Störerhaftung des Anschlussinhabers bei Unterlassen von marktüblichen Sicherungsmaßnahmen des WLAN-Routers

Gericht

BGH

Datum

12.05.2010

Aktenzeichen

12.05.2010

Branche/ Lebenslage

WLAN,Internetanschlussinhaber, ungesicherter Internetzugang, Verschlüsselung, unverschlüsseltes WLAN, Störerhaftung,Prüfpflichten

Akteure

Urheberrechteinhaber, Internet-Anschlussinhaber, unberechtigter Dritter

Wer haftet?

Internetanschlussinhaber

Haftungsart

Unterlassung, Störerhaftung

Haftungsumfang

Abmahnkosten, Anwaltskosten, Verfahrenskosten

Haftungsbegründendes Verhalten

Unterhaltung eines Internetanschlusses, der nicht ausreichend vor dem Zugriff durch unberechtigte Dritte gesichert ist

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, insbesondere ausreichende Verschlüsselung des WLAN

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Ein Nutzer hat über das WLAN des beklagten Anschlussinhabers im Wege des Filesharings (über eine Online-Tauschbörse) eine urheberrechtlich geschützte Musikdatei zum Download angeboten und diese damit öffentlich zugänglich gemacht.

Den Internetanschlussinhaber, von dessen Anschluss eine Urheberrechtsverletzung begangen wurde, trifft insofern eine sog. sekundäre Darlegungslast, wenn er geltend macht, nicht er, sondern ein Dritter habe die Rechtsverletzung begangen. Das bedeutet, dass zunächst eine tatsächliche Vermutung dafür spricht, dass derjenige, dem eine bestimmte IP-Adresse zum Tatzeitpunkt zugewiesen ist (das ist der Internetanschlussinhaber), auch für die Rechtsverletzung verantwortlich ist. Diese Vermutung kann er jedoch dadurch erschüttern, dass er Umstände darlegt und beweist, die seine Verantwortlichkeit ausschließen. Dieser sekundären Darlegungslast kam der Anschlussinhaber im vorliegenden Fall dadurch nach, dass er vortrug, zum fraglichen Zeitpunkt im Urlaub gewesen zu sein und sich sein PC in einem abgeschlossenen Büroraum befand. Damit kamen verschuldensabhängige Schadensersatzansprüche gegen den Anschlussinhaber nicht in Betracht, da dieser nicht als Täter oder Teilnehmer der Urheberrechtsverletzung in Betracht kommt (nach §§ 19a, 97 UrhG).

Der Anschlussinhaber kann unter bestimmten Voraussetzungen jedoch als Störer auf Unterlassung (und somit auch auf Zahlung etwaiger Abmahn- oder Anwaltskosten) in Anspruch genommen werden.

Als Störer haftet, *wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des geschützten Rechts beiträgt (BGH, Urt. v. 18.10.2001 – I ZR 22/99, GRUR 2002, 618, 619 = WRP 2002, 532 – Meißner Dekor I; BGH, Urt. v. 30.4.2008 – I ZR 73/05, GRUR 2008, 702 Tz. 50 = WRP 2008, 1104 – Internet-Versteigerung III). Da dieStörerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers nach der Rechtsprechung des Senats dieVerletzung von Prüfpflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen einePrüfung zuzumuten ist (BGH, Urt. v. 15.10.1998 – I ZR 120/96, GRUR 1999, 418, 419 f. = WRP 1999, 211 – Möbelklassiker; BGHZ 158, 343, 350 – Schöner Wetten; BGH, Urt. v. 9.2.2006 – I ZR 124/03, GRUR 2006, 875 Tz. 32 = WRP 2006, 1109 – Rechtsanwalts-Ranglisten)* (juris Rn. 19).

Nach Ansicht des Gerichts ist der Betrieb eines nicht oder nicht ausreichend gesicherten WLAN adäquat kausal für Urheberrechtsverletzungen, die unbekannte Dritte über den ungeschützten Anschluss begehen.

Der Anschlussinhaber verletzt seine aus dem Betrieb des WLANs resultierenden Sicherungspflichten dann, wenn gebotene Sicherheitsmaßnahmen, die einen unbefugten Gebrauch des Netzwerks durch Dritte verhindern sollen, unterbleiben. Konkret bedeutet das, dass jedenfalls die im Kaufzeitpunkt des Routers für den privaten Bereich marktüblichen Sicherungen einzusetzen sind. Diese Pflicht besteht auch bereits ab Inbetriebnahme des Anschlusses und nicht etwa erst nach Kenntnis entsprechender Nutzung durch Dritte.

ANMERKUNGEN

Im Rahmen der vorliegenden Entscheidung hat sich der Bundesgerichtshof erstmals zu der Frage der Störerhaftung des Betreibers eines nicht oder nur unzureichend verschlüsselten WLAN geäußert. Die Fragestellung war bis dahin nicht höchstrichterlich entschieden worden.

Der BGH konkretisiert insbesondere die Anforderungen, die er an die sekundäre Darlegungslast und an die marktübliche Sicherung eines WLAN-Netzwerkes stellt.

Hinsichtlich den Anforderungen an die sekundäre Darlegungslast sei auf die sog. BearShare-Rechtsprechung des Bundesgerichtshofs (BGH, Urt. v. 08.01.2014 – i ZR 169/12) verwiesen.

Bezüglich des letzteren Punktes, der marktüblichen Sicherung eines WLAN-Routers, geht der Gerichtshof davon aus, dass keine Pflicht zur fortlaufenden Anpassung an den Stand der Technik unter Aufwendung entsprechender finanzieller Mittel besteht.

Allerdings führen die Richter aus, dass eine werkseitig eingestellte WPA-Verschlüsselung des Routers (also keine damals schon mögliche WPA2-Verschlüsselung), die für die Einwahl in das jeweilige Netzwerk einen 16-stelligen

Authentifizierungsschlüssel erfordert, im Jahr 2006 nicht den für den privaten Bereich marktüblichen Sicherungen entspricht. Vielmehr hätte der Anschlussinhaber nach Inbetriebnahme des Routers ein persönliches, ausreichend langes und sicheres Passwort vergeben bzw. verwenden müssen. Offenbar erfüllte die werkseitige Standardeinstellung die damaligen Anforderungen nicht.

Zumindest heutzutage ist es jedoch üblich, dass Hersteller für jedes Gerät ab Werk individuelle Passwörter vergeben. So hat der Bundesgerichtshof insbesondere in der Fortführung der vorliegenden „Sommer unseres Lebens“-Rechtsprechung (vgl. BGH 5. Zivilsenat v. 17. Dezember 2010, V ZR 44/10; BGH 1. Zivilsenat v. 8. Januar 2014, I ZR 169/12 – BearShare; BGH 1. Zivilsenat v. 24. November 2016, I ZR 220/15 – WLAN-Schlüssel) die Anforderungen an die Passwortsicherheit zeitgemäß konkretisiert:

Danach ist der Inhaber eines Internetanschlusses 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* (BGH, Urt. v. 24.11.2016 – I ZR 220/15 – WLAN-Schlüssel, Leitsatz 1).

Dazu genügt auch ein aus einer zufälligen 16-stelligen Ziffernfolge bestehendes, werkseitig für das Gerät individuell voreingestelltes Passwort 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*(BGH, Urt. v. 24.11.2016 – I ZR 220/15 – WLAN-Schlüssel, Leitsatz 2).

Zu erwähnen bleibt, 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 Netzsperre nach § 7 Abs. 4 TMG).