„Offenes WLAN als Super Gau für Ermittlungsbehörden?“

Das Complianceberater.Team hat sich bereits in der Vergangenheit mit der Thematik der Beseitigung der sogenannten Störerhaftung bei offenen WLAN-Hotspots beschäftigt. Hierbei lag bislang jedoch die Erörterung aus zivilrechtlicher Sicht im Fokus.

Hintergrund dieser Störerhaftung war, dass z.B. die Nutzung eines privaten WLAN durch Dritte den Betreiber des WLAN mit in die Haftung nahm.

Anders hingegen für sogenannte Access Provider. Hier findet sich in § 8 des Telemediengesetzes (TMG) für diese eine Haftungsfreistellung. Der Begriff des Access Providers kann mit Zugangsvermittler übersetzt werden. Diese gewerblichen Zugangsvermittler werden, unter bestimmten Voraussetzungen, von einer Haftung für das Verhalten der Nutzer freigestellt. In der Rechtsprechung war es bisweilen höchst umstritten, ob auch der Betreiber eines WLAN-Netzwerkes unter den Begriff des Access Providers einzuordnen ist und er demnach auch von der Haftungsprivilegierung Gebrauch machen kann. Dieser Zwist in der Rechtsprechung führte letztendlich zur Vorlage der Frage beim europäischen Gerichtshof (EuGH).

Durch die nun geplante Reform des Telemediengesetzes soll die sogenannte Störerhaftung für private und nebengewerbliche Betreiber eines WLAN-Hotspots beseitigt werden. Dies hätte zur Folge, dass solche Betreiber ebenfalls zukünftig für die Rechtsverletzungen, welche durch die Nutzer des Netzwerkes begangen werden, nicht mehr zur Verantwortung gezogen werden könnten. Die gewünschte Folge der Änderung des Telemediengesetzes wird sicherlich sein, dass offene WLAN-Hotspots künftig möglichst flächendeckend angeboten werden können.

In diesem Zusammenhang ist anzumerken, dass eine technische Entwicklung stets Fluch und Segen zugleich sein kann, je nachdem aus welcher Perspektive man diese Entwicklung betrachtet. Im Falle der offenen WLAN-Hotspots stellt die geplante Gesetzesänderung sicherlich für die Nutzer dieser Hotspots ein Segen dar. Fraglich ist in diesem Zusammenhang jedoch, ob diese Aussage auch auf die deutschen Strafverfolgungsbehörden zutrifft.

Die Probleme die sich für die Strafverfolgungsbehörden zukünftig in diesem Zusammenhang stellen könnten, sollen an einem kleinen Beispiel illustriert werden.

Person A hat sich zum Ziel gesetzt, mithilfe des Internets diverse kinderpornographische Bilder mit anderen Personen zu teilen. Bisweilen liefen die hieran beteiligten Personen Gefahr, dass ihre jeweils genutzte IP-Adresse des Internetproviders bei diesem Vorhaben registriert wurde. Die deutschen Strafverfolgungsbehörden haben dann über ein entsprechendes Auskunftsersuchen im Nachgang bei dem jeweiligen Internetprovider angefragt, welche Person zu einem bestimmten Zeitpunkt die registrierte IP-Adresse genutzt hat und erhielten auf diesem Weg die personenbezogenen Daten.

Nunmehr hat die kabelnetzbetreibende Firma Unitymedia angekündigt, dass diese bis Ende des Jahres insgesamt 1,5 Millionen WLAN-Hotspots anbieten möchte. Dies kann jedoch nur dadurch erreicht werden, dass bei jedem WLAN-Router eines jeden Unitymedia Kunden automatisch ein separates WLAN-Signal aktiviert wird, sofern der Kunde nicht innerhalb einer bestimmten Frist dieser weitergehenden Nutzung seines Anschlusses wiederspricht. Der dann bestehende offene WLAN-Hotspot wird für jedermann zugänglich sein.

Nun stellen sich dem kritischen Leser jedoch gleich mehrere Fragen. Zum einen, ob die eigenen Daten des Kunden bzw. die über das Heimnetzwerk zur Verfügung stehenden Daten dieses Kunden auch weiterhin sicher sind, da diese beiden Netzwerke auf dem gleichen WLAN-Router wieder zusammengeführt werden. Somit dürfte es potentiellen Hackern mit relativ wenig Aufwand möglich sein, die Netzwerke mittels einer Bridge zu verbinden und somit letztendlich auch an die über das private Netzwerk gesendeten Daten zu gelangen.

Weiterhin stellt sich die Frage, ob die Nutzer des offenen WLAN-Netzwerkes sich einer Authentifizierung unterziehen müssen, da die IP-Adressen ja weiterhin auf den Namen des WLAN Betreibers registriert werden, also dessen personenbezogene Daten bei einer Anfrage der Strafverfolgungsbehörden vom Provider heraus gegeben werden würden.

Nur bei einer Authentifizierung könnte eine spätere Identifizierung des Täters möglich sein, sofern das System neben den konkreten Nutzerdaten auch Zeitpunkt und Dauer registriert.

Sofern man davon ausgehen kann, dass es sich bei dieser Möglichkeit, die der Diensteanbieter hier einrichten will, tatsächlich um eine Variante des offenen WLANs handelt und keine Identifizierung bzw. Authentifizierung des Nutzers nötig ist, stellt sich die Frage, welche Daten in der sogenannten Log-Datei des jeweiligen Routers gespeichert werden, um im Nachgang eine Ermittlung von Rechtsverstößen und Identifizierung des Täters vornehmen zu können.

Am Beispiel des Routers FRITZ!Box lässt sich festhalten, dass standardmäßig bereits eine gewisse Protokollierung über die An-und Abmeldungen der mit dem Netzwerk verbundenen Geräte möglich ist. Diese Protokolldaten kann der Administrator des Routers auch per E-Mail an eine beliebige E-Mailadresse versenden und dementsprechend vorhalten. Es wäre also möglich, auf eine Anfrage einer Strafverfolgungsbehörde hin, diese Daten zur Verfügung zu stellen.

Darüber hinaus kann in dem oben genannte Router die Internetanwendung auf das Surfen und Mailen beschränkt werden, so dass der Download oder Upload von Daten wohl unterbleibt.

Es ist weiterhin möglich und auch sinnvoll die Kommunikation der mit dem Netzwerk verbundenen Geräte untereinander auszuschließen. Diese Einstellung dient letztendlich dem Schutz der Nutzer des Netzwerkes, da andernfalls jederzeit ein Zugriff auf die im Netzwerk aktiven Geräte möglich wäre.

Außerdem wird standardmäßig protokolliert, welche Geräte mit dem Netzwerk verbunden sind bzw. waren. Somit wird letztendlich auch die sogenannte Mac Adresse bzw. physische Adresse der verwendeten Geräte protokolliert und bei Bedarf in den Log-Dateien gespeichert. Die Macadresse bzw. physische Adresse des Geräts kann als digitaler Fingerabdruck des jeweils genutzten Geräts verstanden werden. Über diese Adresse können Rückschlüsse auf den Hersteller des Geräts bzw. der verbauten Netzwerkkarte geschlossen werden. Sodas der Hersteller in der Regel über die Seriennummer des Geräts den Erstkäufer ermitteln kann. Sofern der Täter nun nicht der Erstkäufer wäre, da das Gerät zwischenzeitlich, im schlimmsten Falle ohne Beleg, veräußert wurde, könnte sich demnach anschließend die Spur des Täters verlieren.

Jedoch ist es bereits jetzt mit diversen im Internet erhältlichen Softwarelösungen möglich, die Mac-Adresse des verwendeten Geräts ohne größeren Aufwand zu manipulieren und somit die Ermittlungen enorm zu erschweren.

Darüber hinaus wird bereits jetzt bei allen handelsüblichen WLAN-Routern ein Ereignisprotokoll erstellt. Hierbei bietet sich optional die Möglichkeit die erfolgten An- und Abmeldungen bzw. deren Zeitpunkte ebenfalls zu protokollieren. Somit wäre es letztendlich möglich den Tatzeitraum und die verwandten Geräte einzugrenzen. Jedoch wird auch in diesem Fall lediglich protokolliert, welches Gerät sich mit welcher

Mac-Adresse und mit welcher durch den WLAN-Router zur Verfügung gestellten IP-Adresse an- und abgemeldet hat.

Darüber hinaus bietet beispielsweise der WLAN-Router der Firma FRITZ!Box über einen versteckten Menüpunkt die Möglichkeit, dass alle über diese Netzwerkverbindung übertragenen Datenpakete in dem sogenannten Wireshark-Format mitgeschnitten werden.

Mithilfe der hierdurch gesammelten Daten, wäre es den Strafverfolgungsbehörden, aber auch hierauf spezialisierten Unternehmen, wie dem Teammitglied desmen des Complianceberater.Teams der CARMAO GmbH, im Nachgang mit speziellen gerichtsverwertbaren Softwarelösungen möglich, nachzuvollziehen welches Gerät bzw. der User was auf einer beliebigen Internetseite gemacht hat. In diesem Zusammenhang stellt sich zudem auch unter dem Gesichtspunkt des Datenschutzes die Frage, ob der Nutzer über diese Tatsache, dass Datenpakete mitgeschnitten werden, ausdrücklich belehrt werden müsste und ob nicht der Netzwerkbetreiber zwangsläufig auch das Einverständnis des jeweiligen Nutzers einholen müsste.

In dem vorgenannten Beispielfall würde die fiktive Person A sicherlich davon Abstand nehmen, über den eigenen Netzwerkanschluss und somit mit der eigenen IP-Adresse die Dokumente hochzuladen und mit anderen zu teilen. Stattdessen wird sie beispielsweise den von einem Nachbarn bereitgestellten Hotspot für ihr Vorhaben verwenden.

In der Begründung des Gesetzesentwurfes wird in diesem Zusammenhang ausgeführt, dass eine Zunahme von Urheberrechtsverletzungen nicht zu erwarten wären, da die Bandbreite von öffentlichen WLAN-Hotspots hierfür gerade nicht ausgelegt sei. Zudem sei es technisch möglich die Bandbreite der öffentlichen WLAN-Hotspots dahingehend zu regulieren, dass beispielsweise ein hochladen von großvolumige Dateien erst gar nicht attraktiv würde. Weiterhin heißt es in der Begründung des Gesetzesentwurfes, dass durch die Verbreitung von öffentlichen WLAN-Hotspots keine nachteiligen Effekte auf die Strafverfolgung zu erwarten seien.

Fazit:

Es bleibt sicherlich abzuwarten, wie die geplante Gesetzesreform, möglichst ohne eine Einschränkung für die Nutzer von WLAN-Hotspots umgesetzt werden kann und

gleichzeitig gewährleistet wird, dass die Strafverfolgungsbehörden in der Lage sein werden eventuelle Rechtsverletzungen nicht nur aufzudecken, sondern letztendlich auch nach Ermittlung des Täters zu ahnden.

Denn sicherlich lässt beispielsweise die Mac Adresse eines Apple Produkts Rückschlüsse auf die Firma Apple zu, sodass die Strafverfolgungsbehörden über den Hersteller eventuell an den Kunden mit der entsprechenden Mac Adresse gelangen könnten, dennoch wird ein solcher Rückschluss beispielsweise mit einem Laptop bereits um einiges schwieriger werden, da hier in der Regel nur der Rückschluss auf die in dem Laptop verbaute Netzwerkkarte möglich ist. Weitere Analysen bzw. Ermittlungen bezüglich des zum Zeitpunkt am Laptop angemeldeten Benutzers sind, unter Hinzuziehung spezieller forensischer Tools, für spezialisierte Unternehmen, wie die CARMAO GmbH, zur Unterstützung in Ermittlungsverfahren möglich.

Nach dem Dafürhalten des Complianceberater.Teams wird zukünftig der Dokumentation des Nutzungsverhaltens an dem jeweiligen WLAN-Hotspot mithilfe der Log-Datei eine entscheidende Bedeutung bei Ermittlungen der Strafverfolgungsbehörden zukommen.

Jeder Interessierte, der künftig von der Möglichkeit Gebrauch machen will, einen offenen WLAN-Hotspot bereit zu stellen, sollte sich zumindest mit den technischen Möglichkeiten seines Routers in Bezug auf die Speicherung von Nutzerdaten (Nutzungszeitpunkt und – -dauer, MAC-Adresse) die Einschränkung der Nutzungsmöglichkeiten (Surfen & Mailen), aber auch des Mitschnitts von Datenpaketen informieren, bevor er ein solches Angebot freigibt. Ansonsten läuft er Gefahr immer noch der erste Ansprechpartner für Strafverfolgungsbehörden zu sein, wenn sein Anschluss missbraucht wird.

Sollten Sie weitere rechtliche Fragen zu diesem Themenkomplex haben, wenden Sie sich bitte an:

Rechtsanwalt Kai Schnabel

Friedrich-Ebert Straße 31-33

67574 Osthofen

Tel.: 06242 / 912 88 70

Fax: 06242 / 912 88 71

E-Mail: kschnabel@complianceberater.team

Web: www.complianceberater.team

Sollten Sie weitere technische Fragen zu diesem Themenkomplex haben, wenden Sie sich bitte an:

CARMAO GmbH

Head of Digital Forensic & Cyber Security

Björn Bausch

Fahrgasse 5

65549 Limburg

Tel.: 06431 / 28 333 37

Fax: 06431 / 28 333 31

E-Mail: bjoern.bausch@carmao.de oder forensik@carmao.de

Web: www.complianceberater.team oder www.carmao.de

Sollten Sie weitere Fragen zum COMPLIANCEBERATER.TEAM haben, wenden Sie sich bitte an:

Rechtsanwalt Jürgen Möthrath

Carl-Ulrich-Straße 3

67547 Worms

Tel: 06241 / 93800-0

Fax: 06241 / 93800-8

E-Mail: jmoethrath@complianceberater.team

Web: www.complianceberater.team