Öffentliches WLAN in Deutschland

Zwischen dem technisch Machbaren und den gesetzlichen Vorschriften

Kai-Oliver Detken

Deutschland hinkt gegenüber anderen Ländern beträchtlich in der Nutzung öffentlicher WLAN-Hotspots hinterher. Während man z.B. in Dublin bereits in jedem einfachen Bus einen kostenlosen WLAN-Zugang bekommt, sind in Deutschland nur teure Hotspots in Hotels oder öffentlichen Bereichen anwählbar. Freie Hotspots wurden aufgrund der gesetzlichen Bestimmungen von einigen Betreibern (z.B. kleineren Cafés) wieder eingestellt.
Dabei kann die Hotspot-Umsetzung eigentlich so einfach sein. Trotzdem gibt es in Deutschland relativ wenige Angebote. Warum ist das so? Gibt es eine Lösung aus diesem Fortschrittshemmnis? Oder wird Deutschland weiter hinter der aktuellen Entwicklung hinterherlaufen?

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Dabei macht es die Deutsche Telekom mit ihrem Produkt HotSpots vor, wie man als Provider WLAN-Zugänge ausrollen bzw. anbieten kann. Der Dienst wird an über 1 Mio. Standorten in Deutschland in Hotels und Cafés, auf Flughäfen und Bahnhöfen nicht nur Telekom-Kunden angeboten. Inzwischen kann dieses Angebot auch in ausgewählten Zügen der Deutschen Bahn oder auf einigen Flügen der Lufthansa genutzt werden. Ist man bereits Mobilfunk- oder Internetkunde der Telekom, ist eine Flatrate meistens bereits inklusive. Nur sollte man dann sein Passwort zur Hand haben. Ein Hot-Spot-Pass kann ebenfalls für Nicht-Telekom-Kunden gebucht werden. Die Abrechnung erfolgt über die normale Mobilfunkrechnung der Telekom oder direkt am Hotspot per Kreditkarte.

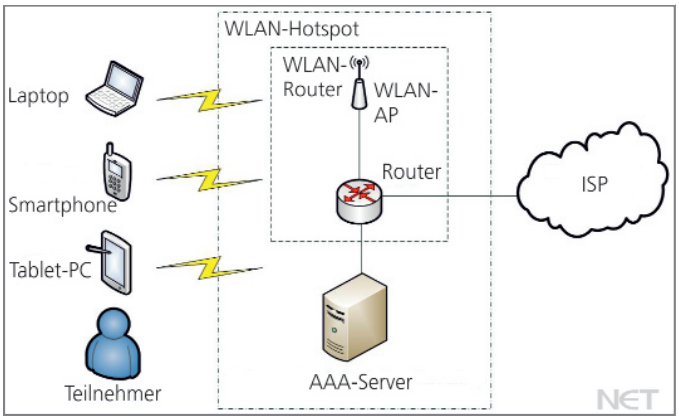

Bild 1: Infrastruktur eines WLAN-Hotspot (AP – Access Point, ISP – Internet Service Provider, AAA – Authentication, Authorization, Accounting)

Technische Realisierung

Ein WLAN-Hotspot ist eine technische Einrichtung, die ein Access oder Internet Service Provider (ISP) beliebigen Teilnehmern anbietet, um per WLAN einen Zugang zum Internet bereitzustellen. Die Infrastruktur besteht dabei aus einem WLAN-Router, der den Zugang zu dem Funknetz bereithält sowie eine Breitbandverbindung zum ISP unterhält (*Bild 1*). Über den ISP kann dann der Hotspot-Teilnehmer direkt auf das Internet zugreifen.
Zur Authentifizierung des Teilnehmers und für die Abrechnung des Dienstes steht innerhalb des Hotspot auch ein AAA-Server zur Verfügung. Er ist natürlich besonders dann notwendig, wenn der Access Provider auch seinen Hotspot-Dienst kostenpflichtig anbieten möchte. Viele Hotels und Cafés im Ausland bieten z.B. einen WLAN-Zugang u.a. auch als Kundenbindungsinstrument kostenlos an. In diesem Fall entfällt ein solcher Server.
Überregionale Access Provider wie die Deutsche Telekom besitzen eine Hotspot-Infrastruktur, die nicht nur für einen Single-Hotspot ausgelegt ist. Hier übernimmt ein zentraler AAA-Server die Aufgaben für alle regionalen Hotspots. Alle Hotspots werden dabei an das eigene Netz angeschlossen und einheitlich bez. des AAA-Dienstes behandelt. Der Teilnehmer kann so den gleichen Zugang an unterschiedlichen Orten nutzen.
Nachdem der Teilnehmer sich authentifiziert hat, wird ihm der Zugang zum Internet freigeschaltet. Die Abrechnung erfolgt nicht lokal, sondern zentral an einer Stelle und kann damit zeit- oder volumenbasiert monatlich abgerechnet werden. Allerdings ist man darauf angewiesen, Kunde des Access Providers zu sein.
Öffentliche Hotspots sind heute in Ballungsgebieten so gut wie überall zu finden. Sie gehören in Hotels und Restaurants, auf Bahnhöfen und Flughäfen zum Alltag. Für den Anwender ist dies ein großer Vorteil, kann er

doch diesen alternativen Zugang zum Internet fast überall unterwegs nutzen, ohne das mobile Datenvolumen seines Mobilfunkvertrags zu belasten. Allerdings bietet auch jeder Access Provider ein anderes Abrechnungsverfahren an, was alles andere als anwenderfreundlich ist. So dauert es mitunter sehr lange, bis man einen Zugang zum Internet herstellen kann. Neben den Kosten schreckt auch die Bekanntgabe zu vieler Informationen vor der Aktivierung eines Zugangs ab. Hier fehlt eine zentrale Abrechnungsmöglichkeit, unabhängig vom Access Provider, die für beliebige Hotspots gilt. Als Basis könnte ein Account dienen, der über die Handy-, Telefon- oder Internetrechnung bezahlt wird. Dazu müsste allerdings ein übergreifendes Roaming und Billing zwischen den verschiedenen Anbietern etabliert werden.

Wie dies umgesetzt werden könnte, zeigt *Bild 2*. Hier wird eine zentrale unabhängige WISP-Instanz (Wireless Internet Service Provider) geschaffen, die nur für das Billing und Accounting zuständig ist. Ein Teilnehmer hat dementsprechend nur noch einen Account bei dieser WISP-Plattform und kann sich mit seinen Anmeldedaten (Credentials) bei lokalen ISPs anmelden. Der jeweilige WLAN-Hotspot meldet die Anmeldung an die WISP-Plattform, wo die Daten überprüft und der Teilnehmer freigeschaltet wird. Abhängig vom Abrechnungsverfahren des Access Providers wird vom WLAN-Hotspot das Datenvolumen oder die Verbindungszeit an die Plattform weitergeleitet. Der WISP-Provider muss nun mit dem jeweiligen ISP regelmäßig abrechnen, der Teilnehmer muss sich nicht kümmern.

Perfekt umgesetzt ist dieses Roaming von WLAN-Zugängen bei dem Hochschulnetz Eduroam (Education Roaming). Diese Initiative hat zum Ziel, dass Mitarbeiter und Studenten von teilnehmenden Hochschulen weltweit einen einheitlichen Internetzugang erhalten. Mithilfe des eigenen Benutzernamens und Passworts wird ein Hotspot-Zugang geschaffenn, der an einer deutschen Hochschule genauso gut funktioniert wie an einer ausländischen. Heute sind fast alle europäischen Länder bei Eduroam vertreten. Viele Unterstützer lassen sich auch im asiatisch-pazifischen Raum, in Nord- und Südamerika und im afrikanisch-arabischen Raum finden (*Bild 3*). So ist es sehr angenehm, wenn man in einem anderen Land, in einer fremden Institution das dortige WLAN mit seinen bekannten Zugangsdaten aus dem Heimatnetz nutzen kann.

Jede Institution stellt dabei ihre eigene WLAN-Infrastruktur zur Verfügung. Die Authentifizierung erfolgt durch die jeweilige Heimorganisation des Benutzers über das Radius-Protokoll. Dabei stellt Terena als Gründer und Besitzer der Eduroam-Marke den Root-Server, während die teilnehmenden Institutionen der kooperierenden Länder den Server mit der eigentlichen Benutzerkennung stellen. Der Serververbund bildet dadurch eine hierarchische Baumstruktur, ähnlich dem DNS-Dienst (Domain Name System), die weltweit Gültigkeit besitzt. Ein weiterer Vorteil: Die Benutzerkennung ver-

lässt nicht das Heimatnetz, wodurch diese Information nicht in fremde Hände gelangt. Zusätzlich wird als lokale Zugangsauthentifizierungstechnik immer das Protokoll IEEE 802.1X verwendet. So ist gewährleistet, dass die Credentials auf dem Weg zur Heimatorganisation verschlüsselt werden. Die Sicherheitsüberprüfung findet dabei am Gerät des Teilnehmers statt. Es liegt also in der eigenen Verantwortung, ob die Vertraulichkeit des eigenen Logins sichergestellt ist.

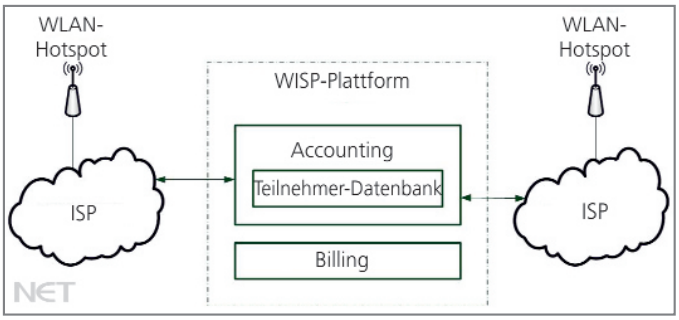

Bild 2: Zentrale WISP-Infrastruktur für gemeinsames Accounting/Billing
WISP – Wireless Internet Service Provider

Gesetzlicher Hemmschuh

Ein Grund für den bisherigen geringen Ausbau der öffentlichen WLAN-Hotspots in Deutschland liegt darin begründet, dass eine unklare Rechtslage bez. der Haftungsrisiken existierte. So kann bei krimineller Nutzung des WLAN durch einen Teilnehmer der Anbieter angeklagt werden und nicht der eigentliche Störer des Rechtsraums. Deshalb verzichteten kleinere Cafés und Hotels oftmals auf ein WLAN-Angebot, auch wenn sie dadurch einen klaren Wettbewerbsnachteil zu verzeichnen hatten. Zusätzlich schrecken Sicherheitsbedenken von der WLAN-Nutzung ab. Daher hinkt Deutschland im internationalen Vergleich stark hinterher: 1,87 Hotspots entfallen hierzulande auf 10.000 Einwohner im Gegensatz zu z.B. Schweden mit 9,94 und Südkorea mit 37,35 Hotspots. Dabei besitzen die Deutschen im weltweiten Vergleich die meisten WLAN-fähigen Geräte und nutzen diese Technik auch ausgiebig zu Hause.

Am 2. Juni 2016 hat deshalb der Bundestag den Gesetzentwurf zur Änderung des Telemediengesetzes (TMG) in einem Entschließungsantrag verabschiedet. Wie von der Bundesregierung vorgeschlagen, wird nun spezifiziert, dass der in § 8 Abs. 1 TMG geregelte Haftungsausschluss von Access Providern auch für WLAN-Betreiber gilt. Das bedeutet, dass jemand, der sein WLAN für andere Teilnehmer zur Nutzung freigibt, den gleichen Haftungsprivilegien unterliegt wie beispielsweise die Deutsche Telekom. Zudem gilt die Regelung für alle gleichermaßen, es gibt also keine Unterscheidung zwischen großen oder kleinen, gewerblichen oder privaten Anbietern. Das Gesetz trat am 27. Juli 2016 endgültig in Kraft, nachdem auch der Bundesrat dem Gesetzentwurf zugestimmt hatte.

Trotz der Verbesserung gibt es Kritik an der Regelung, sie geht einigen Providern nicht weit genug. So ist z.B. in dem neuen Gesetz davon die Rede, dass der entsprechende Provider „zumutbare Maßnahmen zur Verhinderung von Rechtsverletzung durch angemessene Sicherheitsmaßnahmen durch anerkannte Verschlüsselungsverfahren ergreifen soll" (§ 8 Abs. 4 Satz 2 Nr. 1 TMG-E). Der Einsatz eines Verschlüsselungsverfahrens setzt aber voraus, dass der Hotspot-Anbieter dem Nutzer einen Schlüssel überlässt, wodurch die Nutzung des Hotspot diverse Zwischenschritte bei der ersten Anmeldung beinhaltet. Durch diese Hürde werden viele potenzielle Nutzer dieses WLAN-Angebot meiden. Zusätzlich bedeutet die Bereitstellung von Schlüsseln einen nicht zu unterschätzenden Aufwand für einen Access Provider, zumal der mit zusätzlichen Kosten verbunden ist.

Hinzu kommt, dass eine Verschlüsselung zwischen Endteilnehmer und Provider nicht ausschließt, dass eine Rechtsverletzung vorgenommen werden kann. Ein Teilnehmer kann z.B. urheberrechtlich geschütztes Material genauso über eine verschlüsselte Verbindung herunterladen bzw. oder einen Hacking-Versuch vornehmen wie über eine unverschlüsselte Verbindung. Auch wird nicht definiert, was „zumutbare Maßnahmen" sind.

Rechtsverletzungen lassen sich letztendlich viel besser durch geeignete Filter und Portsperren realisieren. Immer häufiger werden daher bestimmte Ports durch Provider abgeschaltet bzw. verboten. Dadurch können nach dem Blacklist-Prinzip unerwünschte Webseiten oder Internetdienste gesperrt oder zumindest stark eingeschränkt werden. Allerdings geht dies auch oftmals mit Unannehmlichkeiten für den Teilnehmer einher, da ein beruflicher Nutzer auf jeden Fall einen sicheren Zugang zu seinem Unternehmensnetz herstellen möchte. Funktioniert dies nicht, weil beispielsweise die relevanten Ports für die VPN-Verbindung geblockt werden, ist der WLAN-Zugang für ihn uninteressant. Hier muss ein Kompromiss zwischen Sicherheit und notwendiger Dienstnutzung gefunden werden.

Dieses Dilemma könnte man damit lösen, indem die kostenpflichtige Nutzung für VPN-Daten freigeschaltet wird, während die kostenfreie Nutzung eingeschränkten Internetverkehr anbietet. Für einen eingeschränkten Internetzugang wird ein Teilnehmer jedenfalls kein Geld ausgeben, weshalb dieses Geschäftsmodell letztendlich vom Aussterben bedroht ist. Denn es ist heute bereits kaum einzusehen, dass man im Ausland kostenfreie WLAN-Hotspots ohne Limitierung nutzen kann, während man in Deutschland oft horrende Summen ausgeben darf. Grundsätzlich muss aber auch noch einmal beim Telemediengesetz dringend nachgebessert werden.

Fazit

Der Entwurf des zweiten Gesetzes zur Änderung des Telemediengesetzes liest sich auf den ersten Blick in der Tat so, als wollte die Bundesregierung die Störerhaftung für WLAN-Betreiber abschaffen. Die Regelung des Paragraphen § 8 TMG, wonach Access Provider für die Handlungen ihrer Nutzer verantwortlich sind, sollen nun auch für die Anbieter drahtloser lokaler

Netze gelten. Dabei wird aber leider nicht zwischen privaten und gewerblichen Anbietern unterschieden. Zudem ist unklar, was unter „zumutbaren Maßnahmen" verstanden wird, um ein WLAN ausreichend abzusichern. Die Entscheidung, ob ein Access Provider bei unsachgemäßer Nutzung eines Hotspot durch einen Teilnehmer in Mithaftung genommen wird, obliegt daher nach wie vor dem zuständigen Gericht. Es ist also weiterhin eine Rechtsunsicherheit vorhanden und es kann von keinem Nachlassen der Abmahnwelle ausgegangen werden.

Dies wird sich auch durch die europäische Entscheidung des EuGH vom 15. September nicht grundlegend ändern. Zwar gibt es nun eine Regelung, die keinen Anspruch auf Schadensersatz gegen WLAN-Betreiber wegen Urheberrechtsverstößen definiert. Allerdings wird auch vorgeschrieben, dass der WLAN-Betreiber sein Netz absichern muss (mindestens durch ein Passwort oder eine Verschlüsselung). Der Verschlüsselungs- und Identitätszwang wird der Entwicklung offener Netze weiter entgegenwirken und eine andere Abmahnwelle zur Unterlassungsanordnung nach sich ziehen. Für den WLAN-Betreiber ändert sich deshalb erst einmal wenig. Deshalb müsste nun die deutsche Regierung wieder nachziehen und klarstellen, dass nach deutschem Recht keine Verschlüsselungspflicht, kein Identitätszwang und keine Unterlassungsansprüche gegen WLAN-Betreiber bestehen.

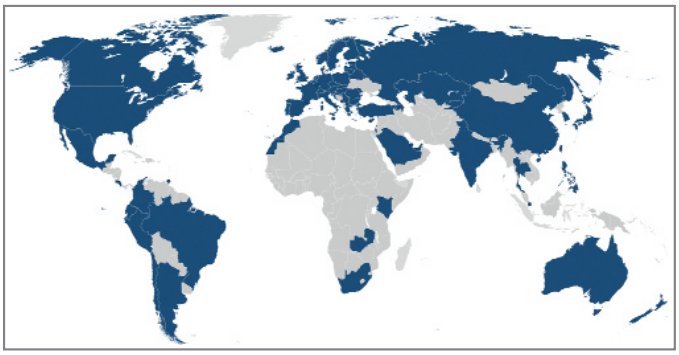

Bild 3: Weltweite Verteilung von Eduroam (Quelle: https://www.i-med.ac.at/itservices/systeme/eduroam/)

Allerdings verfolgen die Access Provider in Deutschland meistens ein anderes Geschäftsmodell als ihre ausländischen Kollegen, da man hier den Hotspot-Dienst meistens kostenpflichtig anbietet. Dieses Modell hat solange noch seine Daseinsberechtigung, bis der rechtsfreie Raum von der Bundesregierung nicht geschlossen wird. Bis dahin werden sich kleine lokale Anbieter mit einem freien WLAN-Dienst zurückhalten. Sobald aber das Anbieten freier WLAN-Hotspots in Deutschland ermöglicht wird, werden neue kostenlose WLAN-Zugänge wie Pilze aus dem Boden schießen. Dann können die Access Provider, die kostenpflichtige Hotspots anbieten, nur noch durch verbesserte Performance oder Roaming-Angebote überzeugen. Ob dies ausreichen wird? *(bk)*