Cyberfahnder-Newsletter 4 vom 24.05.2010

Arbeitspapier Cybercrime

Im April 2010 entstand das ▸ **Arbeitspapier Cybercrime** (▸ Download). Es enthält die zentralen Beiträge im Cyberfahnder über die ▸ IT-Sicherheit, die Erscheinungsformen der Cybercrime (▸ Nummerntricks, ▸ Malware, ▸ Botnetze), das ▸ Social Engineering und schließlich über die Schattenwirtschaft im Internet.

Neu ist der Beitrag über den Identitätsdiebstahl und das Phishing. Die älteren Artikel wurden überarbeitet und aktualisiert, soweit das erforderlich gewesen ist.

Im Zusammenhang mit der Underground Economy sind die Aufsätze über die ▸ Schurkenprovider, das ▸ Russian Business Network und über die ▸ arbeitsteilige und organisierte Cybercrime aufgenommen und überarbeitet worden. Den Abschluss bildet der Artikel über den ▸ Basar für tatgeneigte Täter, der erst im April erschienen ist und jetzt aufgrund des neuen Berichts von G Data [1] noch einmal erweitert wurde [2].

Bestandsaufnahme: Cybercrime

Drei Jahre lang hat der Cyberfahnder die Cybercrime und ihre Entwicklungen beobachtet, beschrieben und kommentiert. Das Arbeitspapier stellt eine Bestandsaufnahme dar, eine Zwischenbilanz.

Die Erscheinungsformen der Cybercrime haben sich erheblich gewandelt. Das gilt besonders für das ▸ Phishing. Es hat sich vollständig automatisiert, wobei die Betreiber von Botnetzen und die Phishing-Täter zusammen gewachsen sind.

Für die Cybercrime insgesamt gilt, dass es nicht mehr um das nächtliche Hacken und spielerische Verbreiten von Malware geht, sondern um das Geld verdienen. Die Hacker-Boards sind nur ein Beispiel dafür. Die Professionalisierung der kriminellen Szene zeigt sich an der Leistungsfähigkeit ihrer Malware und den zunehmenden Aktivitäten Organisierter Internetverbrecher, ein Begriff, der von McAfee geprägt worden ist.

Internetkriminalität ist vor allem Betrugskriminalität [3]. Die wahllosen Kampagnen bei dem Phishing und der Verbreitung von Malware wandeln sich immer mehr zu gezielten Angriffen auf ausgewählte Personen und -gruppen. Sie verfolgen das Ziel, persönliche Geheimnisse zu erforschen, die sich missbrauchen oder zu Geld machen lassen.

Die Cybercrime-Szene besteht aus vielen einzelnen Akteuren, die sich immer mehr zu vertrauten Gruppen und festen Bindungen entwickeln. Kriminelle Großprojekte lassen sich nicht mehr im Alleingang bewerkstelligen. Die konsequente Folge daraus ist, dass sich immer mehr bandenmäßige und organisierte Strukturen entwickeln.

Die Strafverfolgung kämpft dagegen verhältnismäßig hilflos an. Nicht, dass es keine Leute mit Kenntnissen, Erfahrungen und Engagement gebe. Sie werden jedoch im Alltagsgeschäft verschlissen und demotiviert.

Ihre Hilflosigkeit beruht deshalb nicht auf fachlichem Unvermögen, sondern auf angestammten Strukturen, Sparzwängen und fehlenden politischen Prioritäten. Für die öffentliche Verwaltung gilt aber insoweit dasselbe wie für die private Wirtschaft: Die Herausforderungen des Internets, der New und der Underground Economy lassen sich nur strategisch meistern. Das erfordert Analyse, strategische Bewertung und zielgerichtete Maßnahmen.

---

[1] Marc-Aurél **Ester**, Ralf **Benzmüller**, Whitepaper 04/2010. Underground Economy - Update 04/2010, G Data 22.04.2010

[2] **CF**, neue Hacker-Boards schotten sich ab, 23.05.2010

[3] PKS 2009: **CF**, Anstieg der Internetkriminalität, 23.05.2010

Skimming

Auch das ▸ **Arbeitspapier Skimming** (▸ Download) wurde überarbeitet und ergänzt.

Seit dem Jahresanfang hat sich in der Rechtsprechung wenig getan. Nur der 2. Strafsenat des BGH drängt darauf, das Ausspähen von Daten nicht auf das Skimming anzuwenden [4].

In 2009 sind nach den Zahlen des BKA insgesamt 960 Geldautomaten in Deutschland zum Ausspähen von Kartendaten und PIN angegriffen worden. Damit sollen Schäden in Höhe von 40 Millionen Euro verursacht worden sein.

Aus meiner niedrigen, regional geprägten Sicht fällt auf, dass die Ausspähungen zugenommen haben, ohne dass ihnen die mächtigen Cashing-Aktionen des Vorjahres gefolgt sind. Zwei Landsmannschaften fallen dabei besonders auf. Die einen sind mit äußerst professionellem Equipment unterwegs und verursachen ganz erhebliche Schäden und die anderen arbeiten eher mit groben Handwerkzeugen und sind deshalb nicht ganz so erfolgreich.

Seit einem Jahr verfolge ich aktiv die gefassten Skimming-Täter aus meinem örtlichen Zuständigkeitsbereich. Dank engagierter Polizeibeamter und Strafrichter ergingen vier Urteile, die alle auf Freiheitsstrafen lauteten, ohne dass den Tätern das Fälschen oder das Cashing vorgeworfen werden konnte, und die alle rechtskräftig sind.

Auch das vom Cyberfahnder veröffentlichte Urteil des Landgerichts Hannover [5] ist rechtskräftig, nachdem der BGH die Revisionen der beiden Angeklagten Ende April ohne Begründung verworfen hat. Das ist deshalb besonders von Interesse, weil die Angeklagten einer sehr weiten Mittäter-Haftung unterworfen wurden.

[4] **CF**, Ausspähen von Daten und das Skimming, 14.05.2010

[5] **LG Hannover**, Urteil vom 17.11.2009 - 6403 Js 43834/09

Vorratsdaten

Mit Urteil vom 02.03.2010 hat das BVerfG die bis dahin geltenden Regeln zur Vorratsdatenspeicherung als nichtig erklärt [6].

Mit den Konsequenzen daraus hat sich der Cyberfahnder kurzfristig auseinander gesetzt [7]. Ich komme zu den Ergebnissen, dass die nach Maßgabe der Einstweiligen Anordnungen des BVerfG wirksam erhobenen Daten weiterhin verwendet werden dürfen, nur nicht als Zufallsfunde seit dem Entscheidungsdatum, weil es seither an einer schwellengleichen Entscheidungsgrundlage fehlt [8].

Zwei Oberlandesgerichte und alle Justizverwaltungen teilen meine Auffassung, soweit sie sich geäußert haben. Nur das Landgericht Verden ist anderer Meinung. Damit kann ich leben.

Von Interesse ist in diesem Zusammenhang auch die ▸ Auskunft der Bundesregierung über Verkehrsdaten. Die Zahlen belegen m.E. eindeutig, dass die Vorratsdatenspeicherung notwendig ist und dass in der Vergangenheit die Auskünfte gezielt zur Bekämpfung der besonders schweren Kriminalität eingesetzt wurden.

Cyberfahnder intern

Der Cyberfahnder besteht aktuell aus rund 800 Textseiten (HTML) und 1.300 Grafiken. Er benötigt knapp 54 Megabyte Speicherplatz.

2009 haben zwei professionelle Abmahner versucht, beim besten Willen überzogene Forderungen gegen mich durchzusetzen, wobei sie ohne Erfolg blieben.

Im Oktober 2009 habe ich das Karaboga-Netz als Schurkenprovider enttarnt und in der Folgezeit erfahren müssen, dass solche Enthüllungen für eine private Veranstaltung, die der Cyberfahnder

[6] **CF**, Vorratsdatenspeicherung ist unzulässig, 02.03.2010;
BVerfG, Urteil vom 02.03.2010 - 1 BvR 256, 263, 586/08.

[7] **CF**, Umgang mit Verkehrsdaten, 07.03.2010

[8] Dieter **Kochheim**, Zum Umgang mit Verkehrsdaten, 08.03.2010;
grundlegend auch: Dieter **Kochheim**, Verwertung von verdeckt erlangten Beweisen, 17.05.2009.

ist, deshalb nicht machbar sind, weil auch Angehörige von den Reaktionen betroffen werden können. Die Karaboga-/Mediaon-Beiträge habe ich im Internet gelöscht und stelle sie auch interessierten Anfragern nicht zur Verfügung.

Diese Beispiele zeigen, dass ein Internetauftritt keine beliebige Spaßveranstaltung ist, sondern ein Projekt, das gut überlegt und abgewogen werden muss. Das Internet ist keine Spielwiese, auf der man ohne Furcht vor Konsequenzen alles treiben kann.

Das bedauere ich nicht, weil ich Rücksichtsnahmen und angemessenes Verhalten in allen Lebenslagen für wichtig halte. Dabei heißt „angemessen“ nicht zwangsläufig auch angepasst und duckmäuserisch. Wenn ich der Meinung bin, dass mir etwas nicht passt, dann muss ich das auch deutlich sagen können. Dazu gehören auch gezielte Normverstöße, wenn sie einen moralischen Grund haben. Dann darf ich aber nicht jammern, weil sich der Angegriffene mit juristischen oder handgreiflichen Mitteln zur Wehr setzt.

Schon jetzt ist der Cyberfahnder ein prähistorisches Artefakt im Internet. Er kann mit den Content-Maschinen nach dem Vorbild von Heise und Wikipedia bei weitem nicht mithalten, seine Technik ist die von klassischen Homepages unter HTML und Charismatiker mit fachlichem Gewicht betreiben keine Webseiten mehr, sondern absondern sich in Blogs. Schon jetzt bin ich gestrig.

Die jüngsten Reaktionen auf den Cyberfahnder lassen hingegen hoffen [9].

[9] **CF**, Werbung für den Cyberfahnder, 21.05.2010