

Verpflichtung eines privaten Internetanschlusshabers mit WLAN-Funktion zur Prüfung des Verschlüsselungsstandards und Passworts sowie des Routers auf marktübliche Sicherung im Kaufzeitpunkt; Erfüllung der Anforderungen an die Passwortsicherheit bei 16-stelligem, zufälligem und individuell voreingestelltem Passwort; keine Änderungspflicht des werksseitigen Passworts ohne Hinweis auf Sicherheitslücke im Kaufzeitpunkt

Gericht

BGH

Datum

24.11.2016

Aktenzeichen

I ZR 220/15

Branche/ Lebenslage

Passwort, Zugangssicherung, WLAN, Internetanschlusshaber, Verschlüsselung, Verschlüsselungsstandard, Router, Passwortschutz, Passwortsicherheit, WLAN-Schlüssel, marktübliche Sicherung, Werkseinstellung, Werkseinstellungen, Störerhaftung, WPA2-Standard

Akteure

Rechteinhaber, Internetanschlusshaber, unberechtigter Dritter

Wer haftet?

Grundsätzlich Internetanschlusshaber, nicht jedoch, wenn der WLAN-Router über die im Zeitpunkt seines Kaufs für den privaten Bereich marktüblichen Sicherungen verfügt und der Anschlusshaber dies überprüft hat

Haftungsart

Grundsätzlich Störerhaftung, Unterlassung, hier (-)

Haftungsumfang

Grundsätzlich Abmahnkosten / Anwaltskosten, Verfahrenskosten, hier (-)

Haftungsbegründendes Verhalten

bloße Unterhaltung eines Internetanschlusses und unzureichende Sicherung gegenüber dem Zugriff durch Dritte, hier (-)

Technische Umstände

Internetanschluss ermöglicht Up- und Download von urheberrechtlich relevanten Daten

Persönliche Umstände

Arglosigkeit gegenüber den Risiken rechtswidriger Internetnutzung durch Dritte - hier (-)

Möglichkeiten der Haftungsvermeidung

Verwendung eines WLAN-Routers, der den im Kaufzeitpunkt marktüblichen Sicherungen genügt und Überprüfung des Routers hierauf

Zitate, Zusammenfassende Würdigung, Strategien zur Haftungsvermeidung

Über den Internetanschluss der Beklagten wurden urheberrechtliche geschützte Film-Dateien via Filesharing hochgeladen und dadurch der Öffentlichkeit zugänglich gemacht.

Unstreitig ist, dass die Urheberrechtsverletzung durch einen unbekanntem und unberechtigten Dritten über das [Netzwerk](#) der Beklagten vorgenommen worden ist.

Die Rechteinhaberin beabsichtigt, die Anschlussinhaberin auf Erstattung von Abmahnkosten im Rahmen der Störerhaftung in Anspruch zu nehmen.

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. Dabei kann als Beitrag auch die Unterstützung oder Ausnutzung der Handlung eines eigenverantwortlich handelnden Dritten genügen, sofern der in Anspruch Genommene die rechtliche und tatsächliche Möglichkeit zur Verhinderung dieser Handlung hatte. Da die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die weder als Täter noch als Teilnehmer für die begangene Urheberrechtsverletzung in Anspruch genommen werden können, setzt die Haftung als Störer nach der Rechtsprechung des Senats die Verletzung zumutbarer Verhaltenspflichten, insbesondere von Prüfpflichten voraus. Ob und inwieweit dem als Störer in Anspruch Genommenen eine Verhinderung der Verletzungshandlung des Dritten zuzumuten ist, richtet sich nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung seiner Funktion und Aufgabenstellung sowie mit Blick auf die Eigenverantwortung desjenigen, der die rechtswidrige Beeinträchtigung selbst unmittelbar vorgenommen hat (BGH, Urteil vom 12. Mai 2010 - I ZR 121/08, BGHZ 185, 330 Rn. 19 – Sommer unseres Lebens; BGHZ 200, 76 Rn. 22 – BearShare; BGH, Urteil vom 26. November 2015 - I ZR 174/14, GRUR 2016, 268 Rn. 21 = WRP 2016, 341 – Störerhaftung des Access-Providers; Urteil vom 12. Mai 2016 - I ZR 86/15, GRUR 2016, 1289 Rn. 11 = WRP 2016, 1522 – Silver Linings Playbook) (juris Rn. 11).

Diese Voraussetzungen sind jedoch nicht gegeben. So führt der BGH aus:

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 (juris Rn.14).

Hinsichtlich des Verschlüsselungsstandards stellt der Gerichtshof fest:

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 (juris Rn. 16).

ANMERKUNGEN

Mit der vorliegenden Entscheidung hält der Bundesgerichtshof an seiner „Sommer unseres Lebens“-Rechtsprechung fest und konkretisiert diese weiter (BGH, Urt. v. 12.05.2010 – I ZR 121/08). Hielt er es damals noch für notwendig, ein selbst gewähltes, individualisiertes Passwort durch den Anschlussinhaber einzurichten, wird das mittlerweile in den meisten Fällen nicht mehr notwendig sein. Voraussetzung dafür ist, dass es sich bei dem werkseitig durch den Hersteller eingestellten Passwort um einen ausreichend individuellen, nur dem Anschlussinhaber bekannten, Code handelt.

So besteht bei dem Einsatz von WLAN-Routern zwar nach wie vor eine Prüfpflicht des Anschlussinhabers. Diese beschränkt sich jedoch darauf, dass das Netzgerät den zum Kaufzeitpunkt marktüblichen Sicherungen genügen muss. Bei einem aus einer zufälligen 16-stelligen Ziffernfolge bestehenden, werkseitig für das Gerät individuell voreingestellten Passwort – bzw. einem Router mit dem Verschlüsselungsstandard WPA2 – ist dies nach Ansicht des BGH der Fall. Es besteht somit keine Änderungspflicht des werksseitigen Passworts ohne Hinweis auf eine Sicherheitslücke im Kaufzeitpunkt.

Daneben äußert sich der Gerichtshof zur sekundären Darlegungslast des Anschlussinhabers:

So obliegt diesem eine sekundäre Darlegungslast zu den von ihm bei der Inbetriebnahme des Routers getroffenen Sicherheitsvorkehrungen, der er durch Angabe des Routertyps und des Passworts genügt und erklärt, dass es sich bei diesem um einen individuell und nur einmalig vergebenen Code handelt. Für die Behauptung, es habe sich um ein für eine Vielzahl von Geräten voreingestelltes Passwort gehandelt, ist sodann der Kläger/Rechteinhaber darlegungs- und beweispflichtig (juris Rn. 19).