Unterausschuss Neue Medien, 25.10.2010, öffentliche Sitzung
„Kampf gegen Darstellung von Kindesmissbrauch im Internet: technische und organisatorische Fragen“

Einleitung

ICANN ist ein gemeinnütziges Unternehmen nach kalifornischem Recht, das per Akklamation der Aktiven des Internets (Domainanbieter, Domainbetreiber, Internetprovider, Adressverwalter und Nutzer) mit der Festlegung der technischen Betriebsparameter für eine uneingeschränkten Konnektivität, insbesondere den Regelwerken zur Adress- und Domainverwaltung, sowie zum Betrieb der Root-Server beauftragt ist. Desweiteren ist ICANN dafür zuständig, die juristische Weiterentwicklung dieser Gebiete zu betreiben.[1]

Aufgrund der Akklamation bezieht ICANN seine Existenzberechtigung einzig aus dem Fakt, bisher keine wesentlichen Fehlentscheidungen aus Sicht der Internetakteure getroffen zu haben. Die Entscheidungen bei ICANN werden auf Basis von Zuarbeiten der Unterstützungsorganisationen (SO) vom Board getroffen, einer Gruppe von Personen, die nicht in Personalunion mit anderen wichtigen Aufgaben betraut sein dürfen. Die SO setzen sich i.d.R. aus Lobbyvertretungen (CU) zusammen. Diesen Prozess begleiten die Beratungsgremien (AC) durch Hinweise aus einer übergreifenden Position heraus, haben aber weder ein Veto- noch ein Mitbestimmungs- oder Vorschlagsrecht.[2]

Die für diese Anhörung relevanten Organisationen sind – alphabetisch – die Beratungsgremien ALAC (Nutzervertretung), GAC (Regierungsvertretung) und SSAC (Expertengremium für Sicherheit und Stabilität). Ich bin über die NGO Fitug e.V. als Vertreter der Nutzervertretung AtLarge/ALAC bei ICANN aktiv und bearbeite dabei hauptsächlich technische Fragestellungen wie IPv6, DNSSEC und den Auskunftsdienst „Whois“.

ICANN weist explizit jede Verantwortung für Inhalte im Internet von sich[3], die zulässigen Einspruchsmöglichkeiten beschränken sich auf die Domainnamen selbst, typischerweise also Namensmissbrauch[4] durch Markenrechtsverletzungen oder vorsätzliche Fehlbezeichungen. Bei akuter Gefährdung der Netzstabilität ist im Konsens mit allen Beteiligten eine behutsame Einflussnahme auf den Registrierungsprozess möglich, wie das bei Conficker[5] und bei FastFlux[6] geschah.

Die Bekämpfung von Conficker gleicht stark den Vorschlägen bei Netzsperren, so dass ich den Abschlussbericht anhänge und auf die wesentlichen Merkmale bei diesem Vorgang hinweisen möchte.

---

[1] §3, Articles of Incorporation of ICANN, Nov, 21th 1998
[2] Bylaws of ICANN, Aug, 5th 2010
[3] http://www.icann.org/en/dispute-resolution/#content
[4] http://www.icann.org/en/udrp/udrp.htm
[5] http://www.icann.org/en/security/conficker-summary-review-07may10-en.pdf
[6] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf

Der Conficker Fall

Der Wurm Conficker baut ein Botnetz auf, das zu kriminellen Handlungen benutzt wird. Um sich vor Gegenmaßnahmen zu schützen, aktualisiert sich die Software ständig, in dem sie Updates von pseudo-zufälligen Domainnamen nachlädt, um sich zu aktualisieren. Gelingt die Aktualisierung für einige Wochen nicht, löscht sich der Wurm selbst, um sich einer Analyse zu entziehen. Neu an Conficker ist hierbei, dass der Wurm auf Namen statt wie bisher auf Adressen setzt.

Nachdem die Spezialisten der Sicherheitsunternehmen dieses Ergebnis der Untersuchungen vorlegten, lag der Schluss nahe, den Updateprozess durch Blockieren der Domainnamen zu unterbinden. Im Gegensatz zu Netzsperren besteht bei Conficker die Aufgabe daran, noch nicht registrierte Domainnamen vor der Registrierung zu einem bestimmten Zeitpunkt zu schützen. Für bereits bestehende Domainnamen wurde explizit kein Eingriff vorgesehen, da dieser als völlig unverhältnismäßig angesehen wurde und wird.

In einem koordinierten Vorgehen mit über einhundert nationalen Länderdomains gelang es im April 2009 eine wirksame Blockade durch Verhinderung der Neuanmeldungen von Domains zu erreichen. Conficker wich daraufhin in den folgenden Versionen vollständig auf Peer-2-Peer Netze aus und entzog sich so der Einflussnahme im Rahmen von ICANN.

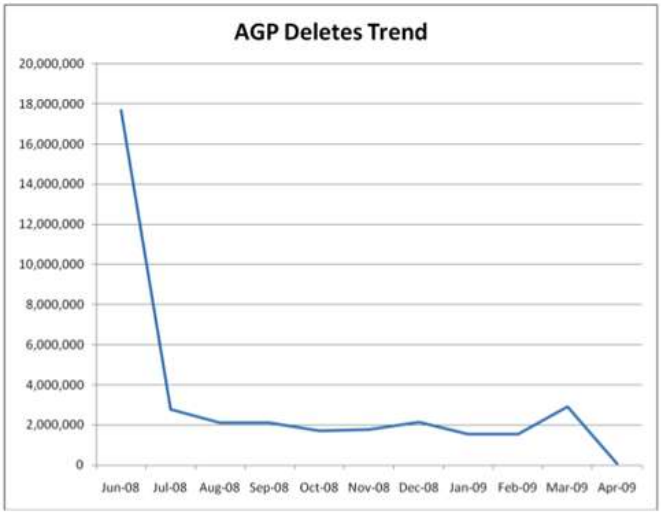
Die wesentlichen Erfolgsparameter bei der Bekämpfung von Conficker waren:

- **Koordinierte Zusammenarbeit** der Strafverfolgungsbehörden der betroffenen Länder, der internationalen Strafverfolgungsorgane, der Top-Level-Domainverwalter und Sicherheitsunternehmen.
- Gezielter und im Vorfeld bereits **allgemein akzeptierter Eingriff** in den Neuregistrierungsprozess, d.h. **ohne Beeinträchtigung bestehender Internetdomains**.
- **Überwachung und Erfolgskontrolle** des Eingriffs durch zeitnahe und **öffentliche Berichte**.

Für die Details verweise ich auf den finalen Report vom 7.3.2010 im Anhang.

Die FastFlux Technik

Der Einsatz von FastFlux unterminiert die Strafverfolgung durch sehr schnellen Wechsel der Internetdomains und der verwendeten IP Adressen. Möglich wurde FastFlux durch eine kostenlose Probezeit (Domain Tasting, Add Grace Period) bei der Domainregistrierung, in der eine neu angemeldete Domain innerhalb einer Woche benutzt werden konnte, ohne dass Registrierungskosten entstanden.



Nachdem – durch Vergleich mit Länderdomain, die nur eine geringe Änderungsrate zulassen – erkannt wurde, welches Missbrauchspotential in diesem Verfahren liegt, hat ICANN alle Anmeldungen im Juni 2008 mit einem minimalen Entgelt belegt und ein Jahr später regulär kostenpflichtig gemacht.[7] Der Erfolg ist deutlich sichtbar.

Aktuell stellt FastFlux keine ernsthafte Stabilitätsbeeinträchtigung mehr dar.[8] Die aktuellen Änderungshäufigkeiten liegen im Schnitt bei acht Tagen und gestatten den Polizeibehörden mittels „Quick Freeze“ einen ausreichend schnellen Zugriff auf die Kontaktdaten. Interessant an der aktuellen Statistik ist, dass die üblichen Länder, in denen FastFlux Systeme betrieben werden, über eine gut ausgebaute Infrastruktur und Justiz verfügen: Unangefochten an der Spitze stehen die USA, Deutschland ist immer unter den ersten zehn der Betreiberländer. Ein Zusammenhang mit „Failed States“ kann an dieser Stelle explizit verneint werden.

Der Abschlussbericht[9] zu FastFlux zeigt auf 154 Seiten den Aufwand, den ICANN in die Auffindung eines Konsenses und die Abwägung aller Interessen steckt. Er ist exemplarisch für die Arbeitsweise von ICANN, insbesondere aber für das komplette Desinteresse seitens der nationalstaatlichen Regierungen an einem konstruktiven Prozess. Dieser Bericht wertet u.a. die in Frage 11 genannte Studie aus und kann erfolgreich zeigen, dass die Maßnahmen von ICANN die Löschzeiten von Phishing Domains halbieren konnten.

Der Schluss, den die Behandlung dieses Falls bei ICANN zulässt, besteht darin, dass im Rahmen der normalen polizeilichen Ermittlungsarbeit **kein Handlungsbedarf hinsichtlich einer Datenspeicherung** auf Vorrat besteht. Sollten die Polizeibehörden nicht innerhalb der aktuell notwendigen Reaktionsfristen reagieren, so ist zuerst an der **Ausstattung der Behörden** und an der **Effizienz der internen Abläufe** zu arbeiten.

[7] http://www.icann.org/en/tlds/agp-policy-17dec08-en.htm
[8] http://atlas.arbor.net/summary/fastflux
[9] http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf

Antworten auf die Fragen

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?*

   Internetinhalte sind Daten, die beliebig oft und fast beliebig schnell kopiert werden können. Inhalte werden auf verschiedensten Wegen im und außerhalb des Internets transportiert. Die Transportwege im Internet sind ca. zu einem Drittel verschlüsselt und somit für den Netzbetreiber nicht einsehbar[10]. Der Transport illegaler Inhalte im Internet erfolgt nach aller Erfahrung nicht öffentlich und ist nicht auf leichtem Wege zugänglich.

   Da ICANN nicht für Inhalte im Internet zuständig ist, liegen wenige Angaben zu länderabhängigen Geschwindigkeiten bei der Löschung von Inhalten vor. Allerdings zeigen Statistiken[11], dass die Löschung am langsamsten in den Ländern USA, Australien und Deutschland geschieht. Schnelle Löschungen sind vor allem in Russland und den angrenzenden Ländern zu verzeichnen.[12]

   Die unterschiedlich schnellen Löscherfolge gehen meiner Meinung nach auf die unterschiedlich effizienten Strafverfolgungsbehörden zurück. Zersplitterte Zuständigkeiten und fehlende Rückmeldemöglichkeiten führen leicht dazu, dass eine Meldung versandet und gar nicht bearbeitet wird.

   Wie bei Conficker zu sehen, werden konkrete Sperrungen schnell und effizient durch die Kriminellen umgangen. Echten Erfolg bringt nur eine effiziente internationale Zusammenarbeit, die öffentlich nachvollziehbar ist und auf einem breiten Konsens beruht. Durch die Maßnahmen zur Eindämmung von FastFlux, ist die Aufklärungsquote deutlich angestiegen. Beide Vorgänge haben aber nichts mit der Gesetzeslage in Deutschland zu tun.

   Das Zugangserschwerungsgesetz hat durch seinen Entstehungsprozess eine erhöhte Sensibilisierung innerhalb Deutschlands erzeugt. Eine konkret zuordenbare Wirkung ist

[10] Siehe Ausschussdrucksache 17(24)008-C der öffentlichen Anhörung vom 4.10.2010, Seite 2
[11] "Lawful access restriction using DNS modification", WG5 at ICANN Mexico Meeting, 2009
[12] http://scusiblog.org/?p=463

jedoch innerhalb Deutschlands nicht feststellbar. Außerhalb Deutschlands ist das Gesetz gänzlich wirkungslos.

2. *Wie viele Hinweise sind beim BKA und den Selbstkontrolleinrichtungen und Beschwerdestellen oder andere Einrichtungen zu strafbaren Inhalten nach § 184 b StGB auf Webangeboten sind seit Inkrafttreten des Zugangserschwerungsgesetzes eingegangen und wie viele Fälle gingen auf Ermittlungen der Polizeibehörden zurück? Wie viele Angebote enthielten tatsächlich strafbewehrte Inhalte nach § 184 b StGB? In wie vielen Fällen konnte seit Verabschiedung bzw. seit Inkrafttreten des Zugangserschwerungsgesetzes und auf wessen Veranlassung eine Löschung – und in welchem Zeitraum – derartige Angebote erreicht bzw. nicht erreicht werden? Welche Erkenntnisse gibt es zu den Serverstandorten (aufgeschlüsselt nach länderspezifischen Erkenntnissen)? Welche Erkenntnisse gibt es zu der Frage, warum eine Löschung nicht erreicht werden konnte?*

   Da ICANN keine Meldestelle für strafbare Inhalte betreibt, liegen hierzu keine Angaben vor. Die Auswertung von Sperrlisten anderer Länder zeigt aber, dass der Anteil der hier relevanten Straftaten deutlich unter einem Prozent der Listen liegt. Diese Straftaten werden schlicht nicht öffentlich zugänglich gehandelt.

   Da ICANN nicht für Inhalte im Internet zuständig ist, liegen wenige Angaben zu länderabhängigen Geschwindigkeiten bei der Löschung von Inhalten vor. Allerdings zeigen Statistiken[13], dass die Löschung am langsamsten in den Ländern USA, Australien und Deutschland geschieht. Schnelle Löschungen sind vor allem in Russland und den angrenzenden Ländern zu verzeichnen.[14] Es ist bekannt, dass lokale Polizeibehörden die Löschung von schwer kriminellen Inhalten bis zu einigen Monaten verzögern, weil sie die Kommunikationspartner der Betreiber ausfindig machen wollen.

   Völlig anders liegt die Lage bei der Ausweitung des Begriffes auf Jugendanscheinspornographie und bei der Anhebung der Altersschranken. Diese Ausweitung des Straftatbestandes kommt einer Verharmlosung der schweren Kindesmisshandlung gleich, indem diese mit einer Zeichnung auf das gleiche Niveau gestellt wird. In analoger Form ist in der Kriminalstatistik deutlich die Korrelation zwischen Ausweitung des Tatbestandes und dem Ansteigen von Straftaten zu erkennen. Dagegen ist die Anzahl der in dieser Anhörung thematisierten Straftaten seit Jahrzehnten auf einem sehr niedrigen Niveau gleich geblieben.[15] Ein erneuter Missbrauch der missbrauchten Kinder zur Durchsetzung eines ungeeigneten Gesetzes erscheint zumindest moralisch fragwürdig.

[13] "Lawful access restriction using DNS modification", WG5 at ICANN Mexico Meeting, 2009
[14] http://scusiblog.org/?p=463
[15] http://blog.odem.org/2009/05/quellenanalyse.html

3. *Es werden immer wieder Mängel wie fehlende Benachrichtigungspflichten oder Rückmeldungen an die Polizeibehörden und Selbstregulierungseinrichtungen genannt. Inwieweit können Sie diese bestätigen und konkretisieren? Wo bestehen hier konkrete Defizite bei der Zusammenarbeit der Polizeibehörden untereinander oder aber bei der Zusammenarbeit der Polizeibehörden und den Selbstkontrolleinrichtungen und inwiefern gibt es hier durch die neue Vereinbarung zur Zusammenarbeit gemäß „Harmonisierungspapier zum zukünftigen Umgang mit Hinweisen auf kinderpornografische Webseiten beim BKA, den deutschen Beschwerdestellen (eco e.V., FSM e.V., jugendschutz.net) sowie der BPjM" Veränderungen? Wann traten die Änderungen in Kraft bzw. wann wurde das Harmonierungspapier unterzeichnet? Wie war das Prozedere vor der neuen Vereinbarung und welche Änderungen wurden mit welcher Begründung vereinbart?*

   Da ICANN keine Beschwerdestelle für strafbare Inhalte im Internet betreibt, kann diese Frage kaum beantwortet werden. Es ist allerdings auffällig, dass die Beteiligung der Regierungsorganisationen und der Strafverfolgungsbehörden bei ICANN in dieser Hinsicht nur lasch erfolgt. Das Interesse der Regierungsvertreter liegt mehr in der Absicherung von „Hoheitsgebieten" im Internet und der Einflussnahme auf die regulatorischen Entwicklungen. Insbesondere wünschen einige Regierungen ein Vetorecht oder gar die komplette Abschaffung von ICANN zugunsten einer straff geführten Internetzentralregierung, die „Unliebsames" und „Störendes" einfach ausknipsen kann. Diese Forderung verkennt sowohl die Legitimitätsgrundlage von ICANN als auch die technischen Eingriffsmöglichkeiten völlig.

4. *Wie ist das Prozedere bei den Selbstkontrolleinrichtungen? Melden diese die fraglichen Inhalte an die zuständigen Polizeibehörden oder aber über die Partnerhotlines direkt an die entsprechenden Hostprovider? In welchem Zeitraum erfolgt eine Benachrichtigung der Polizeibehörden und der Hostprovider?*

   Da ICANN keine Beschwerdestelle für strafbare Inhalte im Internet betreibt, kann diese Frage kaum beantwortet werden. Nach meiner Kenntnis erfolgen Benachrichtigungen der lokalen Polizeibehörden und keine direkte Benachrichtigung des Providers. Hintergrund dieser Vorgehensweise ist, dass nur die lokale Polizeibehörde wissen kann, ob in diesem Fall eine verdeckte Ermittlung durch die Löschung gestört würde. Es ist bekannt, dass lokale Polizeibehörden die Löschung von schwer kriminellen Inhalten bis zu einigen Monaten verzögern, weil sie die Kommunikationspartner der Betreiber ausfindig machen wollen.

5. *In welchen Intervallen und mit welchen Methoden wird überprüft, ob beanstandete Inhalte gelöscht wurden? In welchen Intervallen erfolgt ein Wiederaufforderung bei Nichtlöschung und welchen Zeitraum sehen Sie hier als sachgerecht an?*

   Bei FastFlux und Conficker erfolgte eine Überprüfung laufend, d.h. in Abständen von wenigen Minuten bis Stunden. Im Falle der Untersuchungen von Florian Walther und des AK Zensur sind Überprüfungsfristen durch automatisierten, versuchten Abruf innerhalb einiger Stunden und Tage einschlägig. Aufgrund fehlender Rückmeldungen in den Strafverfolgungsbehörden liegt der Verdacht nahe, dass gar keine Überprüfungen stattfinden. Sachgerecht ist eine Überprüfung im Abstand einiger Tage. Bei Nichtlöschung ist nach ca. einer Woche ein Nachharken erforderlich. Bei Nichtlöschung innerhalb eines Monats ist eine Eskalation angebracht.

6. *Wenn Aufforderungen zur Löschung beim Hosting-Provider nicht erfolgreich waren, welche alternativen Ansprechpartner haben Sie bzw. Ihre Partnerorganisationen angesprochen, und welche Ansprechpartner könnten Sie sich vorstellen?*

   Zur Eskalation – wie in Frage 5 angesprochen – eigenen sich die Provider selbst, bzw. deren Anschlussprovider. Es ist ebenfalls möglich auf die Domain-Registries zuzugehen, da diese in Ihren AGBs teilweise bestimmte Inhalte ausschließen.

   Die notwendigen Kontaktinformationen finden sich in den Whois-Datenbanken, die alle öffentlich einsehbar sind. Es wird derzeit diskutiert, inwieweit diese Datenbanken noch öffentlich sein müssen. Aus Sicht der Strafverfolgungsbehörden wäre ein Auskunftsersuchen entlang der Delegationskette völlig ausreichend.

   In besonders hartnäckigen Fällen ist es möglich, einen kompletten Provider vom Netz zu nehmen: Ein Beispiel dafür findet sich im Anhang.

   Die meisten Straftaten, bei denen die Polizei im Internet ermittelt, sind allerdings Betrugsdelikte, bei denen diese Auskunftsersuchen unverhältnismäßig und viel zu aufwändig sind. Die Sachbearbeiter sind dann regelmäßig dankbar, in den wenigen Minuten, in denen sie pro Woche Zugang zum Internet haben[16], schnell durch eine Whois-Abfrage an nützliche Informationen zu gelangen.

[16] http://www.sh.gruene-fraktion.de/cms/files/dokbin/357/357096.kleine_anfrage_ausstattung_der_polizei_m.pdf

7. *Gibt es Erkenntnisse dahingehend, welche Art von Inhalten nach 184 b StGB nicht zeitnah gelöscht werden können? Dies betrifft beispielsweise das Alter der Missbrauchs-Opfer und die Art der dargestellten sexuellen Handlungen.*

   Nach aktueller Kenntnis sind Bilder dieser schweren Straftaten überall sehr schnell löschbar.[17] Die eigentlichen Straftaten geschehen aber im privaten Umfeld und in über 99% der Fälle ohne Generierung von Bildmaterial.[18] Für Jugendanscheinspornographie sieht es dagegen anders aus: Das Material ist in den meisten Ländern völlig legal und entzieht sich somit zu Recht jeder Löschaufforderung. Insbesondere Manga-Comics sind im asiatischen Kulturkreis keine Straftat, sondern Bestandteil der Alltagskultur.[19]

   Insofern kommt die Ausweitung des Straftatbestandes einer Verharmlosung der schweren Kindesmisshandlung gleich, die die Ressourcen der Ermittlungsbehörden bindet, anstatt den tatsächlichen schweren Kindesmissbrauch zu unterbinden. Die Ausweitung der Straftatbestände führt somit direkt zu einem nachhaltigen Schutz der aktuellen Täter und verlängert die Qualen der Betroffenen.

8. *Gibt es aussagekräftige Erkenntnisse über die Intensität von Strafverfolgungsmaßnahmen in Ländern, die über eine Sperrinfrastruktur verfügen, im Vergleich zu den Ländern, die keine Sperrung vornehmen? Mit welchen Verfahren – also Löschen oder Sperren – ist eine bessere Strafverfolgung der Täter möglich oder haben die Sperrungen Auswirkungen auf die Strafverfolgung? Lassen sich statistische Aussagen dahingehend treffen, dass die Strafverfolgung zu- bzw. abnimmt?*

   Das Verfahren „Löschen“ bietet den lokalen Polizeibehörden Zugriff auf die Täter, die dieses Material verbreiten, da die Täter ja Kontakt zu den Providern aufnehmen mussten, um die Daten bereitzustellen.

   Das Verfahren „Sperren“ enthält keinerlei Benachrichtigungsoption und verdeckt weitere Ermittlungen.[20] Der Vorfall wird mit dem Verfahren „Sperren“ aus dem Bewusstsein der handelten Strafverfolger verdrängt, anstatt die anstrengende Arbeit zu Ende zu führen. Entsprechende bestätigende Aussagen sind seitens der Strafverfolgungsbehörden in den skandinavischen Ländern bekannt geworden.[21]

[17] http://www.bmfsfj.de/bmfsfj/generator/RedaktionBMFSFJ/Internetredaktion/Pdf-Anlagen/vertrag-access-blocking-internationale-lage,property=pdf,bereich=bmfsfj,sprache=de,rwb=true.pdf
[18] http://mogis.wordpress.com/2009/04/29/kern-der-debatte/
[19] http://de.wikipedia.org/wiki/Manga#Literatur
[20] http://www.kjm-online.de/files/pdf1/Gutachten_Sperrverfuegungen_Recht_2008.pdf
[21] http://www.heise.de/newsticker/BKA-Sperrung-von-Kinderporno-Seiten-ist-wirksam-Update--/meldung/135360

9. *Welche Erfahrungen haben Länder, in denen Netzsperren verpflichtend eingeführt wurden, bisher gemacht? In welchem Verfahren werden im Ausland die für die Liste mit Netzsperren notwendigen Daten erhoben? Wie ist sicher gestellt, dass entsprechende Listen mit zu sperrenden Seiten (gelbe Seiten der Kinderpornographie) nicht in der Öffentlichkeit zugänglich gemacht werden können, wie in anderen Ländern geschehen? Ist die Anzahl der Meldungen bei den Hotlines/Behörden in den Ländern, in denen gesperrt wird, nach Einführung der Sperrung signifikant zurückgegangen?*

   Details zu den Erfahrungen – bis auf die Antwort zu Frage 8 – sind nicht bekannt.

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

    Die Fragestellung suggeriert, dass Zentralisierung nur mit „Sperren“ möglich sein. Dies ist aber unrichtig.

    Gebraucht werden eine deutlich effektivere Zusammenarbeit der Strafverfolgungsbehörden auf internationaler Ebene, insbesondere eine Verkürzung der Meldewege und ein verlässliches Rückmeldeverfahren. Auf diese Weise können die meldenden Behörden die Akte offen lassen und somit zum integralen Bestandteil der Überprüfungskette werden. Diese Überprüfbarkeit erhöht den psychologisch wichtigen Erfolg seitens der Mitarbeiter der Behörden, die so merken, wie ihre Arbeit Früchte trägt, anstatt wie bisher den Vorgang an unbekannt mit unbekanntem Ergebnis abgeben zu müssen. Genau diese Überprüfbarkeit und der Erfolgsdruck machen „Sperren“ als Methode ungeeignet: Die Inhalte bleiben ja weiter abrufbar.

11. *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. phishing-sites. 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 phishing-sites durchzuführen?*

    Fehlende Rückmeldungen und mangelnde Durchgriffsmöglichkeiten erschweren die Arbeit erheblich. Bei Phishing-Seiten kommt hinzu, dass die Provider leicht eine Nachahmung einer Bankenseite erkennen können und die Banken in schwierigen Fällen die Möglichkeiten des Namensmissbrauchs[22] ausspielen können.

    Klare Fälle von Kinderpornographie sind so selten, dass diese statistisch irrelevant sind. Die unklare internationale Rechtslage bei Jugendanscheinspornographie macht es den Providern schwer, überhaupt eine Aussage über die Illegalität der Inhalte treffen zu können. Sie sind praktisch immer auf juristischen Beistand angewiesen. Insbesondere in den USA ist das ein erheblicher Verzögerungsgrund, weil die Provider sich zwangsweise an die lokale Polizeibehörde werden müssen und diese die Entscheidung zu treffen hat.

    Im Falle genau dieser Untersuchung hat ICANN eine Lehre gezogen und FastFlux Techniken massiv eingeschränkt, so dass sich die Zeiten für ein erfolgreiches Notice-and-Take-Down drastisch verringert haben, wie auf Seite 3 ausgeführt wurde.

12. *Wie kann die Zusammenarbeit zwischen den Strafverfolgungsbehörden, den Selbstregulierungskräften der Privatwirtschaft wie INHOPE und den Internet Service Providern weiter verbessert werden?*

    Seitens ICANN ist dazu keine Aussage möglich.

[22] http://www.icann.org/en/udrp/

13. *Welche Erkenntnisse gibt es darüber, ob und inwieweit es einen kommerziellen Markt für diese Inhalte nach § 184 b gibt?*

    Alle bekannten Untersuchungen verneinen die Existenz eines kommerziellen Marktes, insbesondere eines Massenmarktes. Es gibt keinerlei Quellen für diese Marktthese, wenn man von unseriösen Hochrechnungen absieht, die auf der unzulässigen Vermischung von Straftatbeständen beruhen. Die gern zitierte Quelle der NSPCC für einen Massenmarkt stellt diese These aber gar nicht auf, im Gegenteil: Sie verneint diesen Markt ausdrücklich.[23] Auch der Rechtanwalt Udo Vetter verneint den Markt[24] und befindet sich damit im Einklang mit dem Bund Deutscher Kriminalbeamter[25] und dem LKA München[26] sowie Europol[27].

14. *Welche Maßnahmen sind sinnvoll und geboten, um gegen die aktive Nachfrage vorzugehen?*

    Die Existenz eines Marktes sowie die Anfixthese werden durchweg bestritten[28], wie in der Antwort zu Frage 13 dargelegt. Demzufolge ist die Konzentration auf das Internet bei der Bekämpfung von schwerer Kindesmisshandlung nicht mehr als ein Ablenkungsmanöver. Selbst das BKA konzentriert sich in den eigenen Unterlagen[29] ausschließlich auf das persönliche Umfeld der Kinder.

15. *Mit welchem Verfahren (Sperren oder Löschen) können die Täter strafrechtlich besser verfolgt werden?*

    Effektiv ist die Verhinderung von schwerer Kindesmisshandlung. Dies kann nur dort geschehen, wo die Misshandlung stattfinden: **Im realen Leben.** Das Internet zu kriminalisieren, ist nicht mehr als ein Wahlkampftrick.

[23] http://www.nspcc.org.uk/inform/research/briefings/imagesofchildabuse_wda48219.html
[24] http://www.lawblog.de/index.php/archives/2009/03/25/die-legende-von-der-kinderpornoindustrie/
[25] http://www.heise.de/newsticker/Polizei-fehlt-Ruestzeug-fuer-Internet-Ermittlungen--/meldung/136680
[26] http://www.sueddeutsche.de/panorama/813/465404/text/19/
[27] http://www.heise.de/newsticker/Familienministerin-kaempft-an-allen-Fronten-fuer-Kinderporno-Sperren--/meldung/132448
[28] http://blog.beck.de/2009/04/22/gesetzentwurf-zu-internetsperren-im-kabinett-beschlossen
[29] http://www.bka.de/kriminalwissenschaften/veroeff/band/band34/band34_vergewaltigung.pdf

Das folgende Dokument wurde durch ICANN zur Unterstützung dieser Stellungnahme angefertigt. Das Dokument wurde von folgenden Personen angefertigt: Heidi Ullrich, Director for At-Large; David Olive, Vice-President for Policy Development; Dave Piscitello, Senior Security Technologist; Matthias Langenegger, ICANN staff.

Response to Request of Lutz Donnerhacke:

Overview

· ICANN, the Internet Corporation for Assigned Names and Numbers, is best known for its role as the technical coordinator of the Internet's Domain Name System.

· The *Affirmation of Commitments*, signed in September 2009 by ICANN and DOC, solidified ICANN's status as a private sector, multi-stakeholder, not-for-profit corporation that manages Internet resources for the public benefit.

· ICANN performs technical and policy coordination of Internet names and numbers (technically, *domain names*, *IP addresses*, and *port and parameter numbers*) under a separate contract with DOC - the *IANA Functions contract*. The central coordination of these functions is a major reason there is one unified global Internet rather than individual national Internets.

· ICANN has about 130 staff members, located in the United States, Europe, Australia and other locations around the world.

Response to Query

With respect to content filtering or access blocking, the mission statement and page at ICANN is quite clear:

"... issues of concern to Internet users, such as the rules for financial transactions, Internet content control, unsolicited commercial email (spam), and data protection are outside the range of ICANN's mission of technical coordination"(Source: http://www.icann.org/tr/english.html).

ICANN is a technical coordinator of registries - databases of names and numbers. ICANN does not host web or other content, provide access to the Internet (bandwidth), or facilitate policy for these issues of concern.

Depending on the jurisdiction(s) involved, law enforcement (LE) works with CERTS, courts, government agencies (like the FTC) and of course other law enforcement to investigate criminal activity. When they have sufficient evidence, they typically get court orders to block access.
How this evolves in multi-jurisdictional cases varies depending on treaties, relationships between LE and governments involved, etc.

When LE approaches ICANN, we cooperate in a manner appropriate to the specific circumstance. Sometimes we lend technical expertise. Sometimes we share information or facilitate communications between LE and our contracted parties.

Article describing the `typical route for law enforcement (at least in the US):`

::
SearchSecurity.com: Security Wire Daily
Breaking security news, the latest industry developments and trends May 25, 2010
::

JUDGE ORDERS PERMANENT SHUTDOWN OF ROGUE ISP, INSTRUCTED TO FORFEIT $1 MILLION TO FTC
Robert Westervelt, News Editor

A rogue ISP that housed the backbone of a number of cybercriminal operations, including botnet command-and-control servers, malware and child pornography, has been permanently shut down by a court order Wednesday.

U.S. District Court Judge Ronald M. Whyte ordered all operations of Web hosting provider Triple Fiber Network (3FN.net), operated by Pricewert LLC, permanently halted and said the rogue ISP's servers, facilities and other equipment would be sold by a court-appointed receiver in 120 days. In addition Whyte ordered the ISP to turn over $1.08 million in revenue it made as a result of the operations to the Federal Trade Commission.
Read more: http://go.techtarget.com/r/11638960/7997906

Additional Reference Material:

Presentation entitled “Standards and Polices Affecting Security: Where does ICANN fit” by Dave Piscitello, ICANN Senior Security Technologist, delivered at an INTERPOL Information Security Conference: http://securityskeptic.typepad.com/files/iisc_2010_piscitello.pdf

Conficker Summary and Review: http://www.icann.org/en/announcements/announcement-11may10-en.htm

Presentations from the Forum DNS Abuse that took place during the ICANN meeting in Brussels in June 2010: http://brussels38.icann.org/node/12513

Meeting information from a session on Proposals for Improvements to the RAA that took place during the ICANN Meeting in Brussels in June 2010: http://brussels38.icann.org/node/12460

Presentations from the Forum DNS Abuse that took place during the ICANN meeting in Nairobi in March 2010: http://nbo.icann.org/node/8917