

Keine Haftung bei Nutzung des werksseitig vorgegebenen Router-Passworts wegen fehlender Verpflichtung zur Einstellung eines persönlichen Passworts

Gericht

AG Hamburg

Datum

09.01.2015

Aktenzeichen

36a C 40/14

Branche/ Lebenslage

Störerhaftung, WLAN, Internetanschlusshaber, Verschlüsselung, Urheberrechtsverletzung, Schutzmaßnahmen, ungesicherter Internetzugang, Router, Werkseinstellungen, Passwort

Akteure

Urheberrechtsinhaber, Internetanschlusshaber, unberechtigte Dritte

Wer haftet?

Anschlusshaber, im konkreten Fall (-)

Haftungsart

Störerhaftung, Unterlassungsanspruch (-)

Haftungsumfang

Im konkreten Fall (-), sonst regelmäßig Abmahnkosten, Verfahrenskosten

Haftungsbegründendes Verhalten

Im konkreten Fall (-), sonst Unterhaltung eines nicht ausreichend verschlüsselten Internetanschlusses

Technische Umstände

Im konkreten Fall (-), sonst ungeschützter Internetanschluss ermöglicht Up- und Download von urheberrechtlich relevanten Dateien durch unberechtigte Dritte

Persönliche Umstände

Im konkreten Fall (-), sonst 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

Über den Internetanschluss der Beklagten wurde eine urheberrechtlich geschützte (Film-)Datei via Filesharing zum Download angeboten. Die Urheberrechtsverletzung wurde dabei nach den Feststellungen des Gerichts unstreitig von einem unberechtigten und unbekanntem Dritten über das nur unsicher verschlüsselte [Netzwerk](#) der Beklagten begangen.

Der Inhaber eines Internetanschlusses hat grundsätzlich für die durch Dritte über seinen Zugang begangenen Urheberrechtsverletzungen – nach den Regeln der Störerhaftung – einzustehen.

Als Störer kann 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 die rechtswidrige Beeinträchtigung nicht selbst vorgenommen haben, setzt die Haftung des Störers nach der Rechtsprechung des Bundesgerichtshofs allerdings die Verletzung zumutbarer Verhaltenspflichten in Form von Prüfpflichten voraus. Ob und inwieweit dem Störer eine Prüfung zuzumuten ist, richtet sich nach den jeweiligen Umständen des Einzelfalls.

Die Störerhaftung kann auch dadurch begründet werden, dass ein Internetanschluss nicht ausreichend vor dem Zugriff durch unberechtigte Dritte gesichert ist (vgl. dazu BGH, Urt. v. 12.05.2010 – I ZR 121/08 – Sommer unseres Lebens). Den Anschlussinhaber trifft hierbei eine sog. sekundäre Darlegungslast. Um dieser zu genügen hat der Beklagte vorzutragen, um was für einen Anschluss es sich handelte, ob ein WLAN eingerichtet war, wann der Anschluss eingerichtet und welcher Routertyp verwendet wurde und mit welcher Sicherung der Anschluss im Zeitpunkt der Rechtsverletzung geschützt war. Dazu gehört auch die genaue Angabe der Verschlüsselungstechnik, des konkret verwendeten Passworts und seiner Generierung, insbesondere, ob es sich um ein individuell gewähltes Passwort handelt. Der Anschlussinhaber hat die genannten Punkte im vorliegenden Fall vorgetragen.

Hinzu kommt vorliegend, dass das werkseitige Verfahren zur Generierung des WPA2-Schlüssels nicht hinreichend sicher war, so dass dieser mit überschaubarem Aufwand „geknackt“ und der Schutzmechanismus so überwunden werden konnte.

Nach Ansicht des Amtsgerichts hat ein Internetanschlussinhaber jedoch für eine ihm nicht bekannte Sicherheitslücke aufgrund einer nicht hinreichend sicheren werkseitig vergebenen WPA2-Verschlüsselung eines WLAN-Routers nicht einzustehen (juris Rn. 30, 31).

Darüber hinaus ist bei einem WLAN-Router, der werkseitig mit einem individuellen Authentifizierungsschlüssel ausgeliefert wird, eine individuelle Änderung des vergebenen WPA2-Schlüssels nicht erforderlich (juris Rn. 37, 38, 39).

ANMERKUNGEN

Das AG Hamburg hat mit seinem Urteil v. 09.01.2015 als Vorinstanz den Grundstein für die „WLAN-Schlüssel“-Entscheidung des Bundesgerichtshofs gelegt (BGH, Urt. v. 24.11.2016 – I ZR 220/15 – WLAN-Schlüssel) .

In der genannten Entscheidung hat der BGH die Anforderungen an WLAN-Passwörter konkretisiert und die in der „Sommer unseres Lebens“-Rechtsprechung (BGH, Urt. v. 12.05.2010 – I ZR 121/08) getroffenen Vorgaben teilweise modifiziert, in deren Rahmen er noch verlangte, dass WLAN-Router ein individuelles Passwort durch den Anschlussinhaber erhalten müssten und der Nutzer nicht auf die werkseitig eingestellten Passwörter vertrauen dürfe.

In der „WLAN-Schlüssel“-Entscheidung hat der Bundesgerichtshof jedoch festgestellt, dass die mittlerweile mit einer WPA2-Verschlüsselung versehenen und werkseitig eingestellten Passwörter so individuell sind, dass sie den Anforderungen der „Sommer unseres Lebens“-Rechtsprechung genügen:

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) (juris Rn. 16, Leitsatz 1).

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) (juris Rn. 16, Leitsatz 2).

Zu erwähnen bleibt weiterhin, 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](#)).