Jugendschutzfilter

Möglichkeiten und Maßnahmen an WLAN-Hotspots

HOTSPLOTS Whitepaper, Stand: März 2022

hotsplots GmbH
Dr. Ulrich Meier, Dr. Jörg Ontrup
Rotherstr. 22
10245 Berlin
E-Mail: info@hotsplots.de
Tel.: +49 (0)30 29 77 348 0

© hotsplots GmbH

Allgemeines zu Filterlösungen bei WLAN-Hotspots

An bestimmten Standorten (z. B. in Schulen oder Kinderbibliotheken) ist der Einsatz eines Jugendschutzfilters oft vorgeschrieben oder von den Betreibern gewünscht. Neben Kindern und Jugendlichen, die durch den Filter geschützt werden sollen, nutzen aber selbstverständlich auch Erwachsene diese Internetzugänge.

Der Betrieb von Filterlösungen an öffentlichen Internetzugängen ist deshalb auch nicht unproblematisch. Erwachsene Nutzer können durch diesen Filter in Ihren Grundrechten verletzt werden. So verstößt etwa ein sogenannter Content-Filter, bei dem der Inhalt aufgerufener Webseiten nach Stichworten durchsucht wird, gegen das Fernmeldegeheimnis. Auch andere Filter wie Inhaltsanalysen, Deep-Paket-Analysen und ähnliche Technologien sind in Deutschland nicht mit dem Fernmeldegeheimnis vereinbar.

Aufgrund des zu wahrenden Fernmeldegeheimnisses sind Filter auf Basis von DNS[1] gegenüber Content-Filtern vorzuziehen. Über DNS werden die für Menschen verständlichen URLs[2] wie www.hotsplots.de auf für Computer verständliche IP-Adressen wie 92.51.175.170 übersetzt.

Hinweise zum Einsatz von Filterlösungen

Da Filterlösungen Erwachsene in ihren Grundrechten einschränken können und die Nichterreichbarkeit von Webseiten auch finanziellen Schaden verursachen kann, muss vor der Nutzung eines Hotspots mit aktivem Jugendschutzfilter darauf hingewiesen werden.

Bei HOTSPLOTS wird der Hinweis auf einen aktiven Jugendschutzfilter auf der jeweils aufgerufenen Login-Seite automatisch angezeigt.

Jeder Standortinhaber sollte sich bewusst sein, dass eine perfekte Filterlösung im Internet technisch nicht realisierbar ist. Jede Filterlösung erlaubt Seiten, die eigentlich blockiert werden sollten und blockiert Seiten, die eigentlich erreichbar sein sollten. Technisch versierte Nutzer können außerdem Wege finden, den Filter zu umgehen.

Sollte ein Hotspot-Nutzer z. B. die IP-Adresse einer unangemessenen Seite kennen und statt der verständlichen URL (z. B. www.hotsplots.de) die Seite über die IP Adresse (z. B. 92.51.175.170) direkt aufrufen, wird kein DNS-Dienst benötigt und der Filter greift nicht. Außerdem kann durch bestimmte Einstellungen auf dem Endgerät ein anderer DNS-Server ohne DNS-Filter gewählt werden – der Schutzmechanismus wird so umgangen.

Auch eine Bildersuche über Suchmaschinen wie z. B. Google wird immer zu entsprechenden Ergebnissen führen, da Suchmaschinen nicht auf der Filterliste zu finden sind und ihre Suchergebnisse entsprechend nicht blockiert werden. Um hier einen besseren Schutz von Kindern und Jugendlichen zu gewährleisten, verweist HOTSPLOTS bei aktiviertem Jugendschutzfilter auf Suchergebnisse, die mit der Konfiguration „SafeSearch“ durch die Suchmaschine generiert werden (vgl. Abschnitt „SafeSearch bei Google oder Bing, YouTube Restricted Mode“ auf Seite 3 dieses Dokuments).

[1] DNS ist die Abkürzung für Domain Name Service (engl.).
[2] Uniform Resource Locator – im allgemeinen Sprachgebrauch werden URLs auch als Internet- oder Webadressen bezeichnet.

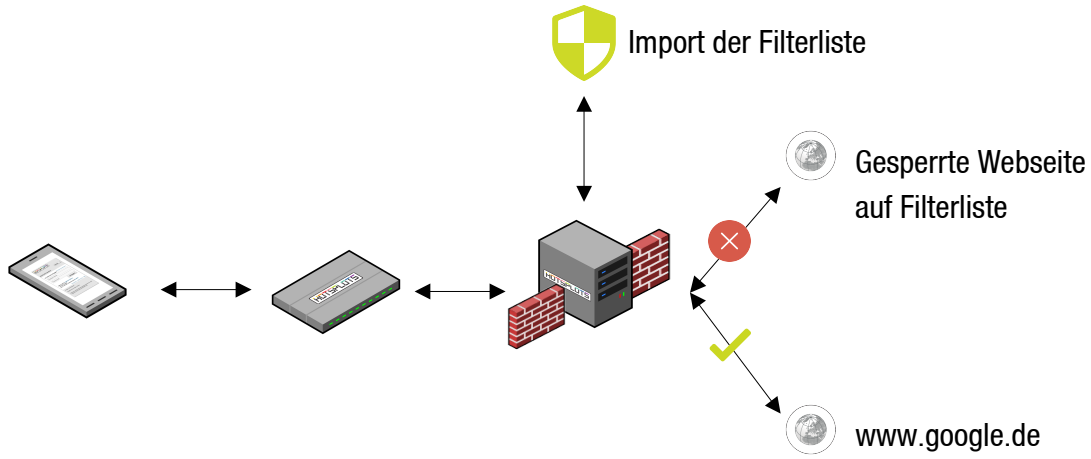
© hotsplots GmbH

Des Weiteren kann es immer passieren, dass Webseiten auf der Filterliste geführt werden, die für einige Nutzer wichtig und hilfreich wären.

Das Fazit muss also lauten: Ein DNS-basierter Filter ist ein einigermaßen wirksames Mittel um Kinder und Jugendliche im Internet vor jugendgefährdenden oder nicht jugendfreien Inhalten zu schützen, ein vollständiger Schutz ist jedoch technisch nie möglich.

Die Filterlösung bei HOTSPLOTS

Jugendschutzfilter bei HOTSPLOTS werden immer auf Basis eines DNS-Filters zur Verfügung gestellt. Konkret bedeutet dies, dass alle Webseitenanfragen der Nutzer zunächst durch den Filter geprüft werden. Sollte die angeforderte Seite auf der Filterliste stehen, wird diese mit einem Hinweis blockiert.



Die durch HOTSPLOTS genutzten Filterlisten beinhalten momentan mehr als zwei Millionen Einträge und werden kontinuierlich aktualisiert und weiterentwickelt.

Alle Nutzer werden auf der Login-Seite des Hotspots darauf hingewiesen, dass an diesem Hotspot ein Jugendschutzfilter aktiviert ist. Dadurch wird auch gegenüber dem Nutzer dokumentiert, dass der Standortinhaber das Thema ernst nimmt und kompetent mit sensiblen Themen umgeht.

SafeSearch bei Google oder Bing, YouTube Restricted Mode

Insbesondere in Suchmaschinen wie Google oder Bing greifen DNS-Filter nicht, da - wie oben bereits erwähnt - Suchmaschinen nicht in den Filterlisten geführt werden.

Ergänzend zum DNS-basierten Filter bieten die Suchmaschinen hierzu Konfigurationen an, mit denen die jeweiligen Suchergebnisse sowohl in der klassischen Suche, als auch bei der Bildersuche vor der Anzeige im Browser gefiltert

© hotsplots GmbH

werden. Der Aufruf dieser Konfigurationen wird bei der Nutzung eines HOTSPLOTS Jugendschutzfilters am jeweiligen Standort serverseitig aktiviert.

Konkret bedeutet das: Sobald der Jugendschutzfilter aktiviert ist, werden die aufgerufenen Daten der Endnutzer über die HOTSPLOTS Server automatisiert auf die Konfigurationen von Google oder Bing SafeSearch oder in den YouTube Restricted Mode umgeleitet.

Als Standortinhaber ist für Sie wichtig zu wissen, dass in diesen Fällen Inhalte gefiltert werden, die nach US-amerikanischem Recht als nicht jugendfrei oder jugendgefährdend gelten. Im YouTube Restricted Mode wird zudem teilweise die Kommentarfunktion zu den angezeigten Videos ausgeblendet.

Technische Implikationen und Einschränkungen beim Einsatz von DNS-basierten Jugendschutzfiltern

Durch die Verwendung der SafeSearch-Varianten der großen Suchmaschinen- und Dienste-Betreiber wie Google oder Microsoft besteht ein nicht unerhebliches Risiko dafür, dass Dienste dieser Anbieter nicht vollständig fehlerfrei und transparent genutzt werden können. An verschiedenen Standorten konnte z.B. beobachtet werden, dass Dienste wie Google Meet oder Microsoft Teams nur eingeschränkt nutzbar sind, wenn der Jugendschutzfilter aktiviert ist. Weitere Einschränkungen wurden zudem im Zusammenhang mit Call by WLAN Funktionen beobachtet. Diese Einschränkungen liegen außerhalb des Einflussbereiches von HOTSPLOTS, da viele Dienste auf DNS zurückgreifen, um bestimmte Funktionen zu realisieren. Daher sollte vor dem Einschalten eines DNS-Filters berücksichtigt werden, dass bestimmte Web-Applikationen oder Dienste nicht mehr vollständig funktionsfähig sein können.

Friendly Wifi

„Friendly WiFi“ ist ein von der britischen Regierung initiierter sicherer Zertifizierungsstandard für öffentliches WLAN. Er wurde im Jahr 2014 ins Leben gerufen, um sicherzustellen, dass öffentliches WLAN die Mindestfilterstandards erfüllt, insbesondere in Bereichen, in denen Kinder anwesend sind.

Friendly WiFi arbeitet mit dem „Project Arachnid“ zusammen. Project Arachnid ist eine globale Lösung, auf die Internet Service Provider (ISPs) und Filterunternehmen zugreifen können, um ihre Filterlösungen im globalen Kampf gegen die Online-Gefährdung von Kindern und Jugendlichen zu verbessern. Diese Filterliste wird täglich aktualisiert. Eine Besonderheit des Project Arachnid ist, dass nicht ausschließlich die zu filternden URLs gesammelt und zur Verfügung gestellt werden, sondern sich das Projekt auch aktiv für das Entfernen der Inhalte aus dem Internet einsetzt.

HOTSPLOTS erfüllt als Internet Service Provider die Anforderungen für das Zertifikat von Friendly WiFi.

© hotsplots GmbH

Einschätzung zur rechtlichen Situation in Deutschland

Oft wird bei der Frage nach Jugendschutz an Hotspots in Deutschland Bezug genommen auf den „Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV)". Insbesondere § 11 bezieht sich hier auf „Jugendschutzprogramme".

Tatsächlich finden die Regelungen des JMStV keine Anwendung für Telekommunikationsdienste oder telekommunikationsgestützte Dienste (§ 2 Abs. 2 JMStV), welche WLAN-Hotspots darstellen. Für HOTSPLOTS finden in erster Linie die Regelungen des Telekommunikationsgesetzes (TKG) Anwendung. Dies gilt zumindest dann, wenn der technische Vorgang der Telekommunikation betroffen ist, was regelmäßig beim Anbieten von WLAN-Hotspots der Fall ist.

Im Bezug auf Jugendschutzfilter, insbesondere z. B. bei Bibliotheken, ist nach Einschätzung durch HOTSPLOTS eine öffentliche Bibliothek kein „Anbieter" eines Telemediums[3]. Denn Juristen zufolge sind beispielsweise Betreiber von Internet-Cafés auch keine Anbieter im Sinne des JMStV[4].

Ein von der Kommission für Jugendmedienschutz (KJM) für geeignet erklärtes Filterprogramm wäre außerdem nur dann erforderlich, wenn das jeweilige Angebot geeignet ist, die Entwicklung und Erziehung von Kindern und Jugendlichen zu beeinträchtigen (§§ 11, 5 JMStV). Das „Angebot" bezieht sich hier auf Telemedien, also Internetseiten oder Apps. Diese müssen geeignet sein, die Entwicklung zu beeinträchtigen. Das Anbieten eines offenen Internets ist nach Einschätzung durch HOTSPLOTS nicht per se geeignet, die Entwicklung zu beeinträchtigen. Das soll selbstverständlich nicht heißen, dass keine Maßnahmen zum Schutz von Kindern und Jugendlichen vor den Gefahren des Internets ergriffen werden sollten. Eine solche Maßnahme ist z. B. der durch HOTSPLOTS angebotene DNS-basierte Jugendschutzfilter.

Aus § 11 JMStV folgt nicht, dass jeder Anbieter von Jugendschutzprogrammen oder Filtern diese der KJM vorlegen muss. Die Kriterien der KJM zielen z. B. auf Software, die auf dem Endgerät des Kindes oder Jugendlichen installiert wird und von den Eltern oder sonstigen Betreuungspersonen dem Alter des Kindes entsprechend konfiguriert wird. Das ist auf einem Router, der den Internetzugang für ein Netzwerk regelt, so nicht umsetzbar. So besagen z. B. die Kriterien, dass für Kinder unter 12 Jahren eine Whitelist eingesetzt werden sollte und alle nicht darin enthaltenen Seiten blockiert werden müssen. Das wäre für die älteren Nutzer allerdings eine extreme Einschränkung.

[3] Im genannten § 11 Abs. 2 (JMStV) geht es letztendlich um die Erfüllung der Verpflichtung aus § 5 Abs. 1 „*Sofern Anbieter ...*". Der Begriff *Anbieter* ist in § 3 Abs. 2 Zi. 2 definiert als „Rundfunkveranstalter oder Anbieter von Telemedien".
[4] vgl. Spindler/Schuster, Recht der elektronischen Medien, 3. Auflage 2015, § 3 JMStV, Rn. 8

© hotsplots GmbH