RECHTSANWALTSKANZLEI RASSI WARAI
Rechtsanwälte | Mediator | anerkannte Gütestelle

Kanzlei Rassi Warai, Viktoriastr. 36, 32423 Minden

OctoGate IT Security Systems GmbH
Technologiepark 32
33100 Paderborn

Rechtsanwalt, Mediator und anerkannte Gütestelle
iSd. § 794 Abs. 1 S. 1 ZPO Markus Rassi Warai
E-Mail: ra@warai.de

Rechtsanwalt *(*) im Angestelltenverhältnis*,
Datenschutzbeauftragter (TÜV) Niels Luckner
E-Mail: nl@warai.de

Tel 0571 / 951 947 58
Fax 0571 / 385 65 76

Internet www.rechtsanwaltskanzlei-warai.de

Kürzel des Sachbearbeiters: *mrw*
Bei Anfragen bitte angeben.

Unser Zeichen: ch-IV-15113657/mrw
Ihr Zeichen :

Minden, den 13.11.2015

OctoGate IT Security Systems GmbH | Stellungnahme WLAN-Betreiberhaftung

Sehr geehrte Damen und Herren,

in der vorstehenden Beratungsangelegenheit übersende ich Ihnen anliegende Stellungnahme zur Kenntnisnahme und weiteren Verwendung.

A. Begebenheit vor Ort

Auftragsgegenständlich wird der Betrieb eines WLAN (Wireless Local Area Network) Routers mit integriertem Modem an einem Breitband-Internetanschluss im Bereich der Sporthalle der weiterführenden Schule der Stadt in Erwägung gezogen. Als Verantwortungsträger ist - ausweislich des Internetauftritts des Kollegs - die Stadt als solcher benannt (*). Der Router (*) ist an eine Hardware-Firewall des Her-

stellers Octogate vom Typ „Rack Solution 100“ mit der aktuellen vorinstallierten Octogate Firewall Software v.3.0.19 angeschlossen (*). Bezweckt wird die Eröffnung eines Zugangs ins World Wide Web für eine bestimmbare Personenmehrheit (mitunter unterschiedlicher Staatsangehörigkeiten und divergierender kultureller Auffassungen) im unmittelbaren Umkreis des drahtlosen lokalen Netzwerks.

*) Nicht vom Auftrag umfasst war die Prüfung der Aktualität der Angaben in der Anbieterkennzeichnung der weiterführenden Schule (obgleich hier etwa noch ein Hinweis auf nicht mehr bestehende Rechtsvorschriften getroffen wird, ist von der Richtigkeit der dort getroffenen Angaben ausgegangen worden).
*) Der zum Einsatz gestellte Router ist dem Unterzeichner nicht bekannt gemacht worden. Es wird insoweit von einer zeitgemäßen und einsatzkonformen Peripherie ausgegangen.
*) Eine Vor-Ort-Sichtung der Begebenheiten durch den Unterzeichner erfolgte nicht. Die vor- und nachstehende Einschätzung basiert auf den Angaben des Auftraggebers sowie den Angaben aus dem Octogate Handbuch v. 5.04.

B. Gefährdungspotential

Betreiberseits wurde die Befürchtung einer Rechtsunsicherheit im Hinblick auf die Haftung des WLAN-Betreibers für etwaige rechtswidrige Handlungen der WLAN-Nutzer unter Verwendung des bereitgestellten Internetzugangs geäußert.

Tatsächlich sind Konfrontationen von WLAN-Betreibern mit Urheberrechtsverletzungen, Eingriffen in Persönlichkeitsrechte u.a. Verfehlungen, die unter der Verwendung eines Internetanschlusses begangen werden können, praxisbekannt. Hierbei stellen Inanspruchnahmen aufgrund von Verstößen gegen Rechte auf den Schutz geistigen Eigentums mit großem Abstand die häufigste Konfrontation dar.

C. Generelle Haftungsaspekte

Neben der Haftung des Initiatoren einer rechtswidrigen Verhaltensweise, der sogenannten „Täterhaftung“, ist auch eine Haftung eines Internetanschlussinhabers und WLAN-Betreibers für rechtswidrige Aktivitäten über das unterhaltene Netzwerk anerkannt. Man spricht insoweit von der sogenannten „Störerhaftung“, die aus einer steten Rechtsprechungsentwicklung der vergangenen Jahre hervorging. Begründet wird diese Haftungsmaxime damit, dass der WLAN-Betreiber durch die Unterhaltung seines Netzwerkes eine Gefahrenquelle für die Rechte Dritter geschaffen hat.

Dessen ungeachtet besteht die Haftung eines „Störers“ nicht uneingeschränkt. Vielmehr setzt sie die Verletzung von Prüfungspflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem „Störer“ nach den jeweiligen Umständen eine Prüfung zuzumuten ist (BGH, Urteil vom 11.03.2004, I ZR 304/01).

D. WLAN-Betreiberhaftung - Kurzüberblick über die aktuelle Rechtslage

Um die in dieser Hinsicht bestehenden „jeweiligen Umstände“ und damit den Prüfungsrahmen bestimmen zu können, differenziert eine Rechtsauffassung (BGH, Urteil vom 12.05.2010, I ZR 121/08), die u.a. Stütze in der Bundesregierung findet, zwischen dem rein privaten und dem gewerblichen WLAN-Betrieb.

Privaten WLAN-Betreibern obliegt es, das Netzwerk vor unberechtigten Zugriffen von außen zu schützen. Berechtigten Zugriffen hat grundsätzlich eine Identitätskontrolle des Nutzers sowie dessen verständliche Aufklärung über die unerwünschten und rechtswidrigen Aktivitäten vorauszugehen. Gegenüber bestimmten Nutzerkreisen (z.B. entwicklungsgehemmten Personen oder - in der Vergangenheit bereits einschlägig auffällig gewordenen - Internetnutzern) besteht ferner eine Kontrollpflicht im Hinblick auf die Einhaltung der Aufklärungsmaßgaben seitens des WLAN-Betreibers (BGH, Urteil vom 15.11.2012, I ZR 74/12).

Im Hinblick auf die Fragen der Störerhaftung im Zusammenhang mit dem kommerziellen Betrieb und/oder dem Betrieb eines drahtlosen lokalen Netzwerkes durch öffentliche Einrichtungen ermangelt es an einer klärenden höchstrichterlichen Entscheidung. Tendenzen in der Jurisprudenz ziehen eine Übertragbarkeit des Haftungsprivilegs für Provider aus §§ 7 ff. TMG auf gewerblich betriebene WLAN-Netze bereits heute - als vertretbar - in Erwägung. Der gesetzgeberische Wille manifestiere sich dahingehend in der im TMG gewählten Begrifflichkeit „Diensteanbieter“ (Martini in: Informations- und Medienrecht, 2014, TMG § 2 Rn 4 f.), die eine bewusst weite Bestimmung erfahre. Begründet wird diese Auffassung der Haftungsprivilegierung damit, dass man es als ungebührlich erachte, einem gewerblichen WLAN-Betreiber das uneingeschränkte Haftungsrisiko für eine immense Informationsflut aufzuerlegen. Für diese anlassungebunden und uneingeschränkt haften zu müssen, würde in einem - praktisch nicht einzuhaltenden - Kontrollpflichtengebot münden. Spricht man geschäftlichen WLAN-Betreibern und/oder öffentlichen Einrichtungen als Betreibern von kabellosen lokalen Netzwerken das Haftungsprivileg zu, so unterstünden sie getreu §§ 7 ff. TMG keiner Kontroll- oder Überwachungspflicht sowie einer nur eingeschränkten Verantwortlichkeit im Hinblick auf die übermittelten Informationen.

E. WLAN-Betreiberhaftung - Kurzüberblick über etwaige künftige Rechtsentwicklungen

Gesetzgebungsbestrebungen auf Bundesregierungsebene weisen eine Entwicklung mit Tendenzen zur Ausschöpfung der gesellschaftlichen und wirtschaftlichen Potenziale von WLAN-Funknetzen auf. Erwägungsgetreu soll eine Verfügbarkeit des Zugangs zum mobilen Internet über WLAN künftig flächendeckend gewährleistet sein. Die konzeptionellen Überlegungen setzen bei der Umsetzung in öffentlichen und privaten Einrichtungen an und verfolgen die Zielsetzung, diesen fortan das unentgeltliche aber rechtssichere Anbieten des unterhaltenen WLAN zu eröffnen. Zur Verwirklichung sei eine Änderung des Telemediengesetzes erforderlich. Der Referentenentwurf zum 2. Telemedienänderungsgesetz vom 11.03.2015 sieht explizit u.a. eine Änderung des aktuellen § 8 TMG vor.

Nach § 8 Abs. 4 S. 1 TMGÄndG sollen nunmehr nicht nur gewerbliche WLAN-Betreiber oder öffentliche Einrichtungen einer Haftungsprivilegierung unterstehen. Vielmehr sollen auch private WLAN-Betreiber der Störerhaftung entzogen werden, soweit sie „zumutbare Maßnahmen“ ergreifen, um eine Rechtsverletzung durch den Netzwerknutzer zu verhindern. Die Identitätskontrolle im Hinblick auf den Netzwerknutzer soll entfallen. Es soll aber eine Zusicherung seitens des Nutzers eingeholt werden, dass dieser keine Rechtsverletzungen über den WLAN-Anschluss begehen wird. Im Gegensatz zur derzeitigen Aufklärungspflicht genügt es allerdings diese in - zu bestätigenden - Nutzungsbedingungen unterzubringen.

G. Pflichtenbereiche des WLAN-Betreibers

Übertragen auf die zur Stellungnahme vorgelegten Fragen hinsichtlich der Pflichtenbereiche des WLAN-Betreibers an der Sporthalle des ausgestatteten Schulgebäudes resultieren folgende Empfehlungen. Zum einen erstrecken sich die Pflichtenbereiche aktuell auf die vom hiesigen Betreiber beherrschbare Peripherie-Sphäre und andererseits auf die Netzwerknutzerebene.

Hinsichtlich der WLAN-Peripherie hat der WLAN-Betreiber angemessene Sicherungsvorkehrungen (vgl. BGH, Urteil vom 12.05.2010, 1 ZR 121/08; LG München, Beschluss vom 18.09.2014, 7 O 14719/12; LG Hamburg, Urteil vom 25.11.2010, 310 O 433/10) zu treffen.

Hinsichtlich der Nutzer des Netzwerkes sind Aufklärungspflichten (vgl. LG Frankfurt a.M., Urteil vom 18.08.2010, 2-06 S 19/09) zu eruieren.

I. Peripherieschutz

Der WLAN-Betreiber hat den Zugang zum WLAN angemessen gegen den Zugriff von Unberechtigten zu schützen.

Der Empfehlungskatalog für eine rechtskonforme WLAN-Umgebung sieht dabei folgende Maßgaben vor:

- Unterbindung des direkten Zugriffs auf die verbindungsgebende Peripherie (Modem, Router, Access Point, Firewall, TAE- bzw. Kabeldose). Aufbewahrung der Peripherie in abgesperrter Räumlichkeit, möglichst mit Zugangsseparation (z.B. durch Alarmanlage, Schließmechanismus etc.).
- Sicherstellung einer verschlüsselten Verbindung (WPA2 Standard) mit frei vergebenem Netzwerkschlüssel beim WPA2-Personal- bzw. WPA2-PSK-Betrieb (dieser sollte aus mindestens 20 Zeichen bestehen und diese wiederum Buchstaben [große und kleine], Ziffern sowie Sonderzeichen beinhalten). Bei größeren Netzen sollte eine WPA2-Enterprise-Lösung mit entsprechend sicher vorkonfiguriertem Radius-Server in Erwägung gezogen werden.
- Die Webkonfigurationsoberfläche des Routers muss einen passwortgeschützten Zugang bieten (das Passwort sollte ebenfalls frei vergeben werden und aus mindestens 20 Zeichen bestehen und diese wiederum Buchstaben [große und kleine], Ziffern sowie Sonderzeichen beinhalten).
- Der Netzwerkschlüssel und das Konfigurationspasswort zur Routerbedienungsoberfläche sollten zyklisch (mindestens quartalsweise) geändert werden.
- Die automatische Firmware-Update-Funktion der Peripherie (sowohl des Routers, als auch der Firewall) sollte aktiviert sein.
- Die Fernkonfigurationsoption des Routers sollte abgeschaltet werden.
- Die Funktion „Wi-Fi Protected Setup“ (kurz WPS) sollte im Router deaktiviert werden.
- Der „Service Set Identifier“ (kurz SSID) des Routers sollte nicht mehr die werkseitig voreingestellte Bezeichnung tragen und möglichst als „nicht einsehbar“ eingestellt werden.
- Optional können noch Verbindungszeiten definiert werden, um in bestimmten Zeiträumen die Datenverbindung zurückzuweisen.
- Optional kann eine MAC Adress-Filterung erwogen werden, um nur registrierter Kommunikationsperipherie den Zugang ins Internet zu eröffnen. Dies ist jedoch mit einem erheblichen Einrichtungsaufwand verbunden.
- Optional kann über einen Hardwarezugangsschlüssel (etwa in Form eines USB Sticks) nachgedacht werden. Allerdings ist diese Lösung mit einem nicht zu unterschätzenden Kostenaufwand verbunden. Zudem kann hierüber keine unbeschränkte Konnektivität aller internettauglichen bildgebenden Geräte gewährleistet werden. Des Weiteren gelten die im Zusammenhang mit der MAC Adressfilterung geäußerten Bedenken.

- Den Netzwerkgeräten der Nutzer sollte die Kommunikationsebene untereinander (über eine sog. „Client Isolation“) vorenthalten werden.
- Es sollte eine datenschutzkonforme Protokollierung der Internetaktivitäten über einen Zeitraum von mindestens 30 zurückliegenden Tagen erfolgen. Diese Protokollierung sollte regelmäßig - unter Beachtung der datenschutzrechtlichen Bestimmungen - ausgewertet werden.
- Es sollten Internetseitenfilter und ggf. Priorisierungsregeln erstellt werden. In dieser „Blacklist“ sollten (unter der Berücksichtigung der Erkenntnisse aus der Protokollauswertung über die Internetaktivität) Internetseiten mit bedenklichem Inhalt erfasst werden.
- Es sollte eine Portsperre zur Unterbindung der gängigen Kommunikationsverbindungen der bekannten P2P Clienten (z.B. Limewire, Morpheus, Bearshare 6346/6347 TCP/UDP; Edonkey, EMule 4662/TCP 4672/UDP; Bittorrent 6881-6889 TCP/UDP; WinMx 6699/TCP 6257/UDP) eingerichtet werden.
- Es ist ein NetBIOS-(Network Basic Input Output System) Filter zu aktivieren, um NetBIOS-Pakete zu sperren, welche für gewöhnlich für das Aufrufen von Internetseiten nicht erforderlich sind, aber Sicherheitsrisiken bergen. Über die TCP- und UDP-Ports 139 und 445 (die Kommunikationsebenen der Programmierschnittstelle) finden nicht selten Übergriffe auf Betriebssysteme statt.
- Empfehlenswert ist die Aktivierung eines Filters zur Sperrung von Teredo-Paketen zur Unterbindung einer Tunnelung des IPv6, über welche Geräte im Netzwerk eine separate Verbindung an der Firewall vorbei aufbauen können.
- Die Systemwiederherstellungsdateien über die Router- und die Firewall-Einstellungen sollten zugriffsgeschützt sein und auf einem Datenträger außerhalb der Zugriffsreichweite Dritter gesichert werden.
- Es empfiehlt sich sowohl an dem Roter, als auch an der Hardware-Firewall einen Überspannungsschutz zu betreiben.
- Ferner empfiehlt sich eine Sorgsamkeits- und Verschwiegenheitspflichtenerklärung des Wartungs-/Einrichtungspersonals (möglichst sollte einer Person die Kennwortherrschaft anvertraut werden) einzuholen.
- Die Wartung und Einrichtung der Peripherie sollte möglichst über eine kabelgebundene Verbindung erfolgen.
- Der Peripheriestand (die Aktualität der Hardware) sollte zyklisch geprüft werden, um ggf. dem Stand der Technik nachzukommen. Zwar hat der BGH mit Urteil vom 12.05.2010 zum Aktenzeichen 1 ZR 121/08 im Rahmen der Störerhaftung für ein unzureichend geschütztes WLAN auf die Konfigurationsmodalitäten im Zeitpunkt des Einrichtens des Netzwerks abgestellt. Doch in der Praxis ergeben sich hier - insbesondere bei länger zurückliegenden Einrichtungszeitpunkten - häufig Beweisproblematiken im Hinblick auf die seinerzeitigen Einrichtungsbegebenheiten.

II. Aufklärungspflichten

Der WLAN Betreiber muss eine Identitätsbestimmung (samt Lebensalterserfassung) im Hinblick auf die Nutzerdaten durchführen. Überdies ist der Nutzer klar und verständlich über die nationalen rechtlichen Begebenheiten im Zusammenhang mit der Internet- und Netzwerknutzung aufklären. Ferner ist dessen Zusicherung dahingehend einzuholen, dass dieser keine Rechtsverletzungen über den WLAN-Anschluss des Betreibers begehen wird und die Zugangsdaten sicher und sorgfältig - d.h. vor einer Einsichtnahme Dritter - verwahrt.

Erforderlich ist hierfür ggf. die Übersetzung der Identitätsangaben, des aufklärungspflichtigen Inhalts sowie der Zusicherungseinholung und des Datenschutzhinweises in die jeweilige Landessprache des Nutzers.

Die Nutzerdaten und Zusicherungsangaben sind - den datenschutzrechtlichen Maßgaben entsprechend - für einen zuvor festgelegten Zeitraum unter Angabe der Zweckbestimmung der Datenverwendung aufzubewahren.

Minderjährigen sollte der Zugang in Betreiber-WLAN versagt bleiben.

H. Erfüllung der Pflichten im WLAN-Betrieb

Die Erfüllung der vorstehend genannten Pflichten eröffnet ein - den aktuellen rechtlichen Bestimmungen entsprechendes - Betreiben des kabellosen lokalen Netzwerkes an der Sporthalle der Schule.

Die Hardware-Firewall Octogate Rack Solution 100 erlaubt im Zusammenwirken mit der Octogate Firewall Software v.3.0.19 eine konfigurationskonforme Filterung und Zugriffsverweigerung unerlaubter Informationsflüsse. Dies beinhaltet neben der Client Isolation auch die Definition eines manuell erweiterbaren Internetseitenfilters und die Setzung von Priorisierungsregeln z.B. für bestimmte Datenflüsse. Die OctoGate Firewall ist überdies im Stande, den Informationsverkehr auf Malware und andere schädliche Inhalte hin zu prüfen.

Die Firewall bietet eine automatische Firmware-Update-Funktion. Sie offeriert die Zurückweisung von Datenverbindungen in definierbaren Zeiträumen. Die Firewall lässt eine MAC Adress-Filterung ebenso

zu, wie eine Protokollierung der Kommunikationsaktivitäten und zwar über einen maximalen Zeitraum von 90 zurückliegenden Tagen.

Die Firewall offenbart ferner eine dauerhafte, frei zu definierende Portsperre, einen NetBIOS- sowie einen Teredo-Filter. Die Systemkonfigurationsdatei der Firewall lässt sich überdies fremdzugriffsgeschützt auf einem beliebigen Datenspeicher sichern.

Das Voucher-System der Firewall ermöglicht zudem eine datenschutzfreundliche und komfortable Nutzer-Authentifizierung samt einer Kommunikationsprotokollierung unter Ausschluss der Erhebung, Verwendung oder Nutzung personenbezogener Daten. Darüber hinaus gewährt die Firewall eine aktionsfeldbasierte Zusicherungseinholung im Hinblick auf definierbare Verhaltensregeln.

Im Hinblick auf die Peripheriegestaltung schafft die angestrebte Hardware-Firewall-Lösung (der Octogate Firewall des Typs „Rack Solution 100" mit vorinstallierter Octogate Firewall Software v.3.0.19 in der Verbindung mit einem zeitgemäßen und einsatzkonformen WLAN Router) die Grundlage für das - den aktuellen rechtlichen Bestimmungen entsprechende - Betreiben des kabellosen lokalen Netzwerkes an der Sporthalle des Berufskollegs Schloß Neuhaus mit der Zielsetzung der Eröffnung eines Zugangs ins World Wide Web für eine bestimmbare Personenmehrheit. Das hier geplante Vorhaben zur Errichtung eines drahtlosen lokalen Netzwerks am Zielstandort ist unter Beachtung der vorstehenden Empfehlungen zur Sorgfaltspflicht rechtlich nicht zu beanstanden. Auch ginge eine empfehlungsgetreue Umsetzung konform mit den Bestimmungen der - über den Referentenentwurf zum zweiten Gesetz zur Änderung des Telemediengesetzes vom 11.03.2015 - in Aussicht gestellten gesetzlichen Entwicklung der WLAN-Betreiberhaftung.

I. Verwendungshinweise im Hinblick auf diese Stellungnahme

Dieses Dokument gewährt dem Auftraggeber ausschließlich eine Verwendung dieser Stellungnahme im Zusammenhang mit der Realisierung der Errichtung eines drahtlosen lokalen Netzwerkes am Standort Berufskolleg Schloß Neuhaus – Sporthalle gegenüber den mit der Umsetzung dieses Vorhabens betrauten Kreisen. Eine Veröffentlichung dieser Stellungnahme - oder Auszügen hieraus - bedarf der vorherigen ausdrücklichen schriftlichen Zustimmung des Unterzeichners. Selbiges gilt für eine Bezugnahme auf diese Stellungnahme oder Teilen daraus im Rahmen einer gerichtlichen Auseinandersetzung.

Mit freundlichen Grüßen

Markus Rassi Warai
(Rechtsanwalt)