Antwort auf: „Kampf gegen Darstellung von Kindesmissbrauch im Internet: technische und organisatorische Fragen“

Sebastian v. Bomhard, SpaceNet AG, 18. Oktober 2010

Frage 1:

> *Wie gestaltet sich die Zusammenarbeit der nationalen Beschwerdestellen mit den Behörden und den Internet Service Providern in Europa und im internationalen Bereich aus? Wie lange dauert es durchschnittlich und je nach Ländern, bis Seiten gelöscht sind? Wie erklären sich die unterschiedlich langen Löschzeiten? Sind die Erfolgschancen auf schnelle Löschung gestiegen? Wie zahlreich ist das Phänomen, dass gelöschte oder gesperrte Inhalte unter anderer Quelle wieder auftauchen? Wie reagieren die Täter auf das Löschen und wie auf das Sperren? Hat sich seit Beginn der Evaluierungsphase des Zugangserschwerungsgesetzes eine Veränderung ergeben?*

Diese, wie auch alle anderen Fragen, kann ich ausschließlich aus der Sicht eines Internetproviders beantworten. Daher bleiben einige Fragen unbeantwortet.

Beschwerden erreichen die Internetprovider meistens über eine von jedem Provider zur Verfügung gestellte Adresse („*abuse*“). Generell wird die Beschwerde dort geprüft und entsprechend eingestuft. Dabei ist zu beachten, daß Netzwerksanbieter keine Prüfungsinstanz für die Legalität von Daten sind. Dennoch gibt es natürlich Vorfälle, die sofort abschätzbar sind.

Viren werden von Virenprogrammen erkannt. Parasitär genutzte Webserver sind ebenfalls meist leicht zu erkennen. Eingeschleuster HTML-Code für eine Phishing-Attacke ist auch in der Mehrzahl der Fälle sicher identifizierbar.

Anders verhält es sich mit pornographischem Material. Kinderpornographisches Material ist nicht eindeutig, sofern der Begriff des „Kindes“ und der der „Pornographie“ weit ausgelegt werden darf. Darüber hinaus, wie wir Provider immer wieder gewarnt werden, dürfen unsere Mitarbeiter kinderpornographische Bilder nicht einmal ansehen, um trotz der Schwierigkeiten wenigstens die eindeutig erkennbaren illegalen Bilder zu identifizieren. Der einzig mögliche Weg ist also, die Polizei von der Beschwerde zu verständigen.

Da umgekehrt nicht einfach auf beliebigen Zuruf irgendwelche Seiten ohne Prüfung gelöscht werden können, kam die Forderung nach Einrichtung einer „Freiwilligen Selbstkontrolle“ auf. Hierbei kann es sich nur um ein Mißverständnis handeln: Eine Selbstkontrolle ist nur sinnvoll bei den für Inhalte Verantwortlichen. Übertragen auf die Bücherwelt hieße das, daß das Buchdruckergewerbe und nicht Autoren oder Verleger eine Instanz gründen würde, die über Inhalte entschiede. Eine Selbstkontrolleinrichtung der Netzwerkanbieter müßte darüber hinaus begründen, wieso sie Aufgaben der Justiz übernimmt, die ihr nicht zustehen.

Übertragen auf ein Löschbegehren ins Ausland ist durchaus vorstellbar, daß die dortigen Netzwerkbetreiber die Sache ähnlich sehen, was dazu führt, daß man die Angebote, die man aus dem Netz entfernen will, eben nicht immer einfach aus dem Netz bekommt. Daher braucht es eine schnelle Reaktion der dafür *zuständigen* Stellen wie Polizei und Staatsanwaltschaft, denn, daß auf eine gültige Verfügung hin gelöscht wird, ist klar.

Mit dem Löschen von Angeboten ist es im übrigen nicht getan. Hier werden ja keine Photos beschlagnahmt, sondern Kopien von Bildern gelöscht, die auf Knopfdruck sofort an anderer Stelle wieder ins Netz eingestellt werden können. Nach heutigem Stand der Technik ist ein statisches Angebot ohnehin recht unwahrscheinlich. Hierzu habe ich ausführlicher im zweiten Teil Stellung genommen (siehe Seite 3: „Allgemeines zum Thema Sperren und Löschen“)

Frage 10

> *Welche Vor- und Nachteile hätte ein zentrales Sperrkonzept gegenüber einem dezentralen Melde- und Löschkonzept? Welchen Personalaufwand erfordern die jeweiligen Konzepte bei staatlichen Stellen?*

Ein zentrales Sperrkonzept ist zum Scheitern verurteilt. Damit meine ich nicht, daß möglicherweise in unverhältnismäßiger Weise Bürgerrechte verletzt werden, oder daß eine Plattform geschaffen würde, die zum zensierenden Machtmißbrauch geradezu einlüde. Vielmehr lege ich im zweiten Teil dieses Dokuments dar, daß es keine funktionierenden Sperren geben kann (siehe Seite 3: „Allgemeines zum Thema Sperren und Löschen“). Dort weise ich ebenfalls auf Probleme bei Melde- und Löschkonzepten hin.

Es bleibt nur der Weg über Polizei, Justiz und internationale Zusammenarbeit.

Frage 11 + 12

> *In einer Untersuchung im Juni 2008 legten Tyler Moore und Richard Clayton von der University of Cambridge dar, dass Seiten mit kinderpornographischem Inhalt eine längere Lebensdauer hätten als andere illegale Webangebote wie z.B. Phishingsites. Dies begründeten sie vor allem mit der damals mangelhaft koordinierten internationalen Kooperation. Worin liegen die Hauptgründe für die unterschiedlichen Zeiten, die das Löschen der jeweiligen Inhalte benötigt? Wäre beispielsweise ein verbessertes notice-and-take-down-Verfahren ein gangbares Mittel, um die Entfernung von Missbrauchsdokumenten analog zur Entfernung von Phishingsites durchzuführen?*
>
> *Wie kann die Zusammenarbeit zwischen den Strafverfolgungsbehörden, den Selbstregulierungskräften der Privatwirtschaft wie INHOPE und den Internet Service Providern weiter verbessert werden?*

Ich kann die Studie nicht überprüfen, aber die Aussage erscheint mir nicht überraschend. Banken haben ein großes Interesse daran, Phishingseiten sofort unschädlich zu machen. Hierfür wurden Stellen geschaffen und internationale Netzwerke, und die Hinweise sind für die jeweiligen Abuse-Stellen erkennbar aufbereitet, was die Arbeit beschleunigt.

Hinzu kommt, daß die Materie leichter zu überprüfen ist. Diesen Schritt können die Provider meist selbst erledigen. Anders bei der Thematik Kinderpornographie. Am schnellsten geht die Löschung, wenn ein richterlicher Beschluß vorliegt. Die beste Maßnahme gegen Kinderpornographie wäre also, die Justiz entsprechend auszurüsten, daß so ein Beschluß schnell herbeizuführen ist.

Dies sollte für alle Rechtsstaaten gelten und entsprechend direkt umzusetzen sein. Private Initiativen wie INHOPE können nur unterstützen. So unterrichtet beispielsweise INHOPE, wie ich gelesen habe, die Polizei des Landes, in dem die zu beanstandenden Seiten liegen. Eine direkte Aufforderung zur Löschung kann in Einzelfällen das erwünschte Resultat liefern, ist aber als Standardprozeß unzulänglich. Es ist ja weiterhin zu berücksichtigen, daß die Rechtsnormen und Vorstellungen von Land zu Land differieren. Daher wird sich an der Methode der Benachrichtigung der Verfolgungsbehörden in dem Land, in dem die Daten vorgehalten werden, nichts ändern.

Die Dauer bis zur Löschung der Seiten mißt demnach nicht die Effizienz von INHOPE, sondern die Effizienz des Rechtssystems des entsprechenden Landes. Und genau hier sollten wir ansetzen.

Allgemeines zum Thema Sperren und Löschen

DNS-Sperren

Mechanismus: Sollen aus einer bestimmten Domain die Daten nicht mehr abrufbar sein, ist eine Variante die Manipulation der Nameserverdaten. Der Provider liefert nicht mehr die korrekten Daten aus, sondern eine andere IP-Adresse. Hinter dieser IP-Adresse verbirgt sich ein Hinweis, daß das angesurfte Angebot illegal sei.

Nachteil des Verfahrens: Es ist leicht zu umgehen und trifft, wenn es nicht umgangen wird, nicht einzelne Seiten, sondern ganze Internetauftritte. Sollte es einem Angreifer gelingen, eine einzige Seite auf bundestag.de zu plazieren, wäre das gesamte Netzangebot von der Sperre betroffen.

Umgehung: Man vertraut nicht mehr dem Nameserver des eigenen Providers, sondern trägt irgendeinen der zahlreichen freien Nameserver im Netz ein.

Aufwand der Umgehung: Nicht nennenswert. Anleitungen für die Konfiguration finden sich zuhauf im Netz, darunter Videos auf YouTube. Einen beliebigen Nameserver auszuwählen läßt sich nicht kriminalisieren.

Risiko der Umgehung: Der Nutzer, der so ein Angebot wahrnimmt, ist in der Gefahr, Opfer eines Angebots vorgeblicher Bürgerrechtsaktivisten zu werden, das in Wahrheit zwar die „gesperrten“ Daten ausliefert, gleichzeitig aber auch andere Verbindungen wie Homebanking umleitet. Zerstört man das Vertrauen der Nutzer in die Nameserver „ihrer“ Provider, steigt das Risiko ausgespähter Daten.

Proxysperren

In früheren Internettagen war die Bandbreite knapp und teuer. Hier wurde ein Mechanismus erfunden, den es heute noch gibt, der sogenannte Proxycache. Antworten auf Webfragen werden nicht an den Zielrechner gestellt, sondern an einen sogenannten Proxyserver. Dieser merkt sich („cache“) die Antwort und kann diese beim nächsten Mal direkt liefern, ohne erneut nachfragen zu müssen. Das spart Bandbreite.

Klinkt man sich hier ein, kann man natürlich dafür sorgen, daß bestimmte Seiten nicht ausgeliefert, sondern durch andere Seiten ersetzt werden.

Nachteil des Verfahrens: Es ist leicht zu umgehen.

Umgehung: Man vertraut nicht mehr dem Proxyserver des eigenen Providers, sondern trägt ihn einfach aus.

Aufwand der Umgehung: Nicht nennenswert. Anleitungen für die Konfiguration finden sich zuhauf im Netz, darunter Videos auf YouTube. Die Nutzung eines Proxyservers ist nicht obligatorisch.

IP-Sperren

Natürlich gibt es immer die Möglichkeit, auf IP-Adreßebene zu sperren. Die Route zu dieser bestimmten Adresse wird geblockt. Etwas aufwendiger, aber technisch machbar wäre das umleiten.

Nachteil des Verfahrens: Es ist leicht zu umgehen und trifft, wenn es nicht umgangen wird, nicht einzelne Seiten, sondern viele weitere komplette Internetauftritte. Hinter einer einzigen IP-Adresse stehen gelegentlich Tausende von Webservern, die alle mitgesperrt würden.

Umgehung: Man wählt einen Proxy, für den die Route nicht gesperrt ist, also etwa einen im Ausland.

Aufwand der Umgehung: Nicht nennenswert. Anleitungen für die Konfiguration finden sich in der Hilfefunktion des verwendeten Browsers. Die Auswahl eines ausländischen Proxyservers läßt sich nicht kriminalisieren.

Risiko der Umgehung: Der Nutzer, der so ein Angebot wahrnimmt, ist in der Gefahr, Opfer eines vermeintlichen Bürgerrechtsangebots zu werden, das in Wahrheit zwar die „gesperrten" Daten ausliefert, gleichzeitig aber in andere Verbindungen wie Homebanking eingreift.

Proxyzwang

Sperrt man den Port 80 (http) auf allen Gatewayroutern, so ist der Nutzer gezwungen, einen Proxy einzutragen. Ab da gilt alles, was zum Thema Proxysperren gesagt wurde.

Nachteil des Verfahrens: Es ist leicht zu umgehen.

Umgehung: Man vertraut nicht dem Proxyserver des eigenen Providers, sondern trägt einen alternativen Proxyserver ein.

Aufwand der Umgehung: Nicht nennenswert, siehe oben.

Deep Packet Inspection

Der komplette Datenverkehr wird mitgeschnitten. Finden sich zu überprüfende Dateien, wird die Übertragung kurz angehalten, eine Anfrage gemacht bei einer zentralen Datenbank (zum Beispiel nach hinterlegten Hashwerten), und die Daten entweder freigegeben und weiter ausgeliefert, oder aber geblockt. Dieses Verfahren wird heute auf Viren angewendet, es läßt sich aber allgemein auf den ganzen Datenverkehr ausweiten.

Nachteil des Verfahrens: Es ist leicht zu umgehen. Gleichzeitig stellt es nicht nur technisch eine ungeheure Anstrengung dar, sämtliche Datenpakete zu überwachen, es wäre völlig unverhältnismäßig. Auch existiert so eine Datenbank nicht.

Umgehung: Man verwendet Verschlüsselung für die Übertragung illegaler Inhalte. Der Anbieter hat darüber hinaus die Möglichkeit, die Daten in Einzelstücken auszuliefern, die erst beim Abrufer wieder zusammengesetzt werden – so ein Verfahren kommt derzeit bei BitTorrent zum Einsatz. Letztlich kann man durch simpelste Eingriffe die Datei maskieren. Vertauscht man nur ein Bit oder kodiert man um in ein anderes Format, ändert sich der Hashwert, anhand dessen die Datei in so einer hypothetischen „Datenbank gesperrter Inhalte" auffindbar gewesen wäre.

Aufwand der Umgehung: Nicht nennenswert. Verschlüsselung ist nicht verboten, im Gegenteil. Angesichts der Risiken im Internet wird regelmäßig empfohlen, alle Daten zu verschlüsseln, die nicht für die Öffentlichkeit bestimmt sind.

Löschen

Ist das Löschen illegaler Inhalte also die einzige funktionierende Variante? Leider nein, auch Löschungen können von professionellen Anbietern leicht umgangen werden. Sie publizieren auf Servern, die dem Angebot nicht direkt zuzuordnen sind. Es gibt technisch keinen Grund, wieso die Einstiegsseiten und die auszuliefernden Bilddateien auf demselben Server liegen müssten. Die Ein-

stiegsseiten enthalten vielleicht gar keine Bilder und können daher nicht „offensichtlich“ gelöscht werden.

Die Bilddaten hingegen sind, sofern sie nicht verschlüsselt sind, möglicherweise zweifelsfrei identifizierbar. Nur handelt es sich ja nicht um „Bilder“, sondern schlicht um Kopien von Dateien, die auf Knopfdruck jederzeit von einem anderen Ort im Netz geholt werden könnten. Das zu bekämpfende Online-Angebot müßte hierzu nur an einer kleinen Stelle umgestellt werden. Wird dies professionell gemacht, entsteht einfach nur ein Hase-Igel-Spiel, das man nicht gewinnen kann, wenn man nicht an die Betreiber herankommt.

Was bleibt?

Es steht bereits da: Der Kampf ist nur zu gewinnen, wenn man direkt bei den Tätern *in persona* ansetzt, also bei Konsumenten, Verteilern und Produzenten. Hierfür sollte man alle verfügbaren Ressourcen und Allianzen verwenden, im Inland wie im Ausland.