Anmerkung zu AG Frankfurt am Main, Urteil v. 14.6.2013 - 30 C 3078/12 (75): Kein persönlicher WLAN-Schlüssel bei werksseitigem individuellen Schlüssel erforderlich

-- erschienen in Multimedia und Recht (MMR) Heft 9/2013, S. 607 ff. --

AG Frankfurt: Kein persönlicher WLAN-Schlüssel bei werksseitigem individuellen Schlüssel erforderlich

Leitsätze der Redaktion: Authentifizierungsschlüssel eines WLAN-Routers, die bereits ab Werk individuell pro Gerät vergeben werden, gewähren ein hinreichendes, hohes Schutzniveau. Eine Personalisierung ist in diesem Fall auch vor dem Hintergrund des Urteils BGH "Sommer unseres Lebens" nicht erforderlich.

§§ 823, 1004 BGB; §§ 97, 97a UrhG
AG Frankfurt, Urteil v. 14.6.2013 - 30 C 3078/12 (75)

Sachverhalt

Die Klägerin begehrt Schadensersatz aufgrund einer behaupteten Urheberrechtsverletzung durch den Beklagten sowie Kostenersatz wegen der durch die erfolgte Abmahnung entstandenen Rechtsanwaltsgebühren.
Die Klägerin gehört zu den führenden deutschen Tonträgerherstellern und ist als solche Inhaberin der ausschließlichen Verwertungsrechte des streitgegenständlichen Musikalbums A (Doppel-CD) der Musikgruppe B für das Gebiet der Bundesrepublik Deutschland.
Mit Anwaltsschreiben vom 08.12.2009 (Anlage K 3) mahnte die Klägerin den Beklagten ab ... Sie forderte ihn zur Abgabe einer strafbewehrten Unterlassungserklärung auf, ... [die] der Beklagte ohne Anerkennung einer Rechtspflicht ab[gab].

Die Klägerin behauptet, die von ihr in Auftrag gegebenen Ermittlungsmaßnahmen zur Feststellung von Verletzungen ihrer Leistungsschutzrechte durch unautorisierte Internet-Angebote hätten ergeben, dass am 18.07.2009 um 12:45 Uhr (MEZ) über den Internetanschluss mit der IP-Adresse "79.229.15.172" das Musikalbum A (Doppel-CD) der Musikgruppe B zum Herunterladen verfügbar gemacht worden sei. ... Der Beklagte selbst habe die streitgegenständlichen Musikalbum für den Abruf durch andere Teilnehmer des Filesharing-Systems verfügbar gemacht.

Der Beklagte behauptet, er habe die behauptete Rechtsverletzung nicht begangen. Er habe zu keinem Zeitpunkt die streitgegenständliche Datei und ein Filesharingprogramm auf seinem Rechner vorgehalten. Zu dem damaligen Zeitpunkt seien seine Ehefrau mit ihrem Rechner, sein 16-jähriger Sohn mit seinem Laptop sowie seine 20-jährige Tochter mit ihrem Laptop über das WLAN-Netzwerk an dem Internetanschluss des Beklagten angebunden gewesen. Der Beklagte habe keine Kenntnis davon gehabt, dass eines der übrigen Familienmitglieder den Anschluss für rechtswidrige Aktivitäten nutzt. Er habe im September 2006 im Familienkreis mit der Ehefrau die zwei Kinder belehrt, illegales und strafbares Herunterladen und zum Download bereit stellen von urheberrechtlich geschützten Werken zu unterlassen und insbesondere keine Tauschbörsen zu nutzen. Er habe seinen Kindern ausdrücklich die Nutzung der Dienste BitTorrent, Applejuice, Directconnect und eDonkey, aber auch die Nutzung vergleichbarer Dienste untersagt.

Der Beklagte behauptet ferner, der von ihm im streitgegenständlichen Zeitpunkt genutzte W-Lan-Router sei eine Fritz-Box W-Lan 750 gewesen. Der Internetanschluss sei WEP-verschlüsselt gewesen. ...

Aus den Gründen

I. Die Klage ist zulässig. Die örtliche Zuständigkeit des Amtsgerichts Frankfurt am Main ergibt sich aus § 32 ZPO. ...

II. Die Klage ist jedoch unbegründet.

1. Die Klägerin hat gegen den Beklagten keinen Anspruch auf Schadenersatz aus § 97 Abs. 2 UrhG, da eine Haftung des Beklagten als Täter oder Teilnehmer der behaupteten Urheberrechtsverletzung nicht in Betracht kommt. Die Klägerin hat dafür, dass der Beklagte selbst die Urheberrechtsverletzung begangen hat, keinen Beweis angeboten. Die Klägerin kann sich insofern auch nicht auf Beweiserleichterungen stützen. Denn die tatsächliche Vermutung, dass der Inhaber eines Internetanschlusses für eine von diesem Anschluss aus begangene Rechtsverletzung verantwortlich ist (vgl. BGH, Urteil vom 12.05.2010, I ZR 121/08 - juris), ist hinreichend entkräftet. ...
[Der Beklagte] hat substantiiert dargetan und in seiner informatorischen Anhörung angegeben, dass neben ihm, die im Haushalt wohnende Ehefrau, seine damals 20-jährige Tochter und sein damals 16-jähriger Sohn über eigene Rechner verfügten, die jeweils Zugriff zu dem W-Lan-Anschluss hatten. Seine Angaben sind glaubhaft und lebensnah. Er berichtete in Übereinstimmung mit der Zeugin widerspruchsfrei und objektiv von den damaligen Verhältnissen. Das Gericht hat keinen Zweifel, dass in einem Vier-Personenhaushalt im Jahr 2009 alle Familienmitglieder – insbesondere Kinder im Alter von 16 und 20 Jahren – über eigene Computer verfügen und das Internet nutzen.
Es ist daher ernsthaft möglich, dass die rechtsverletzende Handlung von einem der drei weiteren Familienmitglieder begangen worden ist, das ebenfalls den W-Lan-Anschluss des Beklagten nutzte. ...

2. Die Klägerin hat gegen den Beklagten auch keinen Anspruch auf Erstattung von Rechtsanwaltsgebühren aus § 97a Abs. 1 S. 2 UrhG. Der Beklagte haftet als Inhaber des Internetanschlusses auch nicht als Störer wegen einer von einem Dritten begangenen Urheberrechtsverletzung auf Unterlassung. Auch die von der Klägerin geltend gemachten Ansprüche auf Erstattung von Abmahnkosten sind daher nicht begründet, da die Abmahnung unter keinem Gesichtspunkt berechtigt war.

Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wer - ohne Täter oder Teilnehmer zu sein - in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt. Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers die Verletzung von Prüfpflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen eine Prüfung zuzumuten ist (vgl. BGH, Urteil vom 12.05.2010, I ZR 121/08 – juris).

Die Anforderungen an die Aufsichtspflicht, insbesondere die Pflicht zur Belehrung und Beaufsichtigung von Kindern, richten sich nach der Vorhersehbarkeit des schädigenden Verhaltens. Dabei hängt es hauptsächlich von den Eigenheiten des Kindes und seinem Befolgen von Erziehungsmaßnahmen ab, in welchem Umfang allgemeine Belehrungen und

Verbote ausreichen oder deren Beachtung auch überwacht werden muss (vgl BGH, NJW 2009, 1952 Rn. 17; NJW 2009, 1954 Rn. 14, jeweils mwN).

Danach genügen Eltern ihrer Aufsichtspflicht über ein normal entwickeltes Kind, das ihre grundlegenden Gebote und Verbote befolgt, regelmäßig bereits dadurch, dass sie das Kind über die Rechtswidrigkeit einer Teilnahme an Internettauschbörsen belehren und ihm eine Teilnahme daran verbieten. Eine Verpflichtung der Eltern, die Nutzung des Internets durch das Kind zu überwachen, den Computer des Kindes zu überprüfen oder dem Kind den Zugang zum Internet (teilweise) zu versperren, besteht grundsätzlich nicht. Zu derartigen Maßnahmen sind Eltern erst verpflichtet, wenn sie konkrete Anhaltspunkte dafür haben, dass das Kind dem Verbot zuwiderhandelt (BGH, Urteil v. 15.11.2012, I ZR 74/12 - juris).

Der Beklagte hat seiner Aufsichtspflicht dadurch genügt, dass er seinen Kindern die rechtswidrige Teilnahme an Internettauschbörsen nach einer entsprechenden Belehrung verboten hat. Der Beklagte hat in seiner informatorischen Befragung nachvollziehbar, lebensnah und glaubhaft vorgetragen, er habe seinerzeit über so genannte illegale Tauschbörsen gehört und mit seinen Kindern im September 2006 darüber gesprochen und ihnen die Teilnahme an solchen verboten. Er sei hierfür sensibilisiert gewesen, da er auch selbständig sei, er von den finanziellen Nöten von Musikern wisse, und dass es sich bei der entsprechenden Musik um geistiges Eigentum handle, was man nicht ohne Zahlung illegal herunterladen dürfe. Für die Glaubhaftigkeit seiner Angaben spricht auch, dass der Beklagte in seiner informatorischen Anhörung nicht nur für ihn Günstiges mitteilte, sondern u.a. auch angab, dass er den Authentifizierungsschlüssel auf seiner Fritz-Box nicht personalisiert habe.

Damit ist der Beklagte den an die Vorgabe von Verhaltensregeln zu stellenden Anforderungen gegenüber seinen Kindern nachgekommen.

Eine Verletzung zumutbarer Prüfpflichten gegenüber der Ehefrau des Beklagten, der Zeugin C, ist ebenfalls nicht festzustellen. Denn es sind keine konkreten Anhaltspunkte zu erkennen, dass der Beklagte wusste oder hätte wissen müssen, dass seine Ehefrau Urheberrechtsverletzungen über seinen Internetanschluss begeht, die er durch zumutbare Maßnahmen hätte verhindern können. Denn ein Ehemann kann seiner Ehefrau, solange er keine konkreten Anhaltspunkte für Rechtsverletzungen hat, den auf seinen Namen laufenden Internetanschluss überlassen, ohne diese ständig überwachen zu müssen. Sofern der Anschlussinhaber nicht mit einer Rechtsverletzung durch seinen Ehepartner rechnen muss, sind Hinweis-, Aufklärungs- und Überprüfungspflichten diesem gegenüber unzumutbar (OLG Frankfurt, Beschluss v. 22.03.2013, Az. 11 W 8/13).

Der Beklagte hat auch die ihm als Betreiber eines WLAN-Anschlusses obliegende Prüfungspflicht hinsichtlich ausreichender Sicherungsmaßnahmen nicht verletzt.

Im Rahmen seiner informatorischen Anhörung teilte der Beklagte mit, seine W-Lan-Verbindung sei über WEP und einen 13-stelligen werksseitigen Authentifizierungsschlüssel gesichert gewesen. Dieser habe sich auf der Rückseite seiner Fritz-Box befunden. Zwar hat der Beklagte dieses Passwort nicht in ein persönliches Passwort geändert. Allerdings handelt es sich – gerichtsbekannt - bei den auf einer Fritz-Box seit 2004 verwendeten Authentifizierungsschlüsseln um solche, die bereits ab Werk individuell pro Gerät vergeben werden. Vor diesem Hintergrund ist der seitens des Bundesgerichtshofs in seiner Entscheidung vom 12.05.2010, I ZR 121/08 erstrebte Zweck eines hohen Schutzniveaus, welches den Zugriff unbefugter Dritter ausschließt, auch ohne ein persönliches Passwort – das regelmäßig nicht länger als 13-stellig sein wird – erreicht. Der Bundesgerichtshof kann in der

oben zitierten Entscheidung lediglich die Fälle im Blick gehabt haben, in denen die Router einer Modellreihe werksseitig über den gleichen Authentifizierungsschlüssel verfügen, so dass ein effektiver Schutz für diese Fälle nur über eine sofortige Personalisierung des Passwortes gewährleistet war (vgl. Mantz, Anm. zu BGH Urt. v. 12.05.2010 in MMR 2010, 569).

Anmerkung

Das Urteil des *AG Frankfurt* ist ein Beleg dafür, dass in Teilbereichen der Störerhaftung der privaten Internetanschlussinhaber Rechtssicherheit einkehrt. Es enthält aber zusätzlich begrüßenswerte Klarstellungen.

1. Insbesondere mit seiner Entscheidung „Morpheus" (*BGH* MMR 2013, 388 m. Anm. Hoffmann) im Hinblick auf die Aufsichtspflichten von Eltern für ihre (zumindest jugendlichen) Kinder hat der *BGH* eine klare Linie dahingehend aufgezeigt, dass Eltern ihre Kinder belehren, aber ohne konkrete Hinweise nicht überwachen müssen. Diese Linie ist von den Instanzgerichten nun übernommen worden. Das *OLG Frankfurt* hat die Rechtsprechung kürzlich insoweit ergänzt, dass Ehepartner sich nicht gegenseitig überwachen müssen (OLG Frankfurt GRUR-RR 2013, 246). Diesen Vorgaben der höheren Rechtsprechung ist das *AG* in überzeugender Weise gefolgt.

2. Von Interesse ist an dem Urteil insbesondere der letzte Abschnitt: Der Beklagte hatte vorgetragen, dass er zum Zeitpunkt der angeblichen Rechtsverletzung als WLAN-Router eine „FritzBox W-Lan 750" mit WEP-Verschlüsselung und einem 13-stelligen Kennwort verwendet und das zuvor werksmäßig im WLAN-Router eingestellte Passwort für den Zugang zum WLAN nicht verändert habe.
Diese Unterlassung – das Nichtändern des werkseitig eingestellten Kennworts in ein individualiertes WLAN-Kennwort – hatte der BGH in seinem Urteil „Sommer unseres Lebens" als Verletzung der Prüfungs- und Überwachungspflichten angesehen (BGH MMR 2010, 565 m. Anm. *Mantz* Rn. 22 ff., 32 ff. – Sommer unseres Lebens) und hierzu ausgeführt:

> *Die Prüfpflicht des Bekl. bezieht sich aber auf die Einhaltung der im Kaufzeitpunkt des Routers für den privaten Bereich marktüblichen Sicherungen. Diese Pflicht hat der Bekl. verletzt. Der Bekl. hat es nach dem Anschluss des WLAN-Routers bei den werkseitigen Standardsicherheitseinstellungen belassen und für den Zugang zum Router kein persönliches, ausreichend langes und sicheres Passwort vergeben. Der Schutz von Computern, Kundenkonten im Internet und Netzwerken durch individuelle Passwörter gehörte auch Mitte 2006 bereits zum Mindeststandard privater Computernutzung und lag schon im vitalen Eigeninteresse aller berechtigten Nutzer. Sie war auch mit keinen Mehrkosten verbunden.*

Bereits im Fall „Sommer unseres Lebens" war dieser Befund nicht nachvollziehbar. Denn wie im vorliegenden Fall war das Kennwort im Router individualisiert und bestand aus einer zufälligen Zeichenfolge (*Mantz*, MMR 2010, 568, 569; (vgl. http://www.avm.de/de/News/artikel/2010/wlan_urteil.html). Ein solches nur dem Inhaber des WLAN-Routers bekanntes Kennwort ist daher mindestens ebenso sicher wie ein selbst gewähltes, in vielen Fällen sogar sicherer. Richtigerweise folgerte das *AG* daher, dass der *BGH* ein hohes Schutzniveau im Auge hatte, das im vorliegenden Fall gewahrt war. Eine Ausnahme hiervon muss man allerdings wohl machen, wenn das werkseitig vorgegebene

Kennwort tatsächlich nicht zufällig ist, sondern vom Hersteller fehlerhaft und damit für Angreifer ausrechenbar vergeben wurde (vgl. z.B. zu bestimmten Routern der Telekom und Vodafone Meldung von heise-security v. 20.08.2011, http://heise.de/-1326796). Dies war aber bei den von AVM hergestellten WLAN-Routern bei *BGH* „Sommer unseres Lebens" und hier – soweit bekannt – nicht der Fall.

3. Eine andere spannende Problematik ergibt sich aus der Entscheidung des *AG Frankfurt* dadurch, dass der Beklagte lediglich eine Verschlüsselung nach dem Standard WEP (*Wired Equivalent Privacy*) eingesetzt hat. Dieser Standard ist heutzutage als unsicher anzusehen, da die Verschlüsselung – entsprechende online verfügbare Werkzeuge vorausgesetzt – in wenigen Minuten gebrochen werden kann (*Sorge*, CR 2011, 273 m.w.N.). Zur Problematik des eingesetzten Sicherheitsstandards hatte der *BGH* ausgeführt (*BGH* MMR 2010, 565 Rn. 23 – Sommer unseres Lebens):

> *Welche konkreten Maßnahmen zumutbar sind, bestimmt sich auch für eine Privatperson zunächst nach den jeweiligen technischen Möglichkeiten (vgl. BGHZ 172, 119 Rdnr. 47 – Internetversteigerung II). Es würde die privaten Verwender der WLAN-Technologie allerdings unzumutbar belasten und wäre damit unverhältnismäßig, wenn ihnen zur Pflicht gemacht würde, die Netzwerksicherheit fortlaufend dem neuesten Stand der Technik anzupassen und dafür entsprechende finanzielle Mittel aufzuwenden. Die Prüfungspflicht im Hinblick auf die unbefugte Nutzung eines WLAN-Routers konkretisiert sich vielmehr dahin, dass jedenfalls die im Kaufzeitpunkt des Routers für den privaten Bereich marktüblichen Sicherungen ihrem Zweck entsprechend wirksam einzusetzen sind*

Daher ist jeweils die Frage zu stellen, welche Sicherungsmaßnahmen beim Kauf des WLAN-Routers des Beklagten marktüblich waren. Der Vortrag des Beklagten im Hinblick auf den Zeitpunkt des Kaufs des WLAN-Routers ist nicht ganz eindeutig, vermutlich erfolgte dieser 2006, als der Beklagte auch seine Kinder belehrte. Der Beklagte hat allerdings die werksseitige Einstellung mit einer WEP-Verschlüsselung mit einer Kennwortlänge von 13 (zufälligen) Zeichen belassen. Daher kann davon ausgegangen werden, dass diese Form der Sicherung beim Kauf noch marktüblich war, obwohl im Jahr 2006 die Unsicherheit der Verschlüsselung mit WEP zumindest in Fachkreisen grundsätzlich bekannt war (heise-security, Meldung vom 02.05.2005, http://heise.de/-270672; vgl. auch *Mantz*, MMR 2006, 763, 765). Im Ergebnis konnte daher die Unsicherheit von WEP dem Beklagten nicht zur Last gelegt werden. Die Entscheidung des *AG* hält sich insoweit streng innerhalb der vom *BGH* gesetzten Grenzen.

4. Diese Vorgaben des *BGH* offenbaren übrigens eine weitere „Sollbruchstelle" bei der Haftungssituation des privaten Anschlussinhabers. Nach dem *BGH* ist eine Verschlüsselung mit WEP bei Privatpersonen hinreichend, wenn diese zum Zeitpunkt des Kaufs des WLAN-Routers marktüblich war. Da aber jedermann heutzutage diese (rechtlich hinreichende) Verschlüsselung ohne Probleme brechen kann, kann man gegen die tatsächliche Vermutung, dass eine Verletzungshandlung über das Internet vom Anschlussinhaber begangen worden sein wird (s. nur BGH MMR 2013, 388 Rn. 33 – Morpheus), jedenfalls bei Betrieb eines WLAN-Routers mit WEP-Verschlüsselung einwenden, dass jeder Dritte die Verschlüsselung gebrochen und den Anschluss genutzt haben kann. Es fehlt in diesen Fällen somit bereits die Tatsachengrundlage für die Vermutung, unabhängig von der Existenz von das WLAN mitnutzenden Familienmitgliedern. Angemerkt sei noch, dass auch die Verschlüsselung nach dem Standard WPA (*WiFi-Protected Access*), die bis vor wenigen Jahren marküblich war und möglicherweise heute in Teilen noch ist, mittlerweile ebenfalls als unsicher gilt

(vgl. *Ohigashi/Morii*, A Practical Message Falsification Attack on WPA, 2009; heise-security, Meldung v. 27.08.2009, http://heise.de/-753357).

5. Wer heute einen WLAN-Router kauft und einrichtet, sollte daher auf eine Verschlüsselung nach dem Standard WPA2 mit einem zufällig generierten, aus Groß- und Kleinbuchstaben, Zahlen und möglichst auch Sonderzeichen bestehenden, mindestens 16 (besser mehr) Zeichen langen Kennwort setzen. Hierfür existieren im Internet entsprechende Generatoren, bspw. unter http://www.gaijin.at/olspwgen.php (dort „WPA2-Schlüssel" auswählen).
Zu beachten ist ferner, dass der BGH in „Sommer unseres Lebens" nur für Privatpersonen im Hinblick auf die Zumutbarkeit auf die zum Zeitpunkt des Kaufs marktübliche Sicherung abgestellt hat. Bei Anbietern gewerblicher WLANs könnte daher der jeweils (wohl aufgrund regelmäßiger Prüfung) marktübliche Sicherheitsstandard zu verwenden sein (so evtl. LG Frankfurt MMR 2011, 401; LG Frankfurt, Urt. v. 28.6.2013 – 2/06 O 304/12).
Betreiber öffentlich zugänglicher oder Kunden zur Verfügung gestellter WLANs dürften im Hinblick auf die Absicherung eines WLANs jedoch vielmehr allein den Pflichten nach § 109 TKG unterliegen. Gemäß § 109 TKG ist die Verschlüsselung eines öffentlichen WLANs aber nicht angezeigt, vielmehr ist die Anlage selbst z.B. gegen unbefugten (physischen und nicht-physischen) Zugriff zu sichern.
Gegenüber Schadensersatzansprüchen sind die Betreiber öffentlich zugänglicher WLANs ohnehin nach § 8 TMG privilegiert (*Hoffmann*, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl. 2011, § 8 Rn. 17; *Spindler*, CR 2010, 592, 595; *Altenhain*, in MünchKommStGB, 2. Aufl. 2010, vor § 7 TMG Rn. 43; *Mantz*, Rechtsfragen offener Netze, 2008, 48 m.w.N.).