

Störerhaftung bei Anbieten von gegenüber unbefugtem Zugriff Dritter nicht geschütztem WLAN-Zugang

Gericht

LG Berlin

Datum

03.03.2011

Aktenzeichen

16 O 433/10

Branche/ Lebenslage

Störerhaftung, ungesichertes WLAN, Verschlüsselung, Passwörter, unverschlüsseltes WLAN, Internetanschluss, Prüfpflichten, Verhaltenspflichten

Akteure

Urheberrechtsinhaber, Internet-Anschlussinhaber, unberechtigte Dritte

Wer haftet?

Anschlussinhaber

Haftungsart

Störerhaftung, Unterlassungsanspruch

Haftungsumfang

Ablehnung eines Antrags auf Gewährung von Prozesskostenhilfe

Haftungsbegründendes Verhalten

Unterhaltung eines unverschlüsselten Internetanschlusses

Technische Umstände

Ungeschützter Internetanschluss ermöglicht Up- und Download von urheberrechtlich relevanten Dateien durch unberechtigte Dritte

Persönliche Umstände

Arglosigkeit gegenüber den Risiken rechtswidriger Internetnutzung durch unberechtigte Dritte

Möglichkeiten der Haftungsvermeidung

Ergreifen technischer Schutzmaßnahmen zur Verhinderung von Rechtsverletzungen durch Dritte

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Eine über den privaten und ungesicherten Internetanschluss des Beklagten wurde eine Film-Datei auf einer Internet-Tauschbörse der Öffentlichkeit zugänglich gemacht.

Aus dem Vortrag des Klägers, eine Urheberrechtsverletzung sei über eine IP-Adresse begangen wurde, die dem

beklagten Anschlussinhaber zu diesem Zeitpunkt zugeordnet war, ergibt sich daraus eine tatsächliche Vermutung dafür, dass dieser auch für die Rechtsverletzung verantwortlich ist. Im Rahmen seiner sekundären Darlegungslast obliegt es dem Anschlussinhaber sodann, vorzutragen, dass eine andere Person als Täter in Betracht kommt. Dazu muss der Anschlussinhaber tatsächliche Anhaltspunkte anführen, die dafür sprechen, dass die Rechtsverletzung durch eine andere Person begangen wurde

Betreibt der Inhaber eines Internetzugangs ein lokales Funknetzwerk (WLAN), ohne dieses gegen den Missbrauch durch Dritte zu sichern, haftet er als Störer (juris Rn. 5, Orientierungssatz).

Der Beklagte hat also keine Maßnahmen, die er eventuell zur Sicherung des Netzwerks vor einem Zugriff durch unberechtigte Dritte ergriffen hat, vorgetragen.

Darüber hinaus führt das Gericht aus, dass, wenn eine Film-Datei vor dem Start des DVD-Verkaufs öffentlich zugänglich gemacht wird, keine unerhebliche Rechtsverletzung i.S.d. § 97a Abs. 2 [UrhG](#) vorliege, da die Verletzungshandlung noch vor Beginn der relevanten Verwertungsphase erfolgt ist (juris Rn. 6).

ANMERKUNGEN

Das LG Berlin richtet sich im Großen und Ganzen nach der im Zusammenhang mit Sicherungsmaßnahmen gegenüber unberechtigten Dritten höchst bedeutsamen „Sommer unseres Lebens“-Rechtsprechung des Bundesgerichtshofs (BGH, Urt. v. 12.05.2010 – I ZR 121/08), die die Anforderungen konkretisiert, die an die marktübliche Sicherung eines WLAN-Routers (insbesondere die Verschlüsselung des Netzwerks) zu stellen sind.

An diesen Grundsätzen hat der Bundesgerichtshof seit jeher festgehalten (siehe zuletzt BGH, Urt. v. 24.11.2016 – I ZR 220/15 – WLAN-Schlüssel).

Der Beklagte unterhielt im vorliegenden Fall ein WLAN, das zum Zeitpunkt des Schadenseintritts nicht ausreichend gegen den Zugriff unberechtigter Dritter gesichert war. Nach der eben erwähnten Rechtsprechung des Bundesgerichtshofs hat der Störer in dem ihm zumutbaren Rahmen diejenigen erforderlichen Vorkehrungen zu treffen, um Rechtsverletzungen durch unbefugte Dritte zu verhindern. Zu beachten sind die in den Leitsätzen der Entscheidung BGH, Urt. v. 24.11.2016 – I ZR 220/15 – WLAN-Schlüssel getroffenen Feststellungen:

1. Der Inhaber eines Internetanschlusses mit WLAN-Funktion ist nach den Grundsätzen der Störerhaftung zur Prüfung verpflichtet, ob der verwendete [Router](#) über die im Zeitpunkt seines Kaufs für den privaten Bereich marktüblichen Sicherungen verfügt. Hierzu zählt der im Kaufzeitpunkt aktuelle Verschlüsselungsstandard sowie die Verwendung eines individuellen, ausreichend langen und sicheren Passworts (Festhaltung an BGH, Urteil vom 12. Mai 2010, I ZR 121/08, BGHZ 185, 330 Rn. 34 – Sommer unseres Lebens).(Rn.14)

2. Ein aus einer zufälligen 16-stelligen Ziffernfolge bestehendes, werkseitig für das Gerät individuell voreingestelltes Passwort genügt den Anforderungen an die [Passwortsicherheit](#). Sofern keine Anhaltspunkte dafür bestehen, dass das Gerät schon im Kaufzeitpunkt eine Sicherheitslücke aufwies, liegt in der Beibehaltung eines solchen werkseitig eingestellten Passworts kein Verstoß gegen die den Anschlussinhaber treffende Prüfungspflicht (Fortführung von BGH, 12. Mai 2010, I ZR 121/08, BGHZ 185, 330 Rn. 34 – Sommer unseres Lebens).(Rn.16)

Zu erwähnen bleibt darüber hinaus, dass der Betrieb eines öffentlichen WLAN künftig der Haftungsprivilegierung des § 8 Abs. 3 [TMG](#) – auch im Hinblick auf die Störerhaftung – unterfallen wird. Danach kann der Anbieter eines öffentlichen WLAN grundsätzlich weder auf Schadensersatz noch Unterlassung in Anspruch genommen werden (vgl. jedoch Möglichkeit der Netzsperrung nach § 7 Abs. 4 [TMG](#)).