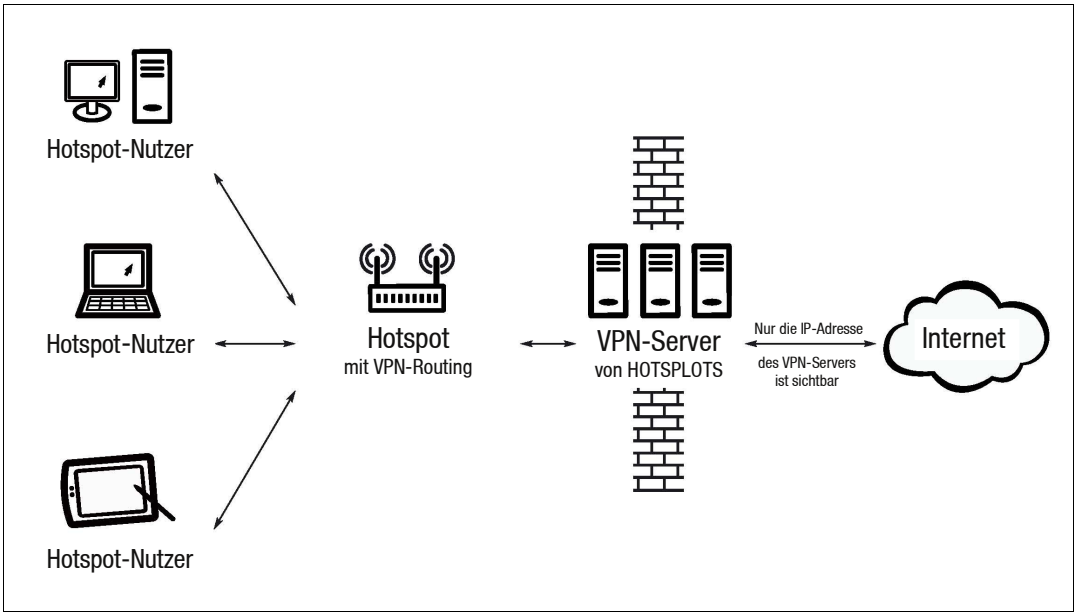

Abbildung 2: Funktionsdiagramm eines Hotspots mit VPN-Routing

Die hotsplots GmbH setzt auf ein System, das den Hotspots dynamisch VPN-Server zuweist. Durch diese Lastverteilung (engl. load balancing) stehen für jeden Hotspot genügend Ressourcen zur Verfügung. Auf Seite des Hotspots kann die Geschwindigkeit durch die Rechenleistung des Hotspot-Routers limitiert sein. Die schnellsten Geräte, HOTSPLOTS Appliances, beherrschen die Lastverteilung auf mehrere parallele Internetanschlüsse und mehrere VPN-Server, so dass auch Geschwindigkeiten von mehr als 100 MBit/s problemlos zu bewältigen sind.

All jene, für die höchster Datendurchsatz und schnellste Reaktionszeiten entscheidend sind und die auf VPN-Routing verzichten können, können ihren Hotspot mit HOTSPLOTS auch ohne VPN-Routing betreiben, denn das Angebot ist optional und kostenfrei. Beim Einsatz von HOTSPLOTS DSL als Internetanschluss werden Ermittlungsbehörden auch ohne VPN-Routing direkt zu HOTSPLOTS geleitet.

5. Das VPN-Routing von HOTSPLOTS aus der Sicht der Hotspot-Betreiber

Entscheidet sich der Hotspot-Betreiber für die Option „VPN-Routing“, sorgt er damit vermeidbaren Behördenkontakten vor. Niemand, der einen privaten oder gewerblichen WLAN-Hotspot betreibt, möchte schließlich die Polizei im Haus haben. Hausdurchsuchungen und Beschlagnahmungen vor den Augen der Nachbarn oder Kunden – das kann einen großen Imageschaden bedeuten, auch wenn der Betreiber letztlich völlig unschuldig ist, da sein Hotspot von einem Nutzer beispielsweise zum Transfer rechtlich geschützter Dateien missbraucht wurde. Mit dem Einsatz von VPN-Servern lässt sich ein solches Szenario ohne großen Aufwand vermeiden.

Die Behörden werden so direkt zu HOTSPLOTS geleitet, ohne dass der Hotspot-Betreiber involviert wird. Dort erhalten die Ermittler dann die Informationen, die für die Aufklärung nötig und im Rahmen der gesetzlichen Vor-

gaben gespeichert sind. An der Funktion und Konfiguration des WLAN-Hotspots ändert sich nichts, sodass Hotspot-Betreiber und -Nutzer den Einsatz der VPN-Server kaum wahrnehmen.

Abbildung 3: Einfaches Aktivieren des VPN-Routing per Mausklick im Webinterface

Das Aktivieren des VPN-Routings erfolgt einfach per Mausklick. Die VPN-Konfiguration wird vollautomatisch vom zentralen Server von HOTSPLOTS geladen.