Information

Nr. 41
Okt 2014

INGENIEURBÜRO MEHNERT
Netzwerktechnik - Prozessleittechnik

Sichere WLAN - Hotspots für Internet-„Gastzugriff“

Gefahren, Rechtliche Grundlagen und: Die Lösung

Vorwort

In vielen Hotels, Bars, Bahnhöfen usw. kann mit einem Notebook, Handy oder Tablet-PC über das Funknetzwerk (Wireless LAN oder WLAN Hotspot) auf das Internet zugegriffen werden - ein toller und kundenfreundlicher Service.
Doch vielen Anbietern solcher „Hotspots“ ist es gar nicht bewußt, daß Gäste dieses Angebot auch mißbrauchen könnten. In der Vergangenheit wurden Gastgeber von Geschädigten abgemahnt oder verklagt, weil Gäste über deren Internetzugang rechtswidrig handelten, z.B. durch unerlaubtes Filesharing.
In den meisten Fällen bekamen die Kläger recht.

Die aktuelle Rechtssprechung und deren Grundlagen

Im Zentrum steht hier der Begriff der Störerhaftung. Ein Störer ist jemand, der selbst nicht Täter ist, aber mit seinem Handeln dazu beiträgt, daß Rechtsverletzungen geschehen.
Bei Urheberrechtsverletzungen kann das zum Beispiel ein Forumsbetreiber sein, in dessen Forum Nutzer Links zu urheberrechtlich geschützten Dateien veröffentlichen. Auch wenn der Betreiber die Dateien nicht selbst hochgeladen hat, so stellt er doch die Plattform zur Verfügung, über die der Zugang gewährt wird. In diesem Sinne ist jemand, der ein WLAN-Netzwerk betreibt, ebenfalls dafür verantwortlich, was darüber geschieht.
Leider ist die Rechtslage sehr unsicher – es gibt keine eindeutigen gesetzlichen Regelungen in dem Bereich, sondern die einzelnen Fälle werden vor Gericht entschieden.
Das ist politisch so gewollt:

Die Bundesregierung hat in einer Stellungnahme erklärt, daß eine gesetzliche Haftungsbeschränkung nicht erforderlich ist. Sie sei durch die Rechtsprechung bereits auf klar umgrenzte Sachverhalte eingeschränkt.
Praktisch bedeutet das, daß Privatpersonen, die ein WLAN betreiben, aber auch Vereine oder Café-Besitzer, die WLAN für ihre Gäste anbieten wollen, in vielen Fällen rechtlich in Unsicherheit leben.

Deutsche Gerichte gelangten zu der Ansicht, Sie als Gastgeber sind verpflichtet, Ihren zur Verfügung gestellten Internetzugang (Hotspot) so zu schützen, daß unerlaubte Zugriffe von außen nicht möglich sind.
Ebenso müssen Sie den Zugang Ihrer Gäste zum Internet in der Form absichern, daß im Fall von rechtswidrigem Verhalten nachvollziehbar ist, wer dieses begangen hat.

Was kann rechtswidriges Verhalten im Internet durch einen Gast sein ?

- Illegales Herunterladen von Bilddateien, Musik und Filmen oder deren Veröffentlichung im Internet,
- Teilnahme an Tauschbörsen, dem so genannten Filesharing
- Besuch von Internetseiten, deren Inhalte strafrechtlich verfolgt werden (z.B. Kinderpornografie)
- Verbreitung von Inhalten, die gesetzeswidrig sind (z.B. Beleidigungen, Volksverhetzung)

Ausreden sind meist zwecklos und Unwissenheit schützt Sie nicht vor der Haftung !

Folgende Gerichtsurteile bestätigen dieses:

- LG Hamburg

Urteil vom 26. Juli 2006, Az: 308 O 407 / 06

- OLG Düsseldorf

Beschluß 27. Dezember 2007, Az: I-20 W 157/07

- OLG Frankfurt/Main

Beschluß 20. Dezember 2007, Az: 11 W 58/07

Allerdings muß man an dieser Stelle auch auf ein Urteil des BGH von 2010 (Az. I ZR 121/08 vom 12.5.2010) verweisen, was die vorhergehenden Aussagen weitgehend relativiert und die Störerhaftung bei ordnungsgemäß installierten und gesicherten Hotspots für den Betreiber (als Access-Provider) auf wenige Ausnahmen reduziert.

Die Lösung

Im Rahmen des Projektes bestand die Aufgabe darin, einen für Kunden frei (ohne Anmeldung) zu nutzenden Hotspot in eine bestehende EDV-Anlage zu integrieren.

Im beschriebenen Projekt (Bild 1) werden die Windows-Server (Datenbank, Webset) und der Linux-Server für gesicherten Clientinternetzugang (Opac) über einen Internetfilter unter VMWare als virtuelle Maschinen betrieben, was die Möglichkeit eröffnete, eine weitere Gateway für den ausschließlichen Hotspotzugang zu installieren.

Eine gleichzeitige Nutzung des Linux-Internetfilters (Content Filter) für Hotspots scheitert an der zunehmenden Zahl von verschlüsselten https-Anfragen, die durch den Proxy (squid) nur über eine „man in the middle“ – Funktion durch Verwendung eigener Zertifikate gelesen und beantwortet werden könnte, was rechtlich höchst bedenklich wäre.

Die Filtersoftware ist zum großen Teil vorkonfiguriert und besitzt für individuelle Anpassungen ein sehr benutzerfreundliches, gut strukturiertes Web-Interface für die Filterkonfiguration (Bild 2), das nach der Inbetriebnahme natürlich auch für die Fernwartung genutzt werden kann.

Steht kein Server mit VMWare oder MS HyperV für die Visualisierung zur Verfügung kann die Filtersoftware auf einem handelsüblichen PC, Mini-PC o.ä. installiert werden, wobei keine besonderen Anforderungen an Speichergröße, Plattenplatz oder Grafik gestellt werden.

Für den Anwender bedeutet dies, daß ein Hotspot mit den vorgenannten Randbedingungen sicher und mit geringen Investitionskosten realisierbar ist (Nutzung bestehender Internetzugang, PC mit lizenzfreier, linuxbasierter, open-source-Software als Gateway incl. Firewall und konfigurierbarem Filter und einem entsprechenden WLAN-Accesspoint).

Je nach den örtlichen Gegebenheiten (z.B. Anzahl der benötigten Access-Points zur lückenlosen Abdeckung des Kundenbereichs durch WLAN) kann eine komplette Realisierung einschl. Hardware und Inbetriebnahme bereits für weniger als 1 T€ erfolgen

Dringend zu empfehlen ist allerdings ein Wartungs- bzw. Servicevertrag zur ständigen Kontrolle und Dokumentation der ordnungsgemäßen Funktion des Hotspots insbesondere der Funktion und der Aktualität des Filters.

Die Lösung ist komplett portabel und kann in unserem Hause vollständig installiert, eingerichtet und getestet werden.
Dadurch ist auch jederzeit eine Präsentation vor Ort möglich.
Vor Ort sind dann lediglich noch mechanische Installationen, wie Ethernetleitungen o.ä., auszuführen und der Hotspot an den bestehenden Internetzugang anzupassen.

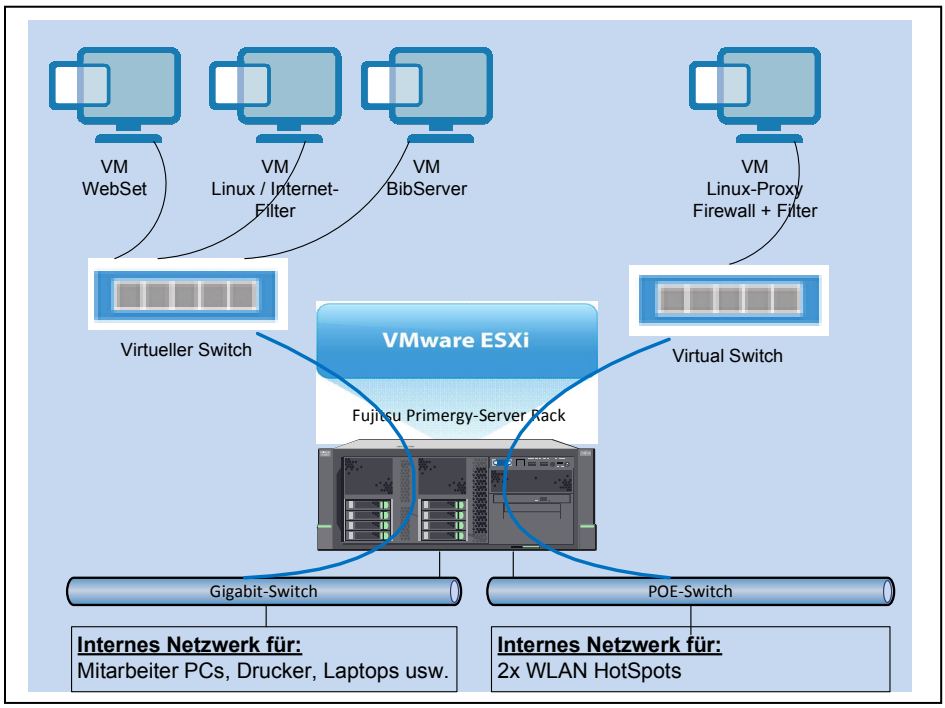

Bild 1: Übersicht über die IT-Struktur des Projektes

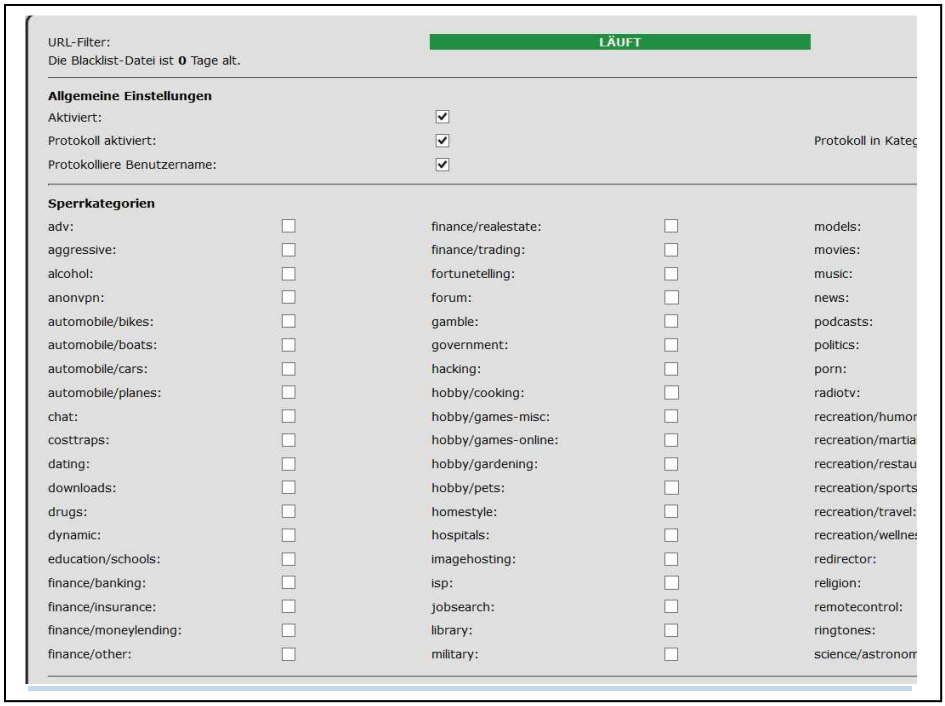

Bild 2: Ausschnitt Web-Interface konfigurierbarer Filter

Ing.-Büro Mehnert, G.-Heinemann-Str.24, D-50170 Kerpen
Tel. +49 2273 52598 / Fax: - 52526 / mail: info@mehnert.com **/** www.mehnert.com