

Michael Knopp

WLAN-Haftung

Anmerkung zum Urteil des BGH vom 12. Mai 2010

Die als „Sommer unseres Lebens“ betitelte Entscheidung des BGH zur WLAN-Haftung hat auf den ersten Blick Klarheit zu den Haftungsrisiken privater WLAN-Betreiber geschaffen. Auf den zweiten Blick wecken die Entscheidungsbegründung und -folgen jedoch Zweifel, ob diese Entscheidung als künftiges Leitbild verwendet werden kann.

Einleitung

Der Betreiber eines unzureichend gesicherten WLANs kann auf Unterlassung, nicht jedoch auf Schadensersatz für unbefugte Handlungen Dritter in Anspruch genommen werden. So lautet zusammengefasst die zentrale Aussage des BGH Urteils vom 12.5.2010.¹

Nach den Sachverhaltsfeststellungen bestritt der Beklagte die korrekte Feststellung der IP-Adresse, trug vor, zur fraglichen Zeit im September 2006 im Urlaub gewesen zu sein und an seiner Computeranlage samt Router den Netzstecker gezogen zu haben. Zu Letzterem konnte der Beklagte den Instanzurteilen² zufolge jedoch nicht ausreichend Beweis führen. Die Standardeinstellungen seines Routers sahen allerdings eine WPA-Verschlüsselung vor. Die Entscheidung geht daher davon aus, dass die Urheberrechtsverletzung über das WPA-gesicherte, mit unverändertem Herstellerpasswort betriebene WLAN erfolgt sei. Dies löse die Störerhaftung aus, denn dem Anschlussinhaber sei zuzumuten, die Sicherungsmaßnahmen zu überprüfen. Es

seien die im Kaufzeitpunkt des Routers für den privaten Bereich marktüblichen Sicherungen von Betriebsbeginn an wirksam einzusetzen. Unzumutbar sei dagegen für die Verwender, ihre Technologie fortlaufend dem neuesten Stand der Technik anzupassen.³ Der Beklagte habe aber, so bereits das LG Frankfurt a.M.,⁴ seine Prüfpflicht verletzt, da er „es bei den werkseitigen Sicherheitseinstellungen belassen und für den Zugang zum Router kein persönliches, ausreichend langes und sicheres Passwort vergeben habe“.

Bereits 2008 haben 40% aller Haushalte in Deutschland WLAN genutzt,⁵ daher kommt der Frage der Sorgfaltspflichten und Haftung der Anschlussinhaber eine große Bedeutung zu. Die bisherige Rechtsprechung war hierzu uneinheitlich.⁶ Bezüglich der Haftungsreichweite hat der BGH nun mit der Begrenzung auf die Störerhaftung eine klare Grenze gezogen. Die auf die Störerhaftung und die Prüfpflichten bezogenen Urteilsbestandteile und ihre Begründung verdienen jedoch eine nähere und kritische Betrachtung.

stellung durch die Instanzgerichte sowie der Umgang mit der Darlegungs- und Beweislast stehen.

Zur allgemeinen Beweislastverteilung führt der BGH aus, dass sich aus der Zuordnung der Handlung zu einer im fraglichen Zeitraum von dem Anschlussinhaber genutzten IP-Adresse eine tatsächliche Vermutung für dessen Verantwortlichkeit ergibt. Infolgedessen träfe den Anschlussinhaber eine sekundäre Darlegungslast. Im Gegensatz zu ebay-Konten komme der IP-Adresse jedoch keine vergleichbare Identifizierungsfunktion zu, daher könne der Anschlussinhaber nicht im Wege einer unwiderleglichen Vermutung behandelt werden, als habe er selbst gehandelt.⁷

Dem Anschlussinhaber aufzuerlegen, sich über die Anschlussnutzung im Rahmen einer sekundären Darlegungslast zu erklären, ist nachvollziehbar. Die Auslegung der Anforderungen an den Vortrag im Rahmen der Darlegungslast sollte jedoch nicht verdeckt zu einer Beweislastumkehr führen und sich zudem auf Vorgänge in der Sphäre des Anschlussinhabers beschränken. Der Beklagte bestritt die korrekte Ermittlung seiner IP-Adresse durch eine Ermittlungsfirma nur pauschal. Dies hielten das LG und später auch das OLG Frankfurt für unerheblich und legten den Klägerausführungen folgend die ordentliche Ermittlung der IP-Adresse zugrunde.⁸ Im Anschluss griff die oben zitierte Vermutung.



**Michael Knopp,
Jurist**

Berater bei der
Secorvo Security
Consulting GmbH.

Schwerpunkte:

Datenschutz und Rechtsfragen im
Kontext der IT-Sicherheit.

E-Mail: michael.knopp@secorvo.de

Sachverhaltsfeststellung und Beweislast

An erster Stelle sollen hierbei zunächst die bereits grob dargestellte Sachverhaltsfest-

³ Entgegen LG Hamburg, Urteil v. 26.7.2006, AZ: 308 O 407/06, CR 2007, 54.

⁴ S. Fn. 2.

⁵ Bitkom PM v. 14.9.2008, http://www.bitkom.org/de/presse/56204_54003.aspx

⁶ Strenge Anforderungen LG Hamburg s. Fn. 3., Standardmaßnahmen verlangend LG Düsseldorf, Urteil v. 16.7.2008, AZ: 12 O 195/08; OLG Düsseldorf, Beschluss v. 11.5.2009, AZ: I-20 W 146/08; LG Mannheim, Beschluss v. 25.1.2007, AZ: 7 O 65/06; gegen Haftung OLG Frankfurt a.M. s. Fn. 2

⁷ Hiermit lehnt der BGH eine Übertragung seiner Halzband-Entscheidung (BGH, Urteil v. 11.3.2009, AZ: I ZR 114/06, BGHZ 180, 134) zu Recht ab. Während Handelsplattformen nur zugangsgesichert genutzt werden können und eine vertragliche Pflicht zum Schutz der Zugangsdaten besteht, ist dies bei der Internetnutzung, für die WLAN ja nur eine zusätzliche Form der Geräteanbindung darstellt, nicht der Fall.

⁸ S. Fn. 2.

¹ BGH, Urteil v. 12.5.2010, AZ: I ZR 121/08, CR 2010, 458.

² LG Frankfurt a.M., Urteil v. 5.10.2007, AZ 2/3 O 19/07; OLG Frankfurt a.M., Urteil v. 1.7.2008, AZ: 11 U 52/07, CR 2008, 582.

Dieses Vorgehen übersieht jedoch, dass die IP-Feststellung vollständig in der Sphäre des Klägers stattfindet, so dass dem Beklagten ein genaueres Angeben von Fehlern gar nicht möglich ist. Auch der Einwand einer willkürlichen Falschbezeichnung kann nicht einfach als unqualifiziert abgeschnitten werden. Es obliegt im Gegenteil dem Kläger, seine Ermittlungsmethode, das ordnungsgemäße Funktionieren seiner Software und die tatsächliche Ermittlung der konkreten IP beweissicher zu dokumentieren und im einfachen Bestreitensfall zu beweisen.⁹ Die Darlegungslast kann sich nicht auf Sachverhaltsfeststellungen aus der Sphäre des Beweisverpflichteten beziehen, auch ist hier bei der Anwendung von § 138 ZPO Vorsicht geboten.¹⁰ Vorgelegte Logfiles haben wie jedes nicht integritätsgesicherte elektronische Dokument nur einen äußerst geringen Beweiswert.

Da für die Instanzgerichte die Anschlussnutzung aber feststand, konnte dem Vortrag des Beklagten, keinerlei Anlage sei im Betrieb gewesen, nicht mehr gefolgt werden, zumal hierfür kein Beweis angeboten wurde. Auch hier ist der Gang der Feststellungen verwunderlich. Soweit es sich nicht um eine statische IP-Adresse gehandelt hat, widerlegt bereits die Vergabe der IP-Adresse an den Beklagten das Vorbringen, auch der Router sei vollständig deaktiviert gewesen. Derartige deutlich handfestere Feststellungen oder Begründungen fehlen aber in den Sachverhaltsfeststellungen der Instanzgerichte.

Die Urlaubsabwesenheit wurde jedoch nicht bestritten und ein Betrieb in Abwesenheit nicht vorgetragen. Hier wiederum stellt sich die Frage, ob derartige Vortrag des Klägers notwendig gewesen wäre. Die Urlaubsabwesenheit ist angesichts automatisiert ausführbarer Prozesse schlicht nicht geeignet, das Unterbleiben von Handlungen zu belegen.

In den Augen der Tatsacheninstanzen blieb jedoch als einzig möglicher Ablauf die Nutzung des WLANs durch Dritte. Auf diese Weise kommt es anhand einer Kette von Vermutungen und Geständnisfiktionen nach § 138 Abs. 3 ZPO zu einer Grundsatzentscheidung über WLAN-Haftung in einem Fall, in dem der Beklagte sich

ursprünglich nicht einmal auf die unbefugte Nutzung seines WLANs berufen hat. Es wäre zu wünschen gewesen, dass der BGH sich nicht damit begnügt hätte, dem Berufungsgericht eine rechtsfehlerfreie Übernahme der Feststellungen der Vorinstanz zu bescheinigen. Es zeichnet sich derzeit eine Tendenz ab, Vorbringen und Bestreiten der Beklagten bei Filesharing-Prozessen oder ähnlich gelagerten Konstellationen von vornherein als prozesstaktisch oder als vorgeschobene Schutzbehauptungen anzusehen. Auch wenn dies in vielen Fällen zutreffen mag, kann dies keine Grundlage für die Überzeugungsbildung im Einzelfall sein, selbst dann nicht, wenn sowohl Kläger wie auch Beklagte erkennbar vorformulierte Schriftsatzteile einsetzen.¹¹

Herleitung der Prüfpflichten

Als Störer kommt nach dem BGH in Betracht, wer willentlich und adäquat kausal unter Verletzung von Prüfpflichten zur Verletzung des geschützten Rechts beiträgt. Die unberechtigte Nutzung des ungeschützten WLANs durch Dritte sei nicht gänzlich unwahrscheinlich, daher sei der ungesicherte Betrieb ein adäquat kausaler Beitrag zur Verletzungshandlung. Die jeweiligen Prüfpflichten bestimmen sich nach der Zumutbarkeit im Einzelfall. Entspricht den Prüfpflichten ein Eigeninteresse des Störers, erhöht dies die Zumutbarkeit.

Ein weiteres Zumutbarkeitskriterium ergibt sich für Privatpersonen aus den jeweiligen technischen Möglichkeiten. Der BGH führt hierzu aus, dass die Nutzung von Zugangssicherungen bei WLANs im Eigeninteresse des WLAN-Betreibers läge, da der Nutzer auch seine eigenen Daten vor unberechtigten Zugriffen schützen. Abgesehen davon, dass die Fremdnutzung des WLANs nicht zu einer Gefährdung der Daten des Betreibers führen muss,¹² ignoriert dies, dass der Betreiber unter Umständen sogar bewusst die Nutzung des WLANs durch Dritte erlauben möchte.¹³ Den berechtigt ange-

meldeten Zweifeln des OLG Frankfurt an der Adäquanz des Störungsbeitrags¹⁴ tritt der BGH darüber hinaus lediglich mit der Aussage, eine unbefugte Nutzung zu Verletzungszwecken sei nicht unwahrscheinlich, entgegen. Gegenüber der Argumentation des OLG, die empirische Nachweise dieser Wahrscheinlichkeit forderte, ist dies wenig überzeugend. Selbst wenn die Nutzung eines ungeschützten WLAN durch Dritte nicht unwahrscheinlich wäre, so bliebe die Frage, ob mit der Nutzung zu Verletzungshandlungen, insbesondere urheberrechtswidrigen Angeboten, zu rechnen ist.

Das OLG Frankfurt hat zurecht hinterfragt, ob die Störerhaftung ein legitimes Mittel ist, um das tatsächliche Problem der regelmäßig fehlschlagenden Begründung der persönlichen Zurechnung über die IP-Adresse zugunsten der Rechteinhaber zu lösen. Tatsächlich wird hier ein beweistechnisches Problem mit einer materiell-rechtlichen Haftungsausweitung gelöst, die jeden WLAN-Nutzer treffen kann.¹⁵ Auch hierzu liefert der BGH keine argumentativ überzeugende Begründung.

Eine Eingrenzung nimmt der BGH dagegen vor, indem er die permanente Aktualisierung der Netzwerktechnik oder das Aufwenden gesonderter finanzieller Mittel zur Herstellung der Sicherheit für unzumutbar erklärt.¹⁶ Daher habe der Betreiber nur die zum Erwerbszeitpunkt seines Routers marktüblichen Sicherungen wirksam einzusetzen.

Da die Werkseinstellungen des streitgegenständlichen Routers eine WPA-Verschlüsselung unter Verwendung eines werkseitig vorgegebenen individuellen 16stelligen Schlüssels für das WLAN vorsahen,¹⁷ wären diese Prüfpflichten durch den Beklagten jedoch ohne sein Zutun erfüllt gewesen. Der BGH erweitert die Prüfpflicht, indem er verlangt, anstelle der Werkseinstellungen habe der Beklagte ein persönliches, ausreichend langes und sicheres Passwort zu vergeben. Damit folgt er dem LG Frankfurt, das allerdings nur pauschal festgestellt hatte, dass zum damaligen Zeitpunkt (2006) viele Routerher-

¹¹ In dieser Weise argumentierend LG Köln, s. Fn. 10, Rn. 26 f. nach juris.

¹² So auch Schwartmann/Kocks, K&R 2010, 433 (436); Mantz, MMR 2010, 586; Nenninger, NJW 2010, 2064

¹³ Siehe etwa Initiativen für die freie WLAN-Mitnutzung, Bspw. <http://www.freifunk.net>. Zu Recht kritisch zur Annahme von Prüfpflichten und zur Wertung offener WLANs Hornung, CR 2008, 585 (586) und 2010, 461 (462), jeweils m.w.N.

¹⁴ S. Fn. 2, II. f.)

¹⁵ Ähnlich Hornung, CR 2010, 461 (462).

¹⁶ Entgegen LG Hamburg, s. Fn. 3, II. 3.

¹⁷ AVM als Hersteller der urteilsgegenständlichen Fritz!Box hat inzwischen klargestellt, dass seit 2004 individuelle Netzwerkschlüssel vergeben werden, PM unter http://www.avm.de/de/News/artikel/2010/wlan_urteil.html. Damit geht die Argumentation des BGH gerade im entschiedenen Fall fehl.

⁹ S. hierzu auch Dietrich, NJW 2006, 809 (811).

¹⁰ A.A. mit vergleichbarem Vorgehen LG Köln, Urteil v. 27.1.2010, AZ: 28 O 241/09. K&R 2010, 280. Das Bestreiten der ordentlichen IP-Adressen-Ermittlung sei rein prozesstaktisch und erfolge ins Blaue hinein, daher sei es unbeachtlich.

steller bei der Auslieferung ein einheitliches Initialpasswort für die Werkseinstellungen verwendet hätten.¹⁸

Hinsichtlich einheitlicher Initialpasswörter ist dem zuzustimmen. Bezüglich werkseitig individuell vergebener Passwörter ergibt sich jedoch kein Sicherheitsgewinn. Im Gegenteil beruhen individuelle werkseitige Passwörter auf weitaus unvorhersehbareren Zeichenkombinationen und dürften damit schwerer herauszufinden sein als häufig durchschaubare Bildungsregeln folgende Nutzerpasswörter. Dass Aufkleben des Passwortes auf die Box wäre nur unsicher, wenn diese dem unbefugten Nutzer in die Hände fiel, was doch recht unwahrscheinlich ist.

Einer Begrenzung der Prüfpflichten ist dagegen grundsätzlich zuzustimmen. Die Folgen der Beschränkung auf bereits vorhandene Sicherheitsmaßnahmen ohne Aktualisierungspflicht muten allerdings seltsam an. Der Nutzer eines mehrere Jahre alten Geräts kann sich hierdurch unter Umständen auf bekannt unwirksame Sicherungsmechanismen beschränken. Für den Besitzer eines neueren Gerätes sind die absoluten Anforderungen dagegen deutlich höher.

Zudem kann sich der Nutzer nicht darauf verlassen, dass die in seinem Router integrierten Maßnahmen ausreichen. Er hat die Marktüblichkeit beim Kauf zu prüfen. Der möglichen Überforderung der Nutzerfähigkeiten hierbei und bei der Inbetriebnahme wird vom BGH keine Rechnung getragen. Ohnehin stellt sich die Frage, weshalb die Entscheidung nicht auf den Stand der Technik zum Kaufzeitpunkt abstellt. Unberücksichtigt bleibt außerdem, dass der Neukauf eines Routers allein nicht maßgeblich ist, wenn die Mehrzahl der von ihm genutzten Empfangsgeräte neue Sicherungsmechanismen nicht unterstützt.

Eine unberechtigte Nutzung schließen die Anforderungen des BGH ohnehin nicht aus. Die WEP- oder die WPA-Verschlüsselung älterer Router ist unzureichend. Es bestehen neben dem offenen WLAN weitere Kompromittierungsmöglichkeiten, und auch Vorfälle wie das versehentliche Deaktivieren der Router-verschlüsselung durch ein fehlerhaftes Hersteller-Update lassen den Ausschluss von Dritthandeln zur Überzeugung der Gerichte regelmäßig nicht zu.¹⁹

Insgesamt betrachtet ist der Entscheidung anzumerken, dass hier versucht wird, ein bestimmtes, als materiell richtig vorausgesetztes Ergebnis zu erzielen. Wenn die Prüfpflichten jedoch mit Blick auf das Ergebnis im Einzelfall konstruiert werden, kann dies keinen Gewinn an Rechtssicherheit erzeugen.

Wäre es hingenommen worden, im konkreten Fall nicht zur Störerhaftung zu gelangen, hätte man wenigstens allgemeingültigere Prüfpflichten formulieren können. Dies würde Raum für sinnvolle Differenzierungen im Einzelfall lassen, etwa danach, ob ein vom Hersteller angebrachtes Passwort individuell ist oder ob die Nutzungsbeschränkung auf bestimmte Geräte nicht auch im Einzelfall ausreichen kann.

Auskunft zu dynamischen IP-Adressen

Versteckt im 29. Abschnitt trifft der BGH eine weitere Grundsatzentscheidung. Da die Auskunft über die Zuordnung dynamischer IP-Adressen keine weiteren Angaben zu Kommunikationsvorgängen und nur Bestandsdaten enthielten, sei § 113 TKG i.V.m. §§ 161 Abs. 1 S. 1, 163 StPO anwendbar. Damit schließt sich der BGH der wohl derzeit herrschenden Rechtsprechung an und folgt ausgerechnet den Ausführungen der Gesetzesbegründung zum für nichtig erklärten Gesetz zur Vorratsdatenspeicherung.²⁰

Auch diesem Entscheidungsteil kann nicht zugestimmt werden. Nach den von der Entscheidung zitierten Gesetzesbegründungen ist § 101 Abs. 9 und 10 UrhG in Kraft getreten und geht ausdrücklich von einer anderen (zutreffenden) systematischen Einordnung aus. § 101 Abs. 9 und 10 UrhG stellt für die Erforderlichkeit eines Richtervorbehalts und bezüglich des Eingriffs in Art. 10 GG auf die notwendige Verwendung von Verkehrsdaten (§ 3 Nr. 30 TKG) ab, nicht allein auf die Art der übermittelten Daten. Für die inhaltlich gleiche Abfrage durch die Ermittlungsbehörden kann eigentlich nichts anderes gelten. Die Einordnung dynamischer IP-Adressen unter Verkehrsdaten entspricht der bisher

weit überwiegenden Spruchpraxis und der herrschenden Literaturmeinung.²¹

Systematisch betrachtet ist es kaum zu halten, den strafprozessualen Auskunftsanspruch nach dieser Entscheidung des Gesetzgebers weiterhin auf § 113 TKG i.V.m. §§ 161, 163 StPO zu stützen. Dies wäre erst nach einer Rechtsänderung mit ausdrücklichem Wegfall des Richtervorbehalts für diese Abfrageart möglich, gegen die das Bundesverfassungsgericht keine prinzipiellen Bedenken geäußert hat.²²

Fazit

Die Wirkung der Entscheidung bleibt abzuwarten. Zu begrüßen ist die grundsätzliche Begrenzung der Haftung. Allerdings wäre die Auffassung der Vorinstanz, des OLG Frankfurt, konsequenter gewesen, das die Adäquanz des offenen WLAN-Betriebs als Tatbeitrag gänzlich verneint, solange keine Anzeichen der Fremdnutzung bestehen.²³ In der Tat ist es durchaus fraglich, ob der private Nutzer stets mit der Fremdnutzung seines Netzes zu rechtswidrigen Zwecken rechnen muss.

Auch wenn die gefundene Kompromissformel nach einem gelungenen Interessensausgleich aussieht, ist es zudem fraglich, ob dies das Ergebnis zukünftiger diesbezüglicher Rechtsstreitigkeiten sein wird. Im Gegenteil könnten sich die starren Prüfungsanforderungen als Freibrief erweisen. Der Vortrag, ein altes Gerät mit aktivierten Sicherheitsmechanismen und neu gesetztem Passwort betrieben zu haben, aber dennoch einem böswilligen Dritten zum Opfer gefallen zu sein, dürfte kaum widerlegbar sein. Somit dürften ohne kontinuierliche Verschärfungen der Prüfpflichten bei entsprechendem Vortrag sämtliche Ansprüche der Rechteinhaber regelmäßig leer laufen.

Auf grundsätzlicher Ebene stellt sich letztlich die Frage, ob die Störerhaftung und die Konstruktion von Prüfpflichten überhaupt das richtige Instrument für einen Interessensausgleich zwischen rechtskonform agierenden Internet- sowie WLAN-Nutzern und Schutzbehauptungen argwöhnenden Rechteinhabern ist.

²¹ Zuletzt m.w.N. OLG Frankfurt, Urteil v. 16.6.2010, AZ 13 U 105/07 Rn. 104 nach juris

²² BVerfG, Urteil v. 2.3.2010, AZ: 1 BvR 256/08 u. a. „Vorratsdatenspeicherung“, Rn. 261 ff.

²³ Dagegen für eine fast unbeschränkte Haftungsausweitung Stang/Hühner, GRUR 2010, 633 (637).

¹⁸ S. Fn. 2, I.

¹⁹ Siehe <http://www.heise.de/newsticker/meldung/Router-Update-schaltet-versehentlich-WLAN-Verschlueselung-ab-1028643.html>.

²⁰ BT-Drs. 16/5846, S. 26 f., 86 ff.; BVerfG, Urteil v. 2.3.2010, AZ: 1 BvR 256/08 u. a., NJW 2010, 833. Zur Problematik m.w.N. Dietrich, NJW 2006, 809; s. hierzu auch die Anmerkung von Schaefer, ZUM 2010, 699.