

Kobik sucht und findet.

Seit 1. Januar 2003 ist die nationale Koordinationsstelle zur Bekämpfung der Internetkriminalität (Kobik) online. Die Kobik steht der Öffentlichkeit, Behörden und Internet-Service-Providern als Kompetenzzentrum für rechtliche, technische und kriminalistische Fragen zur Verfügung. Wie kompetent, das zeigt die Praxis.

Bundesamt für Polizei, Abteilung IMC, Sektion OSINT/KOBİK-Monitoring. Der Name liest sich wie eine kryptische Aufzählung. Das Firmengebäude liegt eingebettet in einem Wohnquartier in der Nähe des Berner Wankdorfstadions – eher unauffällig. Wer hinein will, braucht einen Ausweis. Hier – hinter verschlossener Tür – wird versteckt recherchiert.

Im Visier stehen alle strafrechtlichen Tatbestände. Zum Beispiel das Verbreiten von harter Pornografie und Gewaltdarstellungen, Wirtschaftsdelikte, extremistische und rassistische Äusserungen, Urheberrechtsverletzungen oder illegaler Waffenhandel und – seit 1. April 2007 – auch das Versenden von unerwünschten E-Mails (Spam).

Wirtschaftsdelikte nehmen zu

Im Jahr 2006 hat die Kobik 6300 Hinweise aus der Bevölkerung erhalten. 24,3 Prozent der Inhalte sind harte Pornografie, also auch Kinderpornografie, 23,8 Prozent unangeforderte Mails, 9,6 Prozent Pornografie allgemein, 4,4 Prozent Wirtschaftsdelikte, 2,2 Prozent Betäubungsmittel-/Medikamentenhandel und 2,1 Prozent Rassendiskriminierung. Die übrigen Tatbestände ergeben die restlichen Prozente.

Auffallend ist die stetige Zunahme von Wirtschaftsdelikten, die sich von Jahr zu Jahr verdoppeln. «Wirtschaftskriminalität im Internet» ist ein weit gefasster Begriff. Er umfasst: E-Mail-Phishing, Geldwäscherei, betrügerische Escrow-Dienste (Internet-Treuhanddienste), Missbrauch von Kreditkartendaten, illegaler Datenerwerb und unzählige andere Betrugsformen. Alle stehen für das gleiche Ziel:

Internetnutzer ausspionieren, um sich finanziell zu bereichern.

Neun Angestellte der Koordinationsstelle befassen sich mit dem Aufdecken dieser Verbrechen. Sie verteilen sich auf drei verschiedene Sparten: das Monitoring, das Clearing und die Analyse. Unterstützt werden sie von all jenen, die via Meldeformular Angaben zu verdächtigen Internetinhalten machen.

Rund 23 Prozent der Eingänge sind Spam-Meldungen. Diese werden nicht nur zur Werbung für Massenprodukte eingesetzt, sondern immer mehr für illegale Aktivitäten wie Phishing oder Verbreitung von Kinderpornografie. Für diese Art von Hinweisen gibt es unter kobik.ch neu eine Spam-E-Mail-Analyse. Dieses Hilfsprogramm ermittelt auf Knopfdruck den entsprechenden Internetprovider. Steckt ein Schweizer Anbieter dahinter – zum Beispiel Cablecom –, kann der Geschädigte den Fall direkt Cablecom melden. Das Gesetz verpflichtet die Anbieter, unerwünschte Massenwerbung zu verhindern. «Mit diesem Analysetool geben wir dem

Nutzer eine Chance, sich zu wehren, und leiten ihn dorthin weiter, wo er Hilfe bekommt», fasst Roger Küffer, Leiter der Abteilung Monitoring, das leidige Thema zusammen. Nutzer sind aber nicht nur Opfer, sondern oft auch Täter, allerdings ohne es zu wissen. Der eigene Computer kann unbemerkt gekapert und mit Viren oder Trojanern infiziert worden sein. Beim Aufstarten verschickt der PC dann automatisch Spams – quasi ferngesteuert. Man spricht in diesem Zusammenhang von Bot-Netzen.

Im Internet auf Streife

Der Name «Koordinationsstelle» wird der Kobik nicht wirklich gerecht. «Ein wesentlicher Teil unserer täglichen Arbeit ist das Generieren von Fällen», sagt Küffer. «Generieren» heisst, aktiv im Internet nach Strafbarem suchen. Das Thema ist vom Leitungsausschuss klar vorgegeben: Es geht um Kinderpornografie. Küffer erklärt: «Wir wissen genau, wonach wir suchen und wo wir die meisten Treffer landen.» Gewisse Barrieren sind den Ermittlern aber vorgegeben: So darf Monitoring nur im öffentlichen – nicht aber im passwortgeschützten – Bereich stattfinden. Provozieren oder Ermitteln unter falschen Vorgaben ist nicht erlaubt. Das Überwachen von Chat-Foren braucht deshalb Zeit und Fingerspitzengefühl. «Wir wissen und beobachten, dass gerade beim Chatten sehr viel Rechtswidriges passiert, und arbeiten deshalb eng mit

Roger Küffer
Leiter der Kobik-Abteilung Monitoring

«Wir wissen und beobachten, dass gerade beim Chatten viel Rechtswidriges passiert, und arbeiten deshalb eng mit den Betreibern von Chat-Räumen zusammen.»



den Chat-Betreibern zusammen. Bluewin beispielsweise hat über 300 ehrenamtliche Mitarbeiter, die Chat-Räume intensiv überwachen.» Die sich daraus ergebenden Verdachtsfälle werden an die Kobik weitergeleitet.

Wo aber trifft man die meisten Fälle? «Hauptsächlich in Peer-to-Peer-Netzen.» Bekannte P2P-Netzwerke sind beispielsweise Gnutella, Fast Track oder eDonkey. Auf diesen «Datenautobahnen» werden unzählige Informationen und Bilder übermittelt – auch Bilder von Kinderpornografie. «Hier filtern wir zwischen 30 und 40 Fälle pro Monat heraus.» Küfner demonstriert an einem Beispiel, wie schnell und unwiderruflich ein Treffer gelandet wird. Und das, obwohl gerade in diesem Moment etliche Millionen Surfer im Netz sind. Er selektiert seine Abfrage nach dem Bezug zur Schweiz. Den Suchbegriff hält er geheim – Insiderwissen. Die Liste ist lang und täuscht auf den ersten Blick. Denn nicht hinter jedem Namen verbirgt sich ein Straftäter. Das herauszufinden und abzuwägen, ist auch Teil der Arbeit. Da hilft die Erfahrung.

Verdächtig – was nun?

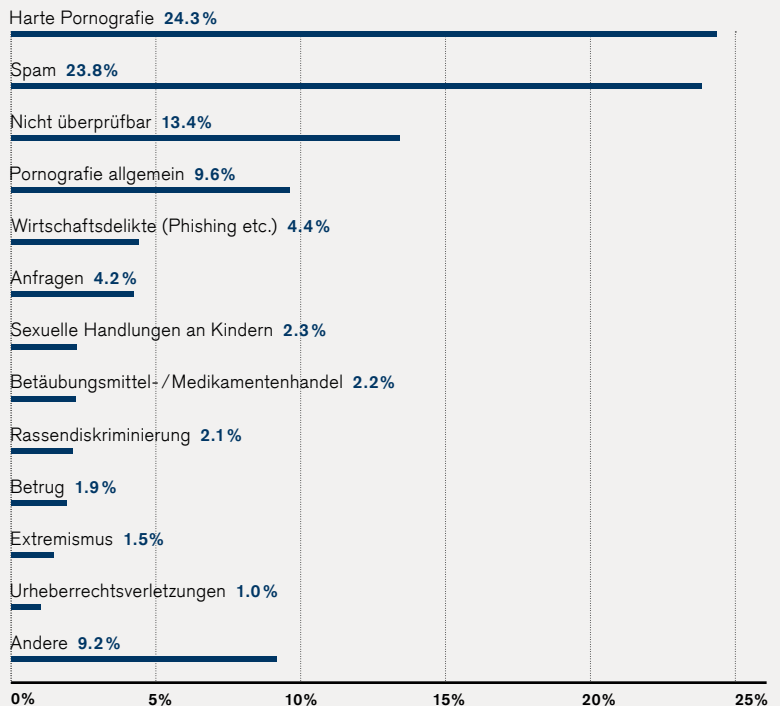
Nachdem alle Hinweise und Verdächtigungen mit Bezug zur Schweiz gerichtsverwertbar gesichert sind, werden die Dossiers an die Kobik-Clearings-Stelle übergeben. Dort werden die Meldungen auf ihre strafrechtliche Relevanz hin überprüft und die verdächtigen Fälle anschliessend an die zuständigen Strafverfolgungsbehörden in den Kantonen weitergeleitet.

Die Kobik hat im letzten Jahr 259 Verdachtsfälle recherchiert. Zwischen 75 und 80 Prozent dieser Fälle werden von der Polizei aufgedeckt. Das sind rund 207 Verhaftungen im Jahr. Mit einem Satz: Die neun Mitarbeiter entlarven jeden zweiten Tag einen Verbrecher – eine «Schreibtischarbeit», die sich lohnt. **fv**

→ Weitere Infos und das Meldeformular für verdächtige Internetinhalte finden Sie unter www.kobik.ch.

Bevölkerungsmeldungen bei der Kobik 2006

Die Trends von 2005 haben sich im letzten Jahr bestätigt: Meldungen zu Kinderpornografie und zu Spam-Mails machen rund die Hälfte aus. Quelle: Kobik



Die wichtigsten Begriffe auf einen Blick

Spam Spam bezeichnet unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Die automatisierte Versendung macht es möglich, mit geringem Zeit- und Geldaufwand eine grosse Anzahl Empfänger zu erreichen.

Phishing Das Wort Phishing setzt sich aus den englischen Wörtern «password» und «fishing» zusammen. Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internetbenutzern zu gelangen.

Schneeballsystem Ein Schneeballsystem charakterisiert sich im Wesentlichen dadurch, dass durch das Anwerben von neuen Teilnehmern, die ihrerseits wiederum eine neue «Generation» von Teilnehmern anwerben sollen, Geldzahlungen an die bisherige Generation zu leisten sind.

Betrug Das Phänomen des Vorschussbetrugs ist seit Anfang der Achtzigerjahre bekannt. Per E-Mail, Fax oder persönlichem Brief werden den Empfängern ausserordentliche Profite in Aussicht gestellt.

Escrow Escrow-Unternehmen treten als Mittler und Verwalter von Zahlungen vor allem bei Internetgeschäften auf, wo ein physischer Kontakt zwischen Käufer und Verkäufer meist nicht herzustellen ist.