KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

Le service national de coordination de la lutte contre la criminalité sur Internet

Il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet

The Swiss Coordination Unit for Cybercrime Control

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität KOBIK

Jahresbericht 2007

INDEX

1. Das Wichtigste in Kürze

- Das fünfte Betriebsjahr von KOBIK zeichnet sich durch einen markanten Anstieg der Meldungen aus der Bevölkerung aus. Mit über 10'000 Meldungen führte KOBIK eine wichtige Triagearbeit durch und konsolidierte seine Rolle als nationaler Ansprechpartner in Sachen Internet-Kriminalität. KOBIK leitete im vergangenen Jahr, die Fälle der eigenen Recherche eingerechnet, 734 Fälle an in- und ausländische Strafverfolgungsbehörden weiter.

- Die steigende Zahl der Meldungen ist auf das starke Wachstum im Bereich der Wirtschaftskriminalität zurückzuführen. Ab Mai 2007 war auch die Schweiz, wie zuvor andere europäische Länder, vermehrt Opfer der internationalen Cyberkriminalität. Die Attacken gegen Finanzinstitute wurden mittels Spamwellen durchgeführt, um so die Schadsoftware auf zahlreiche schweizerische Rechner zu verbreiten.

- Die Meldungen der Bevölkerung konzentrierten sich in erster Linie auf die harte Pornografie (19.91%). Wie im Jahr 2006 waren auch im Berichtsjahr die Spams ein häufiger Meldungsanlass. Eine beachtliche Zahl von Meldungen konnte nicht überprüft werden, da diese Seiten schon zum Zeitpunkt der automatischen Analyse nicht mehr erreichbar waren. Dies zeugt unter anderem auch von einer steigenden Dynamik des Internets..

- Wie schon in vergangenen Jahren konnte aufgrund der KOBIK Dossiers auch im Berichtsjahr eine hohe Erfolgsquote erzielt werden. Die KOBIK Verdachtsdossiers sind offensichtlich eine zuverlässige Grundlage, um ein Strafverfahren gegen verdächtige Personen zu eröffnen und anlässlich einer Hausdurchsuchung illegales Material zu beschlagnahmen, so dass die Verurteilung der Verdachtspersonen die Regel ist.

- Aufgrund des Feedbacks der Strafverfolgungsbehörden kann allerdings eine Tendenz festgestellt werden, dass vermehrt versucht wird, illegales Material auf den Rechnern zu verstecken oder zu eliminieren. In fast 10% der Fälle wurden Verschlüsselungsprogramme oder Software zur unwiderruflichen Löschung der Daten verwendet.

- KOBIK hat in über hundert Fällen illegale Seiten direkt den Providern gemeldet. Aufgrund der Meldung von KOBIK wurden diese Seiten vom Netz genommen.

- Die Leitung von KOBIK zieht nach 5 Jahren eine positive Bilanz und ist überzeugt, dass das KOBIK als nationales Kompetenzzentrum gerüstet ist für künftige Herausforderungen.

2. Meldungseingang

Im Jahr 2007 gingen bei KOBIK rund 10'100 Verdachtsmeldungen ein. Die Zunahme von Delikten im Bereich der Wirtschaftskriminalität führte gegenüber dem Vorjahr zu über 3000 zusätzlichen Meldungen. Auf diese Spamattacken mit Trojanern gegen Schweizer Banken haben viele Betroffene jeweils umgehend reagiert und KOBIK Meldung erstattet.

Abbildung 1 Meldungseingänge über www.kobik.ch

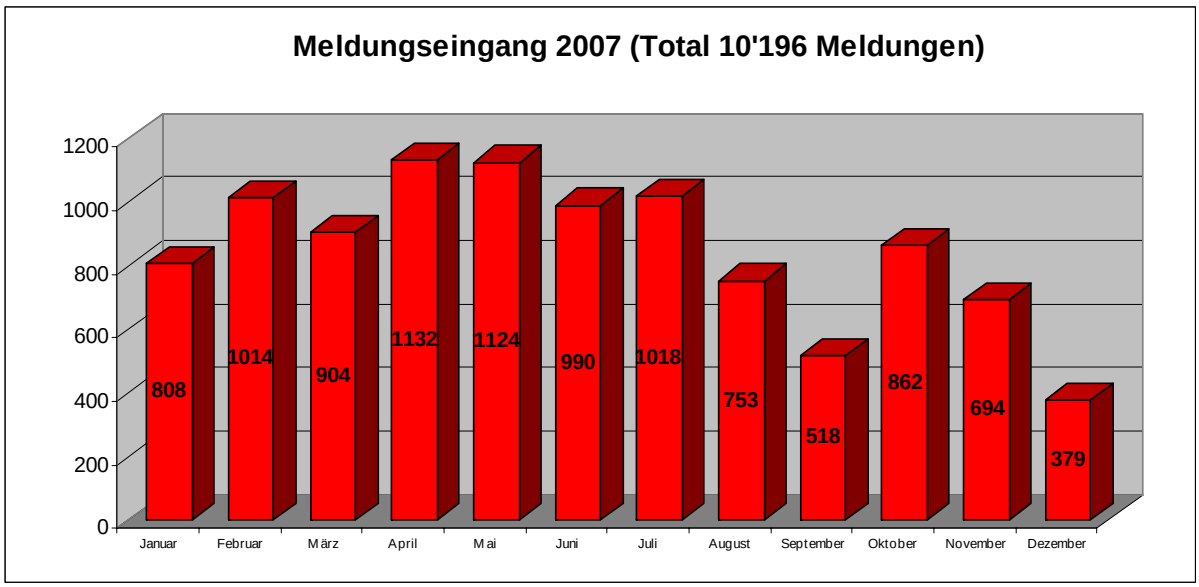
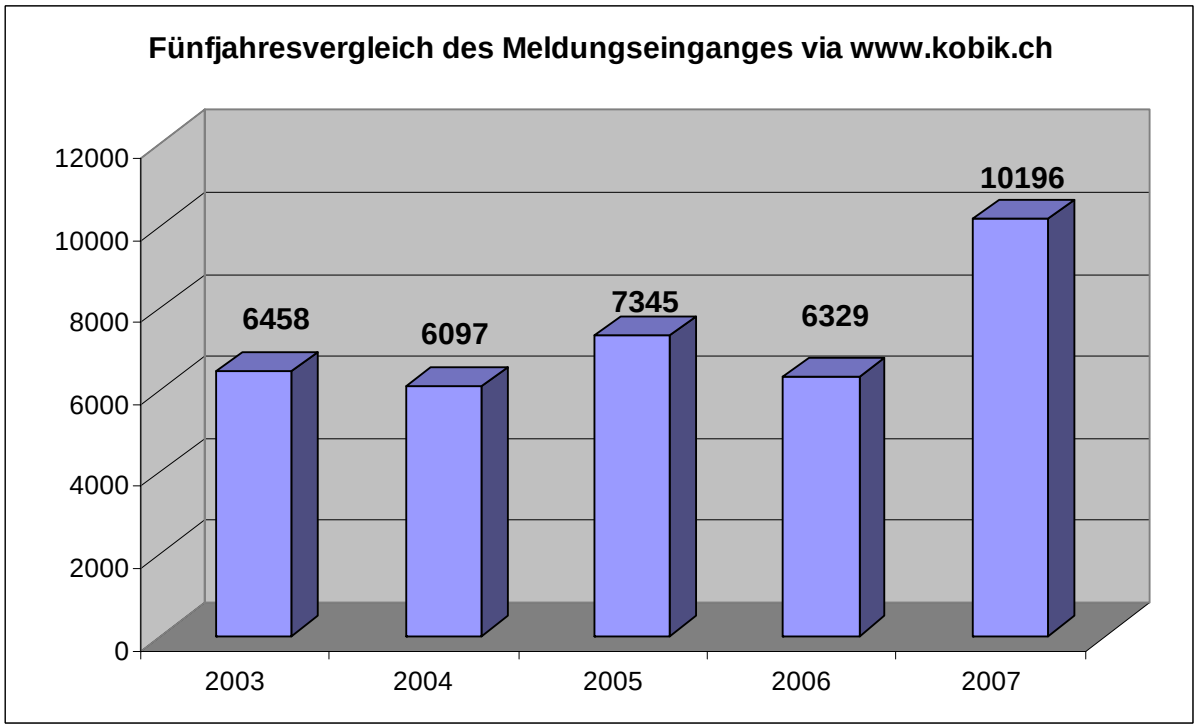


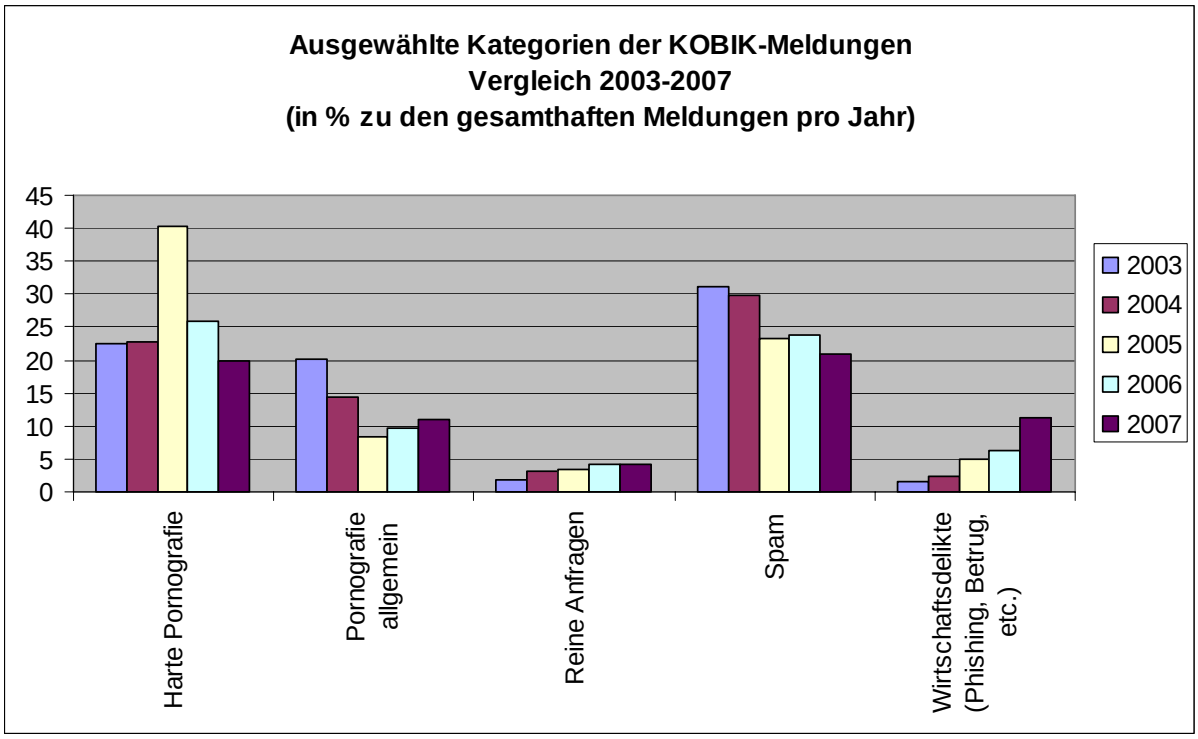
Abbildung 2 Meldungseingänge über www.kobik.ch im Fünfjahresvergleich



3. Was wurde gemeldet ?

Die Tendenzen, welche KOBIK in den vergangenen Jahren aufgezeigt hat, bestätigten sich im Berichtsjahr 2007. Die Abbildung 3 zeigt, wie die Kategorie Wirtschaftskriminalität ein konstantes Wachstum über die letzten fünf Jahre erfahren hat. Die häufigsten Meldungen werden in dieser Kategorie in den Bereichen Phishing, Vorschussbetrug und betrügerischen Gratisangeboten verzeichnet. Dieses Phänomen lässt sich durch verschiedene Begleitumstände erklären: Einerseits hat die Verlockung des Gewinns dazu geführt, dass viele Personen Schadsoftware nicht mehr nur aus „Spass" sondern für Geld programmieren; andererseits kann auch eine Steigerung der Professionalisierung der Instrumente und der Software beobachtet werden, d.h. die Technik und demzufolge auch die Resultate wurden verfeinert und verbessert und bedürfen nicht mehr der aktiven Beteiligung des Benutzers. In Fällen, in denen die aktive Beteiligung des Benutzers doch noch gefragt ist, ist eine starke Professionalisierung im Auftreten und in der Täuschungsabsicht erkennbar.

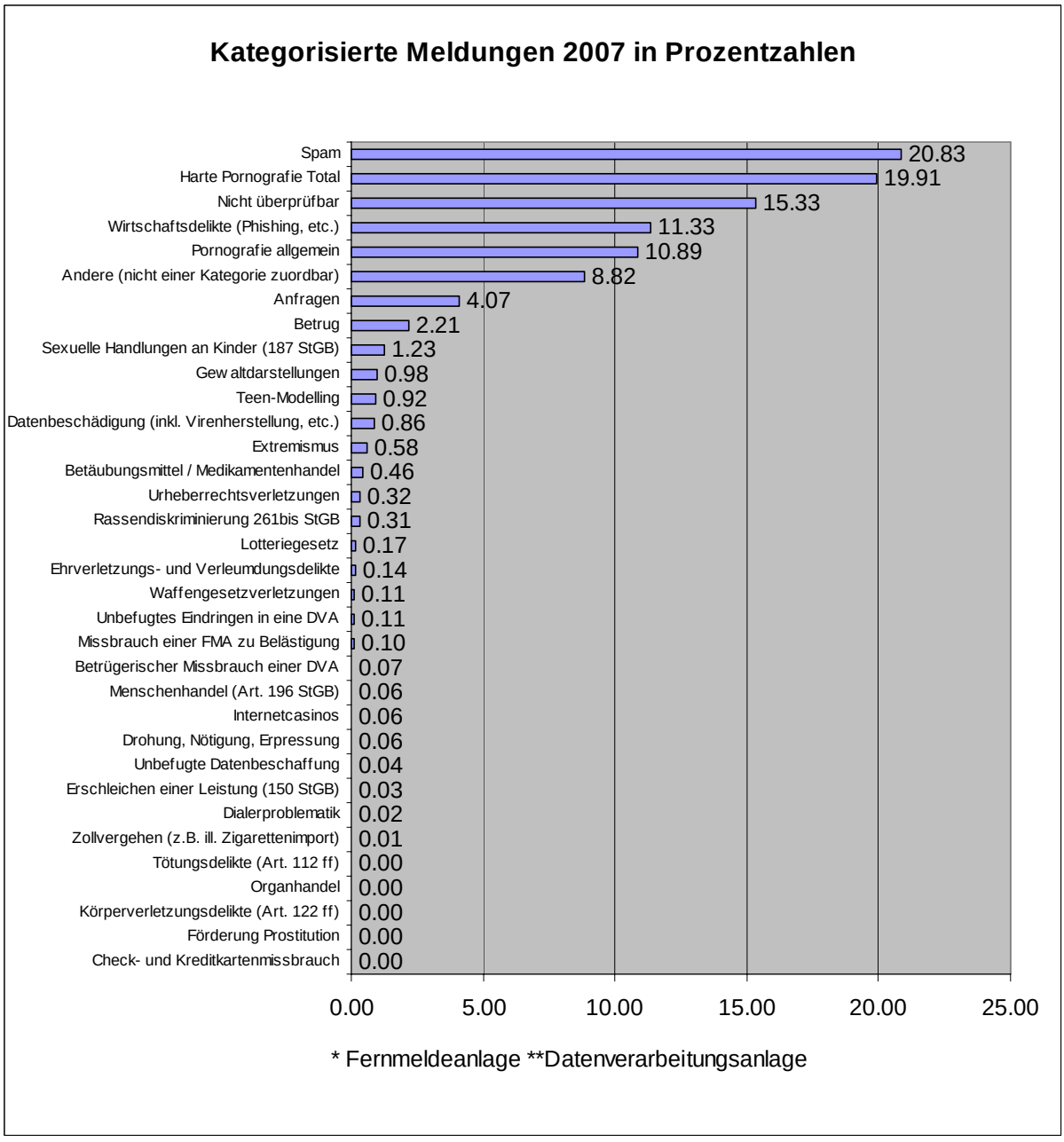
Abbildung 3 Ausgewählte Kategorien im Fünfjahresvergleich



Im Bereich der harten Pornografie, insbesondere der Kinderpornografie, wurde am meisten Verdachtsmeldungen verzeichnet. Auch die Kategorie „Nicht überprüfbar" ist beachtlich. Diese entsteht dadurch, dass ein gewisser Anteil an Meldungen nicht überprüft werden konnten, weil die gemeldeten URLs schon zum Zeitpunkt der automatischen Analyse nicht mehr aktiv waren. Ein Grund scheint darin zu liegen, dass eine grosse Zahl von Seiten mit illegalen (insbesondere kinderpornographischen) Inhalten bei Gratis-Hosting-Providern gehostet werden. Wird die URL entdeckt, wird diese durch den Administrator umgehend gelöscht. Der Produzent hat allerdings Kopien dieser Seite im ganzen Internet verbreitet, welche eine nach der anderen akti-

viert werden. Dies ist unter Umständen ein Hinweis, dass die „bulletproof hosting“[1]-Methode im kinderpornografischen Umfeld noch nicht sehr verbreitet ist.

Abbildung 4 Was wurde KOBIK von der Bevölkerung gemeldet ?



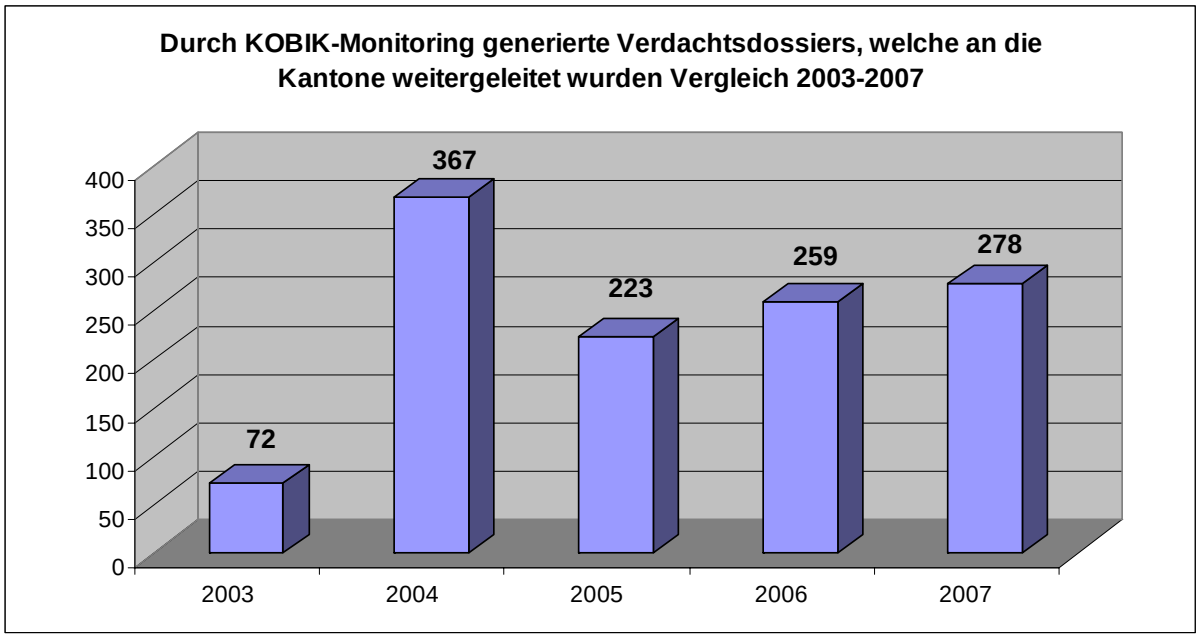
4. Aktive Recherche (Monitoring)

Nebst den 88 Verdachtsdossiers, die sich aus der Bearbeitung der Publikumsmeldungen ergaben, konnte KOBIK durch eigene Recherchen in P2P-Netzwerken, Chats und Foren weitere 278 Verdachtsfälle generieren und an die nationalen Straf-

[1] Als "bulletproof hosting" bezeichnet man Methoden, Inhalte so im Internet zu speichern und zugänglich zu machen, dass die Strafverfolgungsbehörden nicht resp. nur schwer dagegen vorgehen können.

verfolgungsbehörden weiterleiten. Entsprechend dem vom Leitungsausschuss definierten Leistungsauftrag handelt es sich dabei durchwegs um Verdachtsfälle bezüglich des mehrfachen Besitzes und der Verbreitung von Kinderpornografie.

Abbildung 5 Durch aktive Recherche generierte Verdachtsdossiers



5. Adressaten der Verdachtsdossiers

Mit Ausnahme des Kantons Appenzell Innerhoden wurden sämtliche Schweizer Kantone durch KOBIK mit Verdachtsdossiers bedient. Generell kann der Schluss gezogen werden: je grösser die Internetpopulation, desto zahlreicher die Verdachtsdossiers.
Insgesamt leitete KOBIK 368 Verdachtsdossiers über Interpol an ausländische Polizeistellen (vor allem USA und Russland) weiter.

Abbildung 6 Weitergeleitete Verdachtsdossiers

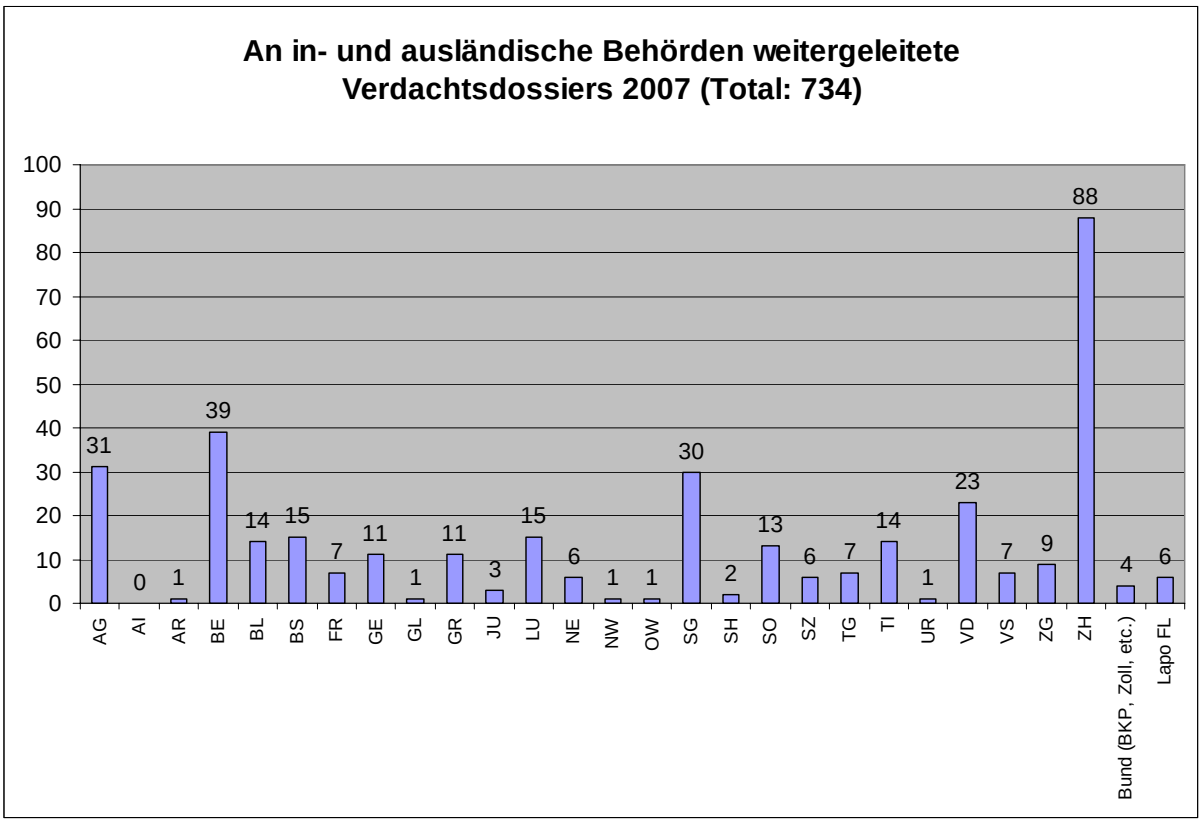
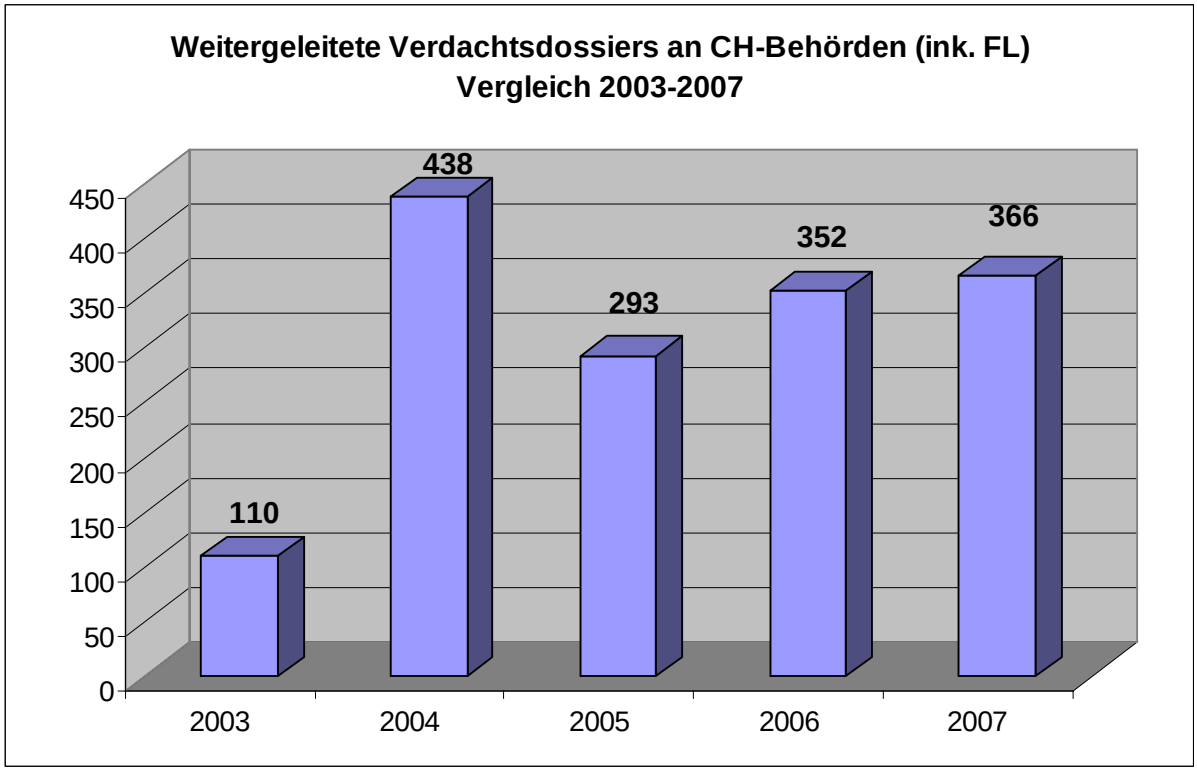


Abbildung 7 Weitergeleitete Verdachtsdossiers



6. Präventionsarbeit

KOBIK war auch im Laufe des Jahres 2007 im Präventionsbereich aktiv. Die enge Zusammenarbeit mit der Schweizerischen Kriminalprävention (SKP) im Bereich der nationalen Kampagne „Stopp-Kinderpornografie“ ging auch im Berichtsjahr weiter. KOBIK ist zudem ein Partner des Präventionsprogramms „Security for Kids“ von Microsoft Schweiz. Weiter hielten KOBIK-Mitarbeiter im vergangenen Jahr verschiedene Präventionsvorträge anlässlich von Lehrerkonferenzen, Versammlungen von Elternvereinen und Kinderschutzorganisationen.

7. Politische Vorstösse auf Bundesebene

Folgende parlamentarische Vorstösse wurden im Berichtsjahr eingereicht:

07.3449 Motion Amherd

Virtueller Kindsmissbrauch im Internet. Neuer Straftatbestand: In dieser Motion wird der Bundesrat aufgefordert, virtuellen Kindsmissbrauch und die Anbahnung eines eindeutigen sexuellen Dialogs zwischen einem Kind und einer offensichtlich erwachsenen Person unter Strafe zu stellen. In virtuellen Parallelwelten wie z.B. „Second Life“ würden virtuelle Kinder durch Mitspieler missbraucht und vergewaltigt werden. Auf gesetzlicher Stufe sei klarzustellen, dass es sich dabei um ein kinderpornografisches Angebot handle, welches unter Strafe steht.
Der Bundesrat hält in seiner Antwort vom 28.09.2007 fest, dass die Motion (a) mit dem virtuellen Kindsmissbrauch und (b) der Anbahnung eines sexuellen Dialogs zwi-

schen einer erwachsenen Person und einem Kind zwei verschiedene Themenkreise zum Gegenstand habe, die einer gesonderten Behandlung bedürfen:
(a) Der Bundesrat hält fest, dass im Bereich virtuellen Kindsmissbrauch prima vista kein gesetzgeberischer Handlungsbedarf besteht, da Art. 197 StGB nicht nur reale, sondern auch virtuelle Darstellungen von sexuellem Missbrauch von Kindern erfasst. Der Bundesrat ist aber bereit, die sich stellenden Fragen im Detail abzuklären und nötigenfalls eine geeignete Ergänzung des Strafgesetzbuches vorzuschlagen.
(b) Der zweite Teil der Motion („Anbahnung eindeutig sexueller Dialoge mit Kindern" im Internet) zielt auf das sog. „Grooming" ab. „Grooming" meint das Führen eines Internet-Dialoges zwischen einer erwachsenen Person und einem Kind, dem dabei ein Treffen zur Vornahme von strafbaren sexuellen Handlungen vorgeschlagen wird. Bereits mehrere Staaten haben ihre Gesetze inzwischen dahingehend geändert, dass sich bereits strafbar macht, wer im Verlaufe eines sexuellen Internet-Dialoges einem Kind ein Treffen zur Vornahme von sexuellen Handlungen bloss vorschlägt. Es scheint sinnvoll, die Einführung einer gesetzlichen Regelung gegen das „Grooming" auch in der Schweiz zu prüfen. Der Bundesrat unterstützt die Motion, behält sich aber vor, die Notwendigkeit entsprechender Regelungen einer eingehenden Überprüfung zu unterziehen und allenfalls vorzuschlagen, auf eine Ergänzung des Strafgesetzbuches zu verzichten.

07.3627 Motion Glanzmann-Hunkeler

Registrierungspflicht von Wireless-Prepaid-Karten: In dieser Motion wird der Bundesrat beauftragt, ein Gesetz vorzuschlagen, das Wireless-Prepaid-Karten unter die Registrierungspflicht stellt. Das Gesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) und entsprechende Verordnungen sind dahingehend anzupassen, dass eine Teilnehmeridentifikation auch innerhalb von privaten Netzwerken obligatorisch ist. Insbesondere muss feststellbar sein, welche Rechner einem solchen Netzwerk angeschlossen sind.
Stand der Beratung: Der Bundesrat beantragt die Annahme der Motion. Im Plenum noch nicht behandelt.

07.3628 Motion Glanzmann-Hunkeler

Effizientere Verfolgung von Internetpädophilie: In dieser Motion wird der Bundesrat beauftragt, dass das Bundesamt für Polizei bei den durch die internationale Zusammenarbeit anfallenden Fällen die Angaben zu den Verdachtspersonen direkt ermittelt. Die Kantone sorgen für genügende Ressourcen zur Bearbeitung aller anfallenden Pädophilie-Fälle.
Stand der Beratung: Im Plenum noch nicht behandelt.

07.3629 Motion Glanzmann-Hunkeler

Cybercrime-Konvention: In dieser Motion wird der Bundesrat aufgefordert, dass er unverzüglich das überfällige Ratifikationsverfahren zur Cybercrime-Konvention des Europarats einleitet.
Die Motion begründet das Anliegen damit, dass die Ermittlung von Tätern, die Straftaten unter wesentlicher Nutzung des Internets begehen, sich oft schwierig gestalten. Effiziente und rasche Verfolgung ist unter anderem nur möglich, wenn vor allem die zeitraubende, überformalistisch ausgestaltete Rechtshilfe, die ein rasches Vorgehen und die rechtzeitige Sicherstellung der Spuren verhindert, vereinfacht wird. In diesem internationalen Kontext würde die Ratifizierung der Cybercrime-Konvention die un-

komplizierte Unterstützung und ein schnelles Vorgehen zur Beweissicherung garantieren.
Stand der Beratung: Im Plenum noch nicht behandelt.

07.3509 Motion Büchler

Rechtssicherheit für Anbieter von Internetdienstleistungen: In dieser Motion wird der Bundesrat beauftragt, die Vorlage Netzwerkkriminalität so weiter zu entwickeln, dass eine zivilrechtliche Rechtssicherheit für die Anbieter von Internetdienstleistungen geschaffen wird. Diese soll sich am europäischen und amerikanischen Rechtsrahmen orientieren. Die Vorlage soll Investitionssicherheit schaffen und Innovation begünstigen. Der Bundesrat soll 2008 eine entsprechende Vorlage ins Parlament bringen.
Stand der Beratung: Im Plenum noch nicht behandelt.

07.3510 Motion Büchler

Strafrechtliche Schritte gegen Cyberkriminalität: In dieser Motion wird der Bundesrat beauftragt, dem Parlament 2008 eine Gesetzesvorlage zur Netzwerkkriminalität zu unterbreiten, welche die bestehenden strafrechtlichen Lücken schliesst. Unter anderem wird um Antwort bzgl. der erfolgten Vernehmlassung und der Botschaft erbeten.
Stand der Beratung: Im Plenum noch nicht behandelt.

07.3689 Motion Büchler

Internetkriminalität: In dieser Motion wird der Bundesrat aufgefordert, eine Gesetzesänderung vorzuschlagen, welche die Zuständigkeit bei der Internetkriminalität generell den Bundesermittlungsbehörden überträgt, wenn das Internet zur Tatausübung zentral ist und entweder

- die Tat einen wesentlichen Auslandsbezug aufweist oder
- mehrere Opfer in verschiedenen Kantonen betroffen sind.

Stand der Beratung: Im Plenum noch nicht behandelt.

07.3750 Motion Büchler

Internetkriminalität. Aufstockung der Spezialisten bei den Ermittlungsbehörden des Bundes: In dieser Motion wird der Bundesrat gebeten, den Ermittlungsbehörden des Bundes eine eigene Abteilung zur effizienten und raschen Verfolgung von Internetkriminalität in ihrem Zuständigkeitsbereich zuzuweisen. Insbesondere sind genügend Internetspezialisten anzustellen.
Stand der Beratung: Im Plenum noch nicht behandelt.

07.3751 Motion Büchler

Kampf dem Terrorismus: In dieser Motion wird der Bundesrat beauftragt, dass das Bundesamt für Polizei den Auftrag und die notwendigen Ressourcen erhält, im Internet Informationen zu beschaffen, die auf Verbrechen wie Terrorismus, Menschenhandel, Proliferation, organisierte Kriminalität und Spionage hindeuten. Besonderen Fokus ist dabei auf dschihadistische Webseiten zu legen. Dschihadistische und gewaltextremistische Seiten auf Schweizer Servern sind sofort vom Netz zu nehmen.
Stand der Beratung: Im Plenum noch nicht behandelt.

Folgende parlamentarische Vorstösse wurden im Berichtsjahr im Rat oder in den Rechtskommissionen behandelt:

06.3170 Motion Schweiger

Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf den elektronischen Netzwerken: Der Bundesrat wird aufgefordert, notwendige Massnahmen für eine bessere Bekämpfung der kindsbezogenen Kriminalität im Internet zu ergreifen. Insbesondere sei 1) der vorsätzliche Konsum von harter Pornografie unter Strafe zu stellen und Art. 197 Ziff. 3bis StGB dahingehend abzuändern; 2) Art. 15 Abs. 3 BÜPF sei im Sinne einer verlängerten Aufbewahrungspflicht von Logbuchdateien von 6 auf 12 Monate abzuändern. Die Missachtung dieser Vorschrift sei mit einer angemessenen Strafe zu versehen; 3) es sei weiter eine gemeinsame Liste von Straftaten zu erstellen inkl. neu Art. 197 Ziff. 3bis StGB, welche für Art. 4 BVE und Art. 3. BÜPF gleichermassen gelte; 4) schliesslich sei ein umfassender Aktionsplan zu Sicherung der Inhalte von Internetseiten auszuarbeiten und die Internetanbieter und –hoster in die Pflicht zu nehmen.
Der Bundesrat beantragte anlässlich seiner Stellungnahme vom 24.05.2006 die Annahmen von Ziffer 1 der Motion sowie die teilweise Annahme von Ziffer 2, soweit es um die Schaffung einer Spezialstrafnorm zur Sanktionierung von Verstössen gegen die Aufbewahrungspflicht geht. Er beantragt ferner die Ablehnung von Ziffer 3 und 4 der Motion sowie die teilweise Ablehnung von Ziffer 2, soweit es um die Verlängerung der Aufbewahrungsfrist von Randdaten geht.
Mittlerweilen wurde die Motion vom Ständerat angenommen und die Kommission für Rechtsfragen des Nationalrates hat die Motion vorberaten. Die Kommission beantragt einstimmig, der Motion in einer abgeänderten Form zuzustimmen. Für die Ziffern 3 und 4 des Motionstextes soll lediglich ein Prüfungsantrag erteilt werden.

06.3554 Motion Hochreutener

Ausdehnung der Motion Schweiger auf Gewaltdarstellungen: Mit dieser wird der Bundesrat beauftragt, die Massnahmen, welche er aufgrund der Motion Schweiger 06.3170 (Bekämpfung der Cyberkriminalität zum Schutz der Kinder auf den elektronischen Netzwerken) bezüglich der Straftaten gemäss Artikel 197 StGB trifft, auch bezüglich der Straftaten gemäss Artikel 135 (Gewaltdarstellungen) zu treffen.
Die von Nationalrat Hochreutener am 5. Oktober 2006 eingereichte Motion wurde vom Nationalrat am 20. Dezember 2006 angenommen. Die Kommission für Rechtsfragen des Ständerates hat an ihrer Sitzung vom 5. November 2007 die Motion vorberaten und beantragt ohne Gegenstimmen, der Motion zuzustimmen.

8. Medienauftritte, Lehrtätigkeit und Publikationen

8.1 Medienpräsenz

Wie bereits in früheren Jahren konnte KOBIK im Allgemeinen wieder eine sehr positive Resonanz in den Medien verzeichnen. Zahlreiche Artikel in Printmedien und einige Berichte der elektronischen Medien befassten sich mit der Arbeit von KOBIK.
KOBIK war in den Medien aller Sprachregionen gleichermassen vertreten, was für einen hohen Bekanntheitsgrad spricht.

8.2 Lehrtätigkeit

Im Berichtsjahr nahmen KOBIK-Mitarbeiter als Referenten an nachfolgenden Tagungen und Lehrveranstaltungen teil:

- Cybercop-Diplomlehrgang (Fachhochschule Luzern)
- Masterlehrgang Economic Crime Investigation (Fachhochschule Luzern)
- Masterlehrgang Forensic (Fachhochschule Luzern)
- Nationale Tagung der IT-Ermittler
- Ausbildungsveranstaltung der Staatsanwaltschaft Winterthur
- Gefahren für Kinder im Internet, CVP Murten
- Pro Familia Schweiz – Familien und Medien – Chancen und Risiken
- Vormundschaftsbehörde Basel-Stadt, Netzwerk Kindesschutz, Jugend online – wann und wie sind Kinder und Jugendliche gefährdet?

8.3 Juristische Analysen

- Chatproblematik – Entwicklung und aktueller Stand der Rechtsprechung (Aktualisierung der Abhandlung und Darstellung der Positionen).

- Fundierte Analyse der Plattform „Second Life“ im Vorfeld der Stellungnahme zur Motion Amherd (07.3449).

9. Partnerschaften und Kontakte KOBIK

9.1 Erfahrungsaustausch und Wissenstransfer mit Österreich

Diesen Sommer hielten sich zwei Kriminalbeamte der Meldestelle für Kinderpornografie im Internet des Bundeskriminalamtes Österreich zum Zwecke eines Erfahrungsaustausches und der Intensivierung der Zusammenarbeit beim KOBIK-Team in Bern auf. Im Zuge der Besprechung wurden ihnen auch die Ermittlungsmethoden bei der Verfolgung von kinderpornografischem Material im P2P-Netzwerk vorgeführt. Mit Schreiben vom August erbat das Bundesministerium für Inneres als vorgesetzte Dienststelle, die Unterstützung von KOBIK bei der Installation, Anwendung und Unterhalt dieser speziellen, durch KOBIK modifizierten Software. Zu diesem Zwecke hielten sich im November zwei KOBIK-Mitarbeiter in Wien auf und erbrachten den österreichischen Kollegen/Innen folgende Dienstleistungen:

- Installation der von KOBIK modifizierten Software zur Recherche auf dem P2P-Netzwerk
- Installation des von KOBIK erstellten IP-Filters (Treffer beschränken sich dadurch auf österreichische IP-Bereiche)
- Schulung für Anwendung und Unterhalt der Software

9.2. Zusammenarbeit mit Providern im Bereich Child Sexual Abuse Anti-Distribution Filter

Die Sperrung bekannter Kinderpornografie-Websites, der sog. Child Sexual Abuse Anti-Distribution Filter, nahm im Berichtsjahr den Echtbetrieb auf. Zur Zeit machen 10 Schweizer Provider auf freiwilliger Basis mit und sperren den Zugriff auf kommerzielle Kinderpornografieseiten.
Die Blockade-Aktion richtet sich gegen kommerzielle Anbieter illegaler Kinderpornografie im Ausland. Die Liste der zu bannenden Sites wird international aktualisiert, wobei jeder Eintrag von KOBIK zusätzlich auf die spezifische schweizerische Rechtslage hin überprüft wird.

9.3 Arbeitssitzungen und Erfahrungsaustausch

Im Laufe des Jahres traf sich KOBIK mit Vertretern der kantonalen Polizeikorps (Besuch von oder bei der Kapo VS, BS, BL, GE, Stapo ZH)

Eine Arbeitssitzung im Bereich Chat wurde mit einem Schweizer Provider abgehalten und direkte Kontakte wurden zu einem in der Schweiz ansässigen Registrar[2] wie auch zu einem grossen Anbieter von Online-Speicherplatz geknüpft.

10. Trends

10.1 Wirtschaftskriminalität

Die Wirtschaftskriminalität ist ein Bereich, welcher in den letzten fünf Jahren ein konstantes Wachstum erfahren hat und mit einer steigenden Zahl an Meldungen einhergeht. Das Jahr 2007 steht für den Beginn von Malwareangriffen gegen Schweizerische Finanzinstitute. Schadsoftware wurde eingesetzt, um die Computer von Bankkunden zu infizieren und in ihrem Namen Überweisungen zu tätigen. Angesichts der Effizienz dieser Form von Kriminalität, ist es möglich, dass dieser Modus operandi in den kommenden Jahren in einer weiter entwickelten Form zu einer der beliebtesten Aktivität der kriminellen Netzwerke werden wird.

10.2 Botnetze und kompromitierte Webserver

Der Begriff Botnetze steht für die Summe aller mit einer Schadsoftware infizierten Rechner, welche in einem Netzwerk zusammengeschlossen sind und im grossem Stil für kriminelle Aktivitäten genutzt werden. Unter anderem werden sog. DDoS Attacken (Distributed Denial of Service) über Botnetze geführt. Die ersten Attacken dieser Art wurden im vergangenen Jahr auch in der Schweiz beobachtet: von der kleins-

[2] Ein Domain Name Registrar ist eine Organisation bzw. ein Unternehmen, das Regsistrierungen von Internet-Domains durchführt. Der Registrar wird von der Internet Corporation for Assigned Names and Numbers (ICANN) oder einer Domain Name Registry akkreditiert.

ten Webseite bis zum grossen Provider können alle Dienste, die mit dem Internet verbunden sind, durch DDoS Attacken bedroht sein.
Diese Aktivitäten scheinen erst am Anfang zu stehen und erfordern angesichts der Abhängigkeit kritischer Infrastrukturen von funktionierenden IT-Netzwerken die konsequente Überprüfung und Optimierung des Informationssicherungsprozesses. Die Schweiz hat hier mit der Melde- und Analysestelle Informationssicherung (MELANI) bereits einige auch im internationalen Vergleich beachtliche Schritte unternommen.
Eine weitere Aktivität, welche stark auf dem Vormarsch ist, ist die Kompromitierung von Webservern mit dem Ziel den Rechner der ahnungslosen Surfer zu infizieren. Webbesucher. Diese Technik, auch „drive-by-infection“ genannt, ist momentan sehr erfolgreich und wird laufend verbessert.

Für den Leitungsausschuss KOBIK

Urs von Daeniken

Für KOBIK

Philipp Kronig