Schleswig-Holsteinischer Landtag
Umdruck 18/564

An den Innen- und Rechtsausschuss

Stellungnahme - Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet

Vorstand - Toppoint e.V.

21. Dezember 2012

Sehr geehrte Damen, sehr geehrte Herren,

gerne möchten wir Ihnen im Folgenden die in Ihrer Anfrage [1] zur Klärung erfragten Punkte beleuchten und einen Überblick über die zu dieser Problematik gehörenden Sachverhalte liefern. Dazu möchten wir die aktuelle Situation und insbesondere auf Aspekte hinweisen, welche in der derzeitigen Rechtssprechung kontra-intuitiv oder technisch wenig realistisch gelöst sind und damit besonders bei Laien für Rechtsunsicherheit sorgen.

Bei der Neugestaltung des rechtlichen Rahmens für die Bereitstellung von Telekommunikationsinfrastruktur sollte darauf geachtet werden, dass die hierfür geltenden Regeln insbesondere für Privatleute und Firmen ohne speziellen technischen Hintergrund einfach verständlich und nachvollziehbar gestaltet sind. Insbesondere sollten diese Regeln die nicht-technischen Analogien aus dem Alltag aufgreifen, um abstruse Auswirkungen zu vermeiden und wenig nachvollziehbare Sonderbehandlungen zu vermeiden.

Stellvertretend für die Freifunk-Gemeinschaft werden wir uns hier hauptsächlich mit den uns betreffenden Punkten beschäftigen und die anderen Aspekte in Kürze in Abschnitt 2 ansprechen. In Abs. 1 werden wir uns mit der aktuellen Situation auseinander setzen. Um dann im folgenden Abs. 1.2 den praktischen Umgang mit dieser zu erläutern.

1 Aktuelle Situation

Deutschland liegt im Vergleich mit anderen europäischen Staaten in Bezug auf den Ausbau von Netzinfrastruktur zurück. Was sich in der Dominanz weniger großer Anbieter und wenig bzw. zögerlichem Netzausbau widerspiegelt. Offener Internetzugang an öffentlichen Plätzen ist selten. Vorhandene Zugangspunkte sind in der Regel kommerzialisiert und stark eingeschränkt nutzbar. Dies benachteiligt insbesondere sozial schwache Schichten der Bevölkerung [2] ohne eigenen Internetzugang. Somit tragen vorhandene, öffentliche Zugangspunkte ihrer Bedeutung für eine Informationsgesellschaft nur wenig Rechnung.

Durch die aktuelle Rechtssprechung bzgl. der Störerhaftung, ist es nur unter unklaren rechtsverhältnissen möglich offene Bürgernetze zu betreiben. Weiter ermöglicht die Umkehrung der Beweislast ein wahrloses Verklagen/Abmahnen von Bürgern.

Wir werden im Folgenden betrachten, wie die Störerhaftung in der aktuellen Rechtsprechung wirkt und welche Ansätze in Bürgernetzen genutzt werden, um evtl. Abmahnungen zu entgehen.

1.1 Aushebelung der Unschuldsvermutung

Da die Gerichte Anzeigen bzgl. Urheberrechts-Verstößen wegen Überlastung ablehnen bzw. mit dessen Bearbeitung erst in Jahren zu rechnen ist, wird aktuell der Weg einer Abmahnung von den Rechtevertretern gewählt. Im Vorfeld dieser Abmahnung hat der Rechtevertreter im Rahmen eines festgestellten Urheberrechts-Verstoßes den Internet-Provider der Person kontaktiert, um einen Kontakt-Datensatz zu erhalten. Als Grundlage zur Ermittelung dieses Datensatzes, wird die Internet-Protokolladresse, welche im Zusammenhang mit dem Verstoß steht, verwendet. In vielen Fällen geschieht die Bearbeitung solcher Auskunftsanfragen des Rechtevertreters durch den Internet-Provider vollständig automatisiert.

Konfrontiert mit einer solchen Abmahnung bleiben der Person nur zwei Wege: Entweder die Kosten der Abmahnung werden beglichen und die beiliegende, bzw. eine modifizierte, Unterlassungerklärung abgegeben. Oder die Person bestreitet die Straftat und es kommt zu einer oft langwierigen Gerichtsverhandlung. In diesem Moment kommt die Störerhaftung ins Spiel. Durch die Umkehrung der Beweislast muss nun der/die Beschuldigte seine Unschuld beweisen, was technisch nur schwer bis gar nicht möglich ist.

Da Internet-Provider angehalten sind, Informationen über die genutzen Adressen eines Kunden nach sieben Tagen zu löschen, kann davon ausgegangen werden, dass bei Erhalt der Abmahnung diese Informationen beim Provider nicht mehr vorliegen [3]. Um weiterhin technisch nachzuweisen, ob die Internet-Protokolladresse zum angegeben Zeitpunkt wirklich der beklagten Person zugeteilt war, müsste die Person Verbindungsprotokolle liefern, welche diese Grundlage verneinen. Allerdings sind, auch wenn die Zugangsgeräte diese Daten erfassen, diese Protokolle nicht revisionssicher digital signiert und somit nicht als Beweissmittel brauchbar. Ebenfalls zeigt ein forensisches Gutachten der Computer des Beklagten nur das diese nicht mit dem Verstoß im Zusammenhang stehen. Es ist also nicht möglich oder nur sehr schwer nachzuweisen, dass die Tat nicht vom entsprechenden Anschluss der Person geschehen sein kann. Und auch wenn gezeigt wurde, dass die Person den Verstoß nicht begangen hat, bleibt weiterhin die Störung durch Dritte in Form der Störerhaftung bestehen.

Die von Providern vergebene Internet-Protokolladresse ändert sich providerabhängig bei jedem Verbindungsaufbau des Zugangsgerätes. Da DSL-

Anschlüsse in Deutschland 24 Stunden nach dem Verbindungsaufbau automatisiert neu verbunden werden, geschieht ein solcher Verbindungsaufbau vergleichsweise häufig. Somit gibt es ausreichend Raum, um bei der Anfrage der Kontaktdaten die Daten eines unbeteiligten Dritten zu erhalten, zumal IP-Adressen teilweise bereits nach wenigen Stunden erneut vergeben werden. Wenn diese "unschuldige" Person nun mit der Abmahnung konfrontiert wird, gibt es, wie oben beschrieben, keine realistische Aussicht auf Erfolg gegen diese Anschuldung anzugehen. Siehe auch [4] und [5].

Tatsächlich zahlt ein Großteil der so zu unrecht Beschuldigten die in der Abmahung verlangte Summe und unterschreibt die Unterlassungserklärung aus Angst vor weiteren finanziellen Repressalien. Letztere belaufen sich in Form von Anwaltsgebühren und Kosten für Gutachten auf mehrere tausend Euro.

Die automatisierte Abarbeitung von Kontaktanfragen von Rechtevertretern, ist auf zwei Weisen problematisch: Einerseits liefert der Provider hier Daten seiner Kunden ohne eine richterliche Anordnung [6] an Dritte weiter, was aus Sicht des Datenschutzes ein Vergehen gegen die eigene Datenschutzerklärungen ist, andererseits existieren hier Schnittstellen, mit denen systematisch ein Kontaktdaten-Diebstahl betrieben werden kann.

1.2 Umgang mit der Störerhaftung in Bürgernetzen

Offene Bürgernetze sind von den in 1.1 besprochenen Problemen direkt betroffen. Zwar liefert die richterliche Rechtsprechung klare Richtlinien, wie offene Netze zu betreiben sind, deren Umsetzung führt aber nicht zu rechtlicher Sicherheit. Auch widerspricht hier die von einigen Gerichten geforderte Absicherung des Internet-Anschlusses in Form von Verschlüsslung der Möglichkeit zur öffentlichen Bereitstellung (vgl. [7])

Daher haben sich technische Lösungen entwickelt, um den Auswirkungen der Störerhaftung zu entgehen. Beide hier angesprochenen Ansätze bergen sowohl technische als auch gesellschaftliche Probleme.

1.2.1 Vorgehen nach aktueller Rechtsprechung

Nach aktueller Rechtssprechung hat der Betreiber eines Durchleitungsdienstes eine Kontroll-/Überwachungspflicht. Diese umfasst u.a. die Aufklärung der Nutzer über die zulässige Nutzungsweise des Dienstes und das Sichten/Filtern des Datenverkehrs. Dies entspricht der im privatrechtlichen Bereich praktizierten Haftungsvermeidung nach Anleitung/Aufklärung bei gemeinschaftlicher Nutzung des Internetanschlusses. Siehe [8] und [9]. Während dies in geschlossenen Nutzergruppen handhabbar bleibt, ist eine Anwendbarkeit für offene Nutzergruppen wenig praktikabel.

Der Aufklärungspflicht nachzukommen ist technisch durch sog. Splashing möglich. Dabei werden Daten-Verbindungen des Nutzers auf die Internet-

Protokoll-Adresse des Durchleitungsgeräts umgeleitet, bis der Nutzer die Nutzungsbedingungen akzeptiert. Durch diese Technik werden eigentlich frei zugängliche Dienste wie Internetseiten oder Instant-Messaging zunächst blockiert. Erst nach Bestätigung wird der Zugriff auf alle Dienste gewährt.

Dies wird oft mit einer Unterdrückung von sog. Datei-Austausch-Protokollen kombiniert.

Dieses Verfahren beeinträchtigt das Verhalten von Nutzergeräten, führt zu Fehlfunktionen und macht das Netz unbrauchbar für Geräte ohne Browser (z.B. GPS Navigationsgeräten) Durch die Umleitung des Datenverkehrs stellt dies einen Eingriff in die Netzneutralität dar und entspricht in wesentlichen Teilen der in autoritären Systemen eingesetzten Technik zur Blockade von Internetinhalten. Insbesondere stellt Sichten/Filtern des Datenverkehrs, unserer Meinung nach, einen Verstoß gegen §88 TKG dar.

Das Implementieren dieses Ansatzes ist nicht trivial und benötigt technisches Verständnis für evtl. geforderte Modifikationen der Filter. Trotz dieser Vorsichtsmaßnahmen gibt es keine Garantie auf Rechtssicherheit, da deren Funktionalität zur Strafzeit in Frage gestellt werden kann und der Gegenbeweiß schwer zu erbringen ist.

1.2.2 Umgehen der Rückverfolgbarkeit

Die Nachteile des in 1.2.1 dargestellten Ansatzes lassen sich mit der Nutzung von Anonymisierungs-VPN-Diensten umgehen. Dabei wird der gesammte Datenverkehr von Nutzern verschlüsselt bis zum VPN-Dienst transportiert und geht erst von diesem aus zum eigentlichen Ziel im Internet. Für Dritte ist hierbei nicht nachvollziehbar, von welcher Internet-Protokolladresse der Datenverkehr ursprünglich stammt. Es bleibt der Anonymisierungsdiensteanbieter als rückverfolgbarer Durchleitungsdienstleiter in der Kommunikationskette ermittelbar. Diese Dienstleister halten aus technischen Gründen keine Kommunikationsprotokolle vor und befinden sich meist im Ausland. Für den Nutzer findet die Anonymisierung transparent statt, es ist von ihm nicht unterscheidbar von einem nicht anonymisiertem Internet-Zugang. Durch diese zwangsweise Entkopplung durch Absender und sichtbarem Urheber der Kommunikation wird die Verfolgbarkeit von Straftaten unterbunden, was nicht das gesellschaftlich gewollte Ziel sein kann.

1.3 Folgen der Störerhaftung

Auf Grund der rechtlichen Risiken, die der Betrieb eines offenen WLANs mit sich bringt, sowie der hohen technischen Schranken für die sachgerechte Absicherung schrecken zahlreiche mögliche Betreiber von einem solchen Angebot ab. Gerade in der Gastronomie wäre das Angebot eines offenen Internet-Zugangs oftmals eine Bereicherung für das Dienstangebot an die

Gäste. Dies wird jedoch nur selten umgesetzt, da der Betrieb unter Einhaltung der gesetzlichen Auflagen zu teuer und wartungsaufwändig ist.

Auch im privaten Umfeld führt die rechtlich unklare Lage, und hierbei insbesondere die vielfach fehlende Kenntnis der genauen Haftungsumstände, in vielen Fällen zur Entscheidung gegen die öffentliche Bereitstellung eines Internet-Zugangspunktes. Gerade bei technisch unversierten Nutzern ist die Angst vor Abmahnungen wegen Nutzung oder Nutzungsbereitstellung des Internet-Anschlusses weit verbreitet. Diese Angst wird neben zahlreichen Medienberichten aber insbesondere durch Anwaltskanzleien befördert, die sich auf das massenhafte Abmahnen von Verstößen mit Bezug zum Urheberrecht und Aktivitäten im Internet spezialisiert haben.

Dabei werden, gegen Auffassung von Datenschützern, von Providern die IP-Adressen und Anschriften von Kunden an diese Kanzleien weitergegeben. Insbesondere da diese Herausgabe von Kundendaten zu Ermittlungszwecken an nicht-staatliche Ermittler umstritten ist, birgt sie mangels ausreichender, unabhängiger Kontrollen und Qualitätssicherungsmaßnahmen ein unkalkulierbares Risiko für Dritte unschuldig ins Fadenkreuz zu geraten.

2 Zu den einzelnen Eckpunkten

Im Folgenden werden wir noch einmal gezielt auf die Punkte des Antrags eingehen.

Zu 1. (Verantwortlichkeit von Telekommunikationsanbietern)

Aus unserer Sicht ist es nicht vermittelbar, warum das kostenfreie Bereitstellen von Durchleitungsdiensten nicht vom TMG gedeckt wird. Die aktuelle Rechtssprechung stellt sich für uns als Zweckargumentation dar. Wir können dem Antrag hier nur zustimmen!

Zu 2. (Schutz der Meinungs- und Informationsfreiheit im Internet)

Die Löschung von konkreten Daten durch eine richterliche Anordnung, unter Kostenfreistellung des Speicherdienstes begrüssen wir. Des weiteren sollte von einem so angeordnetem Löschauftrags keine vortzuführende Kontrollpflicht entstehen.

Im Bezug auf Durchleitungsdienste lehnen wir eine Sperrung oder Filterung ab. Diese widerspricht, unsere Auffassung nach, dem §8 TMG (vgl. §88 TKG) und gefärdet die Netzneutralität. Des weiteren sind von einem technischen Laien solche Kontrollpflichten nicht zu leisten, vgl. 1.1.

Zu 3. (Begrenzung der "Störerhaftung“ und Ausschluss privatpolizeilicher Überwachungspflichten)

Wie bereits zu Nr. 2 dargelegt lehnen wir eine Überwachungspflicht ab.

Zu 4./5. (Telemediennutzungsgeheimnis und Internet-Protokolladressen)

Neben Internet-Protokoll-Adressen sollten auch weitere Geräte-Identifikatoren mit geschützt werden. Es sollte weiter gestattet sein, Internet-Protokoll-Adressen und Geräteidentifikatoren für die technische Bereitstellung von Diensten zu verwenden. Eine zweckentfremdete Verwendung, z.B. zur Profilbildung oder Schalten personalisierter Werbung, sollte ausgeschlossen werden (vgl.§9 TMG).

Zu 6. (Internet-Nutzungsprofile)

Mit den vorhandenen Grundlagen im BDSG, TDG und TMG ist bereits ein Schutz der Privatsphäre rudimentär verankert. Eine Durchsetzung dieser Rechte der Nutzer gegenüber einem Anbieter findet auf Grund mangelnder Kontrollen der Einhaltung nur selten bis gar nicht statt. Dies ist jedoch für eine wirksame Durchsetzung von datenschutzrechtlichen Ansprüchen des Nutzers gegenber dem Anbieter unabdingbar.

Um ferner ein größeres Bewusstsein der Nutzer beim Umgang mit personenbezogenen und personenbeziehbaren Informationen zu erreichen, sollten Diensteanbieter verpflichtet werden, eine deutliche und eindeutige Kennzeichnung vorzunehmen, welche Informationen erhoben, korreliert und verarbeitet werden und wie lange diese zu welchem Zweck vorgehalten werden. Ferner sollte für einen Nutzer eines Dienstes klar ersichtlich sein, nicht nur, dass solche Daten erhoben und verarbeitet werden, sondern auch an wen diese weitergegeben werden. Eine Weitergabe muss hierbei explizit bestätigt werden, um dem Nutzer zu ermöglichen, sein Recht auf informationelle Selbstbestimmung ausgewogen wahrnehmen zu können. Diese Zustimmung muss für die nicht-dienstrelevanten Angaben, wie z.B. Interessen, eine bewusste Entscheidung darstellen und darf daher nicht die Voreinstellung sein.

Zu 7. (Schutz vor Ausspionieren des Nutzers durch "Spyware“,"Web-Bugs“ usw.)

Diensteanbieter sollten effektiv verpflichtet sein, die ausdrckliche Einwilligung von Benutzern einzuholen, bevor sie das Benutzerverhalten personenbeogen oder -beziehbar speichern oder an Dritte weitergeben. Die Privatsphäre des Nutzers sollte ähnlich derer in der nicht-technischen Welt respektivert werden.

Zu 8. (Transparenz von Speicherfristen)

In diesem Zusammgenhang sollten auch Ausnahmeregelungen in §34 BDSG neu überdacht werden. Hier werden wirtschaftliche Interessen über die Informationelle Selbstbestimmung des Bürgers gestellt.

Literatur

[1] *LTSH - Drucksache 18/195: Bundesratsinitiative zur Stärkung der Freiheit und der Privatsphäre im Internet*

[2] *27C3: Digitale Spaltung per Gesetz.* – `http://events.ccc.de/congress/2010/Fahrplan/events/4085.en.html`

[3] *LG Darmstadt - Az. 10 O 562/03*

[4] *ARD Kontraste - Unberechtigte Internet-Abmahnungen - Millionengeschäfte mit ahnungslosen Nutzern.* – `http://www.youtube.com/watch?v=zmhpETzC-Gw`

[5] *Offliner-Oma soll "Raubkopiererin" sein.* 2011. – `http://taz.de/Abmahnung-wegen-Hooliganfilm/!84352/`

[6] *BGH - Az. I ZB 80/11: Auskunftsanspruch gegen Internet-Provider über Nutzer von IP-Adressen*

[7] *BGH - I ZR 121/08: Haftung für unzureichend gesicherten WLAN-Anschluss*

[8] *BGH - Az. I ZR 74/12: Filesharing kein Freifahrtschein.* – `http://www.heise.de/-1751538`

[9] *BGH - Az. 11 W 58/07: Eltern haften nicht immer fuer Tauschboersennutzung ihrer Kinder.* – `http://www.heise.de/-176515`