Nur per E-Mail: tmg@bmwi.bund.de

EWE TEL GmbH | Postfach 25 09 | 26015 Oldenburg

Bundesministerium für Wirtschaft und Energie
11019 Berlin

Sie erreichen uns:
EWE TEL GmbH
Cloppenburger Straße 314 | 26133 Oldenburg
Tel. 0441 8000-3860 | Fax 0441 8000-3899
Axel.Sodtalbers@ewe.de | www.ewe.de
Ihr Ansprechpartner: Dr. Axel Sodtalbers
Ihre Zeichen/Nachricht: VIB5-160305/7

Referentenentwurf eines 2. Gesetzes zur Änderung des Telemediengesetzes (2. TMGÄndG) 7. April 2015

Sehr geehrte Frau Dr. Nielandt,
sehr geehrte Damen und Herren,

gerne nehmen wir Stellung zu dem Entwurf eines 2. Gesetzes zur Änderung des Telemediengesetzes.

EWE TEL ist Anbieterin des „EWE WLAN Hotspots". Mit diesem Produkt können Geschäftskunden an ihrem Standort Dritten einen WLAN-Internet-Zugang anbieten. Als Anbieterin eines solchen WLAN-Zugangs-Produkts begrüßen wir das Vorhaben, die Haftungsrisiken durch die aktuelle unklare Rechtslage durch neue Regelungen einzudämmen. Jedoch ist der hierzu veröffentliche Referentenentwurf vom 11.03.2015 nachzubessern.

Das gilt insbesondere für die Regelung, dass als zumutbare Maßnahme zur Verhinderung von Rechtsverletzung angemessene Sicherungsmaßnahmen durch anerkannte Verschlüsselungsverfahren zu ergreifen sind (§ 8 Abs. 4 Satz 2 Nr. 1 TMG-E). Zwar ist dieses nach dem Entwurfstext nur ein Beispiel für eine zumutbare Maßnahme („insbesondere"), jedoch kann als sicher gelten, dass die Rechtsprechung die Einhaltung dieser Vorgabe als zwingende Voraussetzung für eine Haftungsfreistellung ansehen wird.

Der Einsatz eines Verschlüsselungsverfahrens setzt indes voraus, dass der Hotspot-Anbieter dem Nutzer einen Schlüssel (welcher Art auch immer, z. B. auch ein Passwort) überlässt. Bereits dieser Zwang zur Überlassung eines Schlüssels verhindert, dass ein Nutzer ohne wesentliche Zwischenschritte (wie eine persönliche Anmeldung beim Hotspot-Anbieter o. Ä.) einen WLAN-Hotspot nutzen kann. Wir sind aber überzeugt davon, dass ein WLAN-Hotspot nur dann nachhaltig frequentiert wird, wenn er ohne solche Hürden genutzt werden kann. Gerade aus diesem Grund ist das EWE WLAN Hotspot Produkt so gestaltet, dass eine vorherige Registrierung nicht zwingend erforderlich ist. Die Hürde, dem Nutzer erst einen Schlüssel zu übermitteln, würde demgegenüber verhindern, dass WLAN-Hotspots ähnlich flächendeckend genutzt werden wie in anderen Ländern. Ebenso wenig geeignet wäre ein Versuch, die Hürde abzusenken, in dem man keinen individuelle Schlüsselüberlassung vorsähe („Schlüssel auf der Speisekarte"), weil eine Verschlüsselung sinnlos ist, wenn mehreren Personen der Schlüssel zugänglich ist.

Geschäftsführer: Dirk Brameier, Sebastian Jurczyk, Ludwig Kohnen, Norbert Westfal
Aufsichtsratsvorsitzender: Dr. Werner Brinker
Gerichtsstand: Oldenburg HRB 3723, Steuernr: 23/64/200/00622, USt-ID Nr.: DE 184286895
Sitz der Gesellschaft: EWE TEL GmbH, Cloppenburger Str. 310, 26133 Oldenburg

Oldenburgische Landesbank AG, BLZ 280 200 50, Konto 1 429 904 400
IBAN: DE86 2802 0050 1429 9044 00, BIC: OLBO DE H2 XXX
Landessparkasse zu Oldenburg, BLZ 280 501 00, Konto 000 436 436
IBAN: DE28 2805 0100 0000 4364 36, BIC: BRLADE21LZO

Darüber hinaus ist nicht ersichtlich, warum eine Verschlüsselung eine zumutbare Maßnahme darstellen soll, „um eine Rechtsverletzung durch Nutzer zu verhindern" (§ 8 Abs. 4 Satz 1 a. E. TMG-E). Dass Daten über die Verbindung zwischen dem Endgerät des Nutzers und dem WLAN-Hotspot verschlüsselt übertragen werden, verhindert doch keineswegs, dass Nutzer Rechtsverletzungen begehen. Ein Nutzer kann z. B. urheberrechtlich geschütztes Material genauso über eine verschlüsselte Verbindung zu dem WLAN-Hotspot herunter- oder heraufladen wie über eine unverschlüsselte Verbindung.

Möglichen Rechtsverletzungen kann viel besser durch geeignete Filter und Portsperren begegnet werden. Bei den EWE WLAN Hotspots etwa sind bestimmte, potenzielle gefahrenträchtige Ports gesperrt, ebenso nach dem Blacklisting-Prinzip gesperrt sind bestimmte Internetseiten oder Internetdienste mit bestimmten Inhalten (Filesharing, Pornografie, Gewalt, etc.). Solche Beschränkungen sind ohne weiteres zumutbar, weil Nutzer öffentlich zugänglicher WLAN-Hotspots nicht davon ausgehen können – und dieses auch nicht tun –, im öffentlichen Raum sämtliche Internetdienste nutzen zu können.

Dieses Beispiel für die Möglichkeiten, Rechtsverletzungen durch technische Mittel zu verhindern, zeigt auch, dass es sinnvoll ist, zwischen geschäftsmäßigen und privaten Anbietern von WLAN-Hotspots zu unterscheiden. Denn vor allem geschäftsmäßige Anbieter – mehr noch die ohnehin auf diesem Gebiet besonders erfahrenen Telekommunikationsanbieter – verfügen über das notwendige Know-how für einen möglichst gefahrlosen und zugleich nutzerfreundlichen Betrieb von WLAN-Hotspots.

Freundliche Grüße

ppa. Matthias Büning

i. A. Dr. Henning Wellhausen, LL.M.