Fallbeispiele - Das Recht und Wireless-LAN

Die Haftung des Inhabers eines Internetanschlusses gehört noch immer zu den umstrittensten Fragen des IT-Rechts. Die Bandbreite an Entscheidungen ist groß und reicht von der Bezeichnung des Internetrouters als „gefährliches Werkzeug“ (so das LG München I) bis zur Freizeichnung der Haftung des Anschlussinhabers soweit und solange er gar nicht damit rechnen musste, dass sein Anschluss illegal genutzt wird (so das OLG Frankfurt am Main).
Trotz alledem bildet sich nach und nach eine Linie heraus, die insbesondere hinsichtlich der Haftung von ungeschützten Wireless-LAN Netzwerken schon recht einheitlich geworden ist. Die Gerichte sind sich hier nahezu einig, dass ein völlig unbeschütztes WLAN-Netz eine Haftung des Anschlussinhabers – zumindest auf Unterlassung als so genannter Störer – auslöst. Was allerdings zumutbar ist und wie weit die Sicherungsmaßnahmen des Anschlussinhabers gehen ist noch lange nicht entschieden. Reicht eine unsichere WEP-Verschlüsselung aus? Muss immer der neueste Sicherheitsstandard gewählt werden? Was ist mit der Notwendigkeit einer Firewall?

Doch auch der andere Fall ist zu bedenken: Macht sich beispielsweise derjenige, der „schwarz“ in einem fremden WLAN-Netz mitsurft strafbar?

Und: Muss der Betreiber eines offenen WLAN-Netzes die Vorschriften zur Vorratsdatenspeicherung beachten?

Hierzu sollen die folgenden Fallbeispiele die rechtlichen Probleme und den aktuellen Sachstand der bislang bekannten Urteile hierzu beleuchten.

Die Fallbeispiele orientieren sich im Wesentlichen an realen Fällen, versuchen jedoch auch wo es erforderlich ist durch Abweichungen auf bestimmte Konstellationen hinzuweisen.

Fallbeispiel 1:

Die Antragsstellerin macht im Wege eines Verfahrens auf Erlass einer Einstweiligen Verfügung (ein Eilverfahren zur vorläufigen Regelung eines Sachverhalts, um ein langwieriges Klageverfahren zu vermeiden) einen Anspruch auf Unterlassung des Anbietens einer MP3-Datei eines urheberrechtlich geschützten Musikwerks über eine so genannte Internet-Tauschbörse geltend. Der Anschlussinhaber versichert eidesstattlich, er habe nie eine solche Internet-Tauschbörse besucht, geschweige denn ein geschütztes Werk heruntergeladen oder anderen angeboten. Aber er habe zum fraglichen Zeitpunkt ein ungesichertes WLAN-Netz betrieben.

Frage:
Haftet der Inhaber des Internetanschlusses für die über seinen Anschluss begangene Tat auch dann, wenn er nachweislich nicht selbst die Verletzung begangen hat?

Fallbeispiel 2:

Der A surft in der Absicht, kein Entgelt dafür zu bezahlen, und ohne Erlaubnis des Anschlussinhabers von der Straße aus in einem unverschlüsselten W-LAN-Netz eines Anderen mit. Der Anschlussinhaber verfügt über eine Flatrate; ihm entsteht also kein finanzieller Schaden durch das „mitsurfen“ des A. Der Anschlussinhaber bemerkt die Einwahl des A in sein Netzwerk und ruft die Polizei. Er erstattet Strafanzeige gegen den A.

Frage:
Hat sich A strafbar gemacht?

Fallbeispiel 3:

A betreibt zur Förderung der Nutzungsmöglichkeiten des Internets ein kostenloses offenes WLAN-Netz, das alle, die sich in dessen Einzugsbereich befinden, nutzen können und dürfen.

Frage:
Muss A die Verkehrsdaten der Nutzer seines offenen WLAN-Netzes gemäß den Vorgaben der so genannten Vorratsdatenspeicherung für 6 Monate speichern und auf Verlangen den Strafverfolgungsbehörden bzw. Geheimdiensten herausgeben?

ANTWORTEN:

Fallbeispiel 1

JA.
Als Inhaber des genutzten Internetzugangs haftet er, wenn nicht als Täter, so zumindest als so genannter Störer. Ein Verschulden ist im Rahmen des Unterlassungsanspruchs nicht erforderlich.

Störer ist, wer in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechtsguts beigetragen und zumutbare Sicherungsmaßnahmen unterlassen hat. Ob die Urheberrechtsverletzung von seinem Computer aus begangen worden ist oder ob Dritte - z.B. unter Ausnutzung seines ungesicherten WLAN-Netzes - auf seinen Internetzugang zugegriffen haben, ist ohne Bedeutung. Ohne den vom Betroffenen geschaffenen Internetzugang hätte weder die eine noch die andere Möglichkeit bestanden. Die Schaffung des Internetzugangs ist folglich für die Rechtsverletzung in jedem Fall kausal. Dem Vortrag des Anschlussinhabers ist auch nicht zu entnehmen, dass er alle zumutbaren Maßnahmen ergriffen hat, um den Zugriff auf die Internet-Tauschbörse über seinen Anschluss zu unterbinden. Die Obliegenheit, solche Maßnahmen zu ergreifen, folgt aus dem Umstand, dass er mit dem Internetzugang eine Gefahrenquelle geschaffen hat, die nur er überwachen kann. Ihn trifft auch die entsprechende Darlegungslast, da naturgemäß nur er Kenntnis von den getroffenen Vorkehrungen haben kann. Der Anschlussinhaber beschränkt sich hier jedoch darauf, zu behaupten, dass sein Rechner nicht über die erforderliche Software verfügt, um sich in das Netzwerk einzuloggen; dies genügt vorliegend nicht.

Es ist nämlich möglich, dass ein Dritter über das vorhandene unverschlüsselte WLAN-Netz Zugriff auf den Anschluss genommen hat. Es ist einem Anschlussinhaber aber zuzumuten, zumindest Standardmaßnahmen zur Verschlüsselung des Netzwerks zu ergreifen; ansonsten verschafft er nämlich objektiv Dritten die Möglichkeit, sich hinter seiner Person zu verstecken und im Schutze der von ihm geschaffenen Anonymität ohne Angst vor Entdeckung ungestraft Urheberrechtsverletzungen begehen zu können. Auch eine - möglicherweise sogar gestattete - Nutzung durch Familienmitglieder des Anschlussinhabers kommt als Ursache in Frage. Selbst wenn der Anschlussinhaber beweisen könnte, dass die erforderliche Software auf seinem Rechner nicht installiert war bleibt die Möglichkeit über einen weiteren, nicht angeschlossenen Rechner (z.B. ein Laptop mit WLAN-Verbindung) einen Zugriff vorzunehmen. Auch die Zugriffsmöglichkeit durch unbekannte Dritte wäre bei einem ungesicherten W-LAN-Anschluss vom Anschlussinhaber nicht zu widerlegen.

(Angelehnt an LG Düsseldorf, Urteil vom 16.07.2008, Aktenzeichen 12 O 195/08, rechtskräftig; ebenso: LG Mannheim, Urteil vom 25.01.2007, Aktenzeichen 7 O 65/06, bestätigt durch OLG Karlsruhe, Beschluss vom 11.06.2007, Aktenzeichen 6 W 20/07. Es gibt bereits Urteile, die es ausreichen lassen, wenn das WLAN-Netz mittels WEP-Verschlüsselung gesichert war. Die sicherere WPA- oder WPA2-Verschlüsselung sei nicht erforderlich. Irgendetwas muss der Anschlussinhaber aber auf jeden Fall tun, wenn er einer Haftung entgehen will.)

Fallbeispiel 2

JA.
A hat gegen das so genannte Abhörverbot nach § 89 Satz 1 TKG verstoßen und sich somit gemäß § 148 Abs. 1 Nr. 1 TKG strafbar gemacht. Das Abhören von Nachrichten im Sinne dieser Vorschrift umfasst den vorliegenden Sachverhalt. Der WLAN-Router ist eine elektrische Sende- und Empfangseinrichtung und damit eine Funkanlage im Sinne von § 89 TKG. Der Begriff „Nachrichten“,

der entsprechend der Entscheidung des BGH zu Radarwarngeräten sehr extensiv auszulegen ist, umfasst auch die Zuweisung einer IP-Adresse durch den Router. Diese Nachricht hat der A abgehört. Abhören meint dabei das tatsächliche Wahrnehmen. Während der Internetnutzung greift der A. auf die zugesandte IP-Adresse zu und wertet sie aus. Die Nachrichten wurden damit abgehört. Fraglich ist, ob die Nachrichten zudem nicht für A bestimmt waren. Hier ist anzunehmen, dass die IP-Adresse gerade nicht für A bestimmt war, auch wenn dieser der eigentliche Kommunikationspartner mit dem WLAN-Router ist. Denn die Festlegung, wer zur Verwendung der IP-Adresse berechtigt ist, wird vom Eigentümer des WLAN-Routers und nicht dem Gerät selbst getroffen.

Außerdem hat sich A gemäß § 44 i.V.m. § 43 Abs. 2 Nr. 3 BDSG strafbar gemacht. Voraussetzung ist das Vorliegen von personenbezogenen Daten. Nach der Legaldefinition des § 3 Abs. 1 BDSG sind Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Solche Daten fallen grds. auch bei IP-Adressen und Zugangsdaten an. Denn insb. die IP-Adresse kann jederzeit zurückverfolgt und einer bestimmten Person zugeordnet werden. Indem auf den Router zugegriffen wird, werden personenbezogene Daten i.S.d. Gesetzes abgerufen. Voraussetzung ist weiterhin, dass der jeweilige Täter in Bereicherungs- oder Schädigungsabsicht handelte. Unzweifelhaft war es Ziel des A, die Internetnutzung, die üblicherweise nur gegen Entgelt gewährt wird, zu erhalten. Um diesen Wert der Nutzung wollte sich A bereichern. Außerdem hat er billigend in Kauf genommen, dass der Anschlussinhaber möglicherweise über keine Flatrate verfügte und seinen Internetanschluss nach Volumen oder Zeit abrechnen musste.

A konnte auch nicht davon ausgehen, dass im reinen Wohngebiet ein sog. kostenloser „Hot-Spot“ eingerichtet war.

(Angelehnt an AG Wuppertal, Urteil vom 03.04.2007, Aktenzeichen 22 Ds 70 Js 6906/06, rechtskräftig. Das Urteil ist vielfach auf Kritik gestoßen und wird unter Juristen kontrovers diskutiert. Das Gericht hat eine Geldstrafe von 20 Tagessätzen zu je 5,- Euro vorbehalten, um den Angeklagten in Zukunft vom „Schwarz-Surfen“ abzuhalten. Einer Einstellung des Verfahrens gegen Verzicht auf den Laptop hat der Angeklagte nicht zugestimmt. Der Laptop nebst Adapter wurde als Tatwerkzeug eingezogen)

Fallbeispiel 3

JA.
Nach § 11 TKG erbringt A durch sein offenes WLAN-Netz einen „öffentlich zugänglichen Telekommunikationsdienst für Endnutzer“. Die Kostenpflichtigkeit des Dienstes oder eine wie auch immer geartete Gewinnerzielungsabsicht ist dafür nicht erforderlich.
Auf die Frage der Verhältnismäßigkeit des Aufwands der Speicherung und Archivierung dieser Daten im Hinblick auf den „kostenlosen Service“ durch A kommt es bei der Frage der Speicherpflicht nicht an. Die Speicherpflicht besteht bereits seit dem 01.01.2008, wird jedoch erst seit dem 01.01.2009 im Falle des Unterlassens der Speicherung als Ordnungswidrigkeit sanktioniert. Das Telekommunikationsgesetz (TKG) sieht immerhin Bußgelder bis zu 300.000,00 Euro vor.

(Diese Fragen sind höchst umstritten und noch nicht Gegenstand von gerichtlichen Entscheidungen gewesen. Es ist auch noch keine Verhängung eines Bußgeldes bekannt. Die Behörden warten wohl die Grundsatzentscheidung des Bundesverfassungsgerichts zu der ganzen Thematik ab, die dieses Jahr erfolgen soll.)

Timo Schutt
Rechtsanwalt & Fachanwalt für IT-Recht