Cyberfahnder-Newsletter 6 vom 28.11.2010

Asimbonang' uCyberfahnder

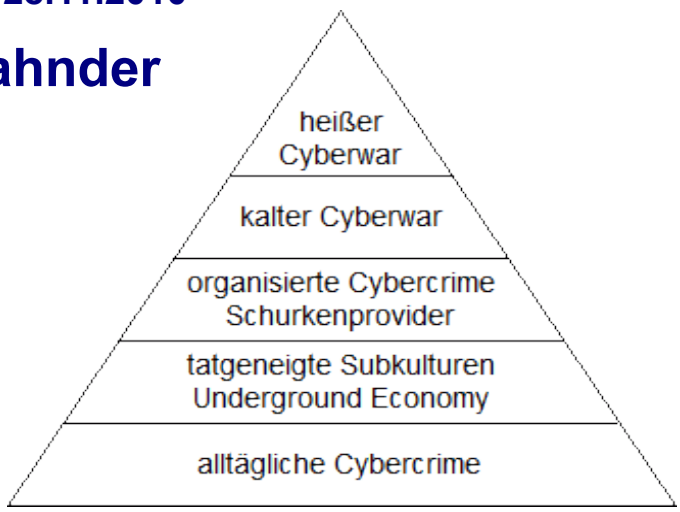
„Asimbonanga“ entstammt der Zulu-Sprache und bedeutet sinngemäß, man habe ihn lange nicht gesehen. Auch: Lied von Johnny Clegg & Savuka als Hommage an Nelson Mandela.

Cybercrime und Cyberwar

Im Juni 2010 habe ich das ▸ Arbeitspapier Netzkommunikation veröffentlicht, das eine erste Verbindung zwischen der Cybercrime und dem Cyberwar hergestellt hat [1]. Als Cyberwar verstehe ich den strategischen Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt. In ihm kämpfen nicht nur Staaten, sondern mit verschiedenen Motiven auch Kriminelle, Terroristen, politische Eiferer und nicht zuletzt Wirtschaftsunternehmen. Ihre Werkzeuge sind zunächst vor allem Botnetze, gezieltes Hacking, Malware und die Methoden des Social Engineering.

Nach meinem Eindruck befinden wir uns in einer noch kalten Phase des Cyberwars, in der die Beteiligten ihre Claims abstecken, die Leistungsfähigkeit ihrer Gegner testen, sie ausforschen und mit Nadelstichen provozieren. Das dazu erforderliche Wissen und Personal ist weitgehend dasselbe, das auch die qualifizierte Cybercrime betreibt.

In seiner heißen Phase, die ich nicht erleben möchte, werden neben den informationstechnischen Methoden auch militärische, terroristische und kriminelle Aktionen zum Einsatz kommen, ohne dass sich die Akteure um das Völkerrecht kümmern werden [2].



Das Verhältnis zwischen Cybercrime und Cyberwar sehe ich in dem oben abgebildeten Entwicklungsmodell. Es fußt auf der Typenlehre, die McAfee bereits 2006 vorgestellt hat [3]. Darin werden die Beteiligten nach den mittelmäßig gefährlichen, ruhmgierigen Amateuren und Nachahmern sowie den seltenen, aber wenig gefährlichen Innovatoren unterschieden. Sie bilden zusammen die unterste Stufe des Pyramidenmodells. Gefährlich hingegen seien die (verärgerten) Insider und hoch gefährlich die Organisierten Internetverbrecher, die auf der dritten Stufe des Modells angesiedelt sind.

Dank des Aufsatzes von Balduan (2008) [4] habe ich das Bild von der modularen Cybercrime entwickelt [5], die arbeitsteilig aufgestellt ist und von Operation Groups [6], also spezialisierten kriminellen Kleinunternehmen, die sich zum Beispiel auf die Produktion von Malware konzentrieren [7], und kriminellen Projektmanagern (Koordinatoren [8]) geprägt ist. Sie sind in aller Regel auf der zweiten Stufe des Pyra-

---

1 Aus diesem Anlass erschien auch der letzte ▸ Newsletter #5 vom 27.06.2010.

2 Seit dem Sommer 2010 wird eine rege Diskussion über den Cyberwar geführt: ▸ CF, Kriegsrecht im Internet, 14.09.2010.

3 ▸ CF, Organisierte Kriminalität im Internet, 05.10.2008; ▸ Zweite große europäische Studie über das Organisierte Verbrechen und das Internet, McAfee Dezember 2006 (ZIP-Datei)

4 ▸ CF, Schurken-Provider und organisierte Cybercrime, 13.07.2008; ▸ Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff. (kostenpflichtiger Download, 1 €)

5 ▸ CF, modulare Cybercrime, 07.08.2008

6 ▸ CF, Operation Groups, 11.04.2010

7 ▸ CF, kriminelle Programmierer, 11.04.2010

8 ▸ CF, Koordinatoren, 11.04.2010

midenmodells angesiedelt [9]. Das Russian Business Network [10] (Schurkenprovider [11]) und die Erfahrungsberichte von G Data aus den Hackerboards [12] bilden die Grundlage für mein mehr theoretisches Bild von den Strukturen der Cybercrime und ihrer Underground Economy [13]. Die Schurkenprovider, Botnetz-Betreiber und professionellen Malware-Schreiber befinden sich auf der dritten Stufe des Modells [14] und gehören der Organisierten Cybercrime an.

Das bestätigende Faktenmaterial liefert der Leiter der französischen McAfee Labs, Paget [15]. Seine Studie in englischer Sprache habe mit neuen Schwerpunkten nacherzählt [16]. Bereits Igor Muttik hat 2008 von einer regen Cybercrime-Szene in Russland berichtet und dafür die schlechten wirtschaftlichen Verhältnisse verantwortlich gemacht: *„Die Wirtschaft und nicht die Mafia treibt Malware voran“* [17]. Das sieht Paget, der nicht wie Muttik in Russland lebt, jetzt anders und nennt massenhaft Beispiele, Namen und Hintergründe. Ihre besondere Brisanz bekommen sie, wenn man sie historisch sortiert. Spätestens seit dem Jahr 2000 ist die Cybercrime explodiert, hat sich schnell gewerbsmäßig strukturiert und besonders in den osteuropäischen Ländern organisierte Formen angenommen, die an der russischen Mafia orientiert sind oder von ihr betrieben werden [18]. Damit beschäftigt sich mein jüngstes Arbeitspapier:
▸ Dieter Kochheim, Eine kurze Geschichte der Cybercrime, November 2010 [19].

Den jüngst erschienenen, dritten Quartalsbericht für 2010 überschreibt McAfee zu Recht mit: Das Jahr der gezielten Angriffe [20]. In jedem Monat werden weltweit rund 6 Millionen Computer mit Botware infiziert und kommen täglich rund 60.000 neue Malware-Varianten zu den 14 Millionen bekannten hinzu [21].

Das wichtigste Ereignis des Jahres ist hingegen der Trojaner Stuxnet [22], den ich zunächst wegen seiner Bedeutung zwar richtig eingeschätzt und dennoch unterschätzt habe [23]. Im Juli 2010 wurde Stuxnet im Iran als erste Malware entdeckt, die sich auf die Steuerung von Industrieanlagen von der Firma Siemens konzentriert. Dazu sucht sie gezielt nach einem bestimmten Prozesssteuerungssystem (Process Control System - PCS) und setzt zahlreiche exklusive Exploits ein, deren Schwarzmarktpreis bei mehreren Einhunderttausend Dollar liegen dürfte. Stuxnet sollte sich Anfang 2010 abschalten, ist außer Kontrolle geraten und hat sich weltweit und besonders in Indien verbreitet. Das ist allein deshalb erstaunlich, weil sich die Malware fast ausschließlich per USB-Sticks verbreitet; das spricht dafür, dass sie sehr gezielt und nicht als Massen-Malware eingesetzt werden sollte.

McAfee warnt deshalb [24]:

> *Zahlreiche wichtige Systeme sind selbst dann schutzlos Angriffen ausgeliefert, wenn sie sich in*

---

9 Die Beteiligten sind besonders davon geprägt, dass niemand zur Begehung von Straftaten überredet werden muss. Die rechtliche Konstruktion der „Bande“ lässt sich nur bedingt auf sie anwenden: ▸ CF, kommunizierende Schwärme und zugeneigte Banden, 01.07.2010.

10 ▸ CF, Russian Business Network – RBN, 13.07.2008

11 ▸ CF, Schurkenprovider, 11.04.2010

12 ▸ CF, Basar für tatgeneigte Täter, 11.04.2010; ▸ CF, neue Hacker-Boards schotten sich ab, 23.05.2010.

13 ▸ CF, Geldwäsche in der Underground Economy, 05.09.2010; ▸ CF, Gishing, 15.09.2010.

14 Im Hinblick auf die Cybercrime gibt es auch ähnliche Modelle anderer Autoren. Siehe ▸ CF, Bestätigungen des Entwicklungsmodells von der Cybercrime, 21.11.2010.

15 ▸ CF, Mafia, Cybercrime und verwachsene Strukturen, 20.10.2010; ▸ François Paget, Cybercrime and Hacktivism, McAfee Labs 15.03.2010.

16 ▸ Dieter Kochheim, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010

17 ▸ Igor Muttik, Die Wirtschaft und nicht die Mafia treibt Malware voran, McAfee 12.02.2008; Länderbericht in der wunderbaren Studie ▸ McAfee, Ein Internet, viele Welten, 11.02.2008.

18 ▸ CF, kommerzielles Internet und organisierte Cybercrime, 03.11.2010

19 Siehe auch: ▸ Dieter Kochheim, Cybercrime und Cyberwar, Folienvortrag, 17.11.2010.

20 ▸ McAfee Threat-Report: Drittes Quartal 2010, McAfee Labs 08.11.2010

21 ▸ CF, Das Jahr der gezielten Angriffe, 20.11.2010

22 ▸ CF, Stuxnet, 20.11.2010

23 ▸ CF, Stuxnet spielt erst noch wie Nachbars Kampfhund, 16.09.2010

24 ▸ CF, Stuxnet, 20.11.2010

separaten Netzwerken befinden und nicht mit dem Internet verbunden sind.

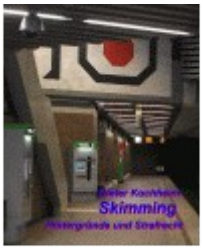
- *Angriffe gegen industrielle Steuersysteme sind Realität.*
- *Sicherheitsforscher warnten davor, dass hochkarätige gezielte Angriffe Zero-Day-Schwachstellen ausnutzen werden, die auf dem Schwarzmarkt erhältlich sind. Jetzt haben wir stichhaltige Beweise dafür.*

Inzwischen sind weitere Einzelheiten bekannt: Die Malware verfügt nicht nur über exklusive Angriffswerkzeuge, sondern offenbar auch über zwei "digitale Sprengköpfe", die sich gegen unterschiedliche Steuerungen richten und wahrscheinlich von verschiedenen Entwicklergruppen stammen. Inzwischen soll der Quellcode auch in kriminelle Hände geraten sein [25]

Mit Stuxnet hat der Cyberwar endgültig begonnen.

Skimming

Im September 2010 hat sich der BGH zum Versuchsstadium beim Skimming geäußert [26]. Danach findet der gesamte Vorgang des Skimmings im engeren Sinne, also das Ausspähen der Zugangsdaten am Geldautomaten, im Vorbereitungsstadium zum Fälschen von Zahlungskarten mit Garantiefunktion statt. Der Versuch beginnt frühestens dann, wenn der Skimmer die ausgespähten Dumps an die Fälscher übermittelt. Damit verlagert der BGH das Versuchsstadium weiter vor als er nach strenger Auslegung müsste. Sie würde verlangen, dass nur der Fälscher selber mit dem Versuch beginnen kann.



Von meiner noch weiter gehenden Position habe ich mich bereits im Frühsommer 2010 abgewandt.

Das ▸ Arbeitspapier Skimming hat jetzt den Stand vom 13.11.2010 (V #2.15)

Einen Überblick über die im laufenden Jahr erschienen Arbeitspapiere gibt es hier:

▸ CF, Auseinandersetzungen mit der Cybercrime, 21.11.2010

Bislang noch unerwähnt ist:

▸ Dieter Kochheim, Skimming, Folienpräsentation 02.10.2010

Verwertung von Vorratsdaten

Über den Umgang mit Verkehrsdaten nach dem Urteil des BVerfG habe ich im Newsletter #3 vom 07.03.2010 berichtet [27]. Wegen der Verwertbarkeit von Vorratsdaten aus der Zeit kurz vor dem Urteil gibt es mindestens zwei einander widersprechende Urteile der Landgerichte Verden und Hannover. Das Machtwort des BGH steht noch aus [28].

Quick Freeze

Eine verfassungskonforme Novelle des § 100g StPO und der für die Vorratsdatenhaltung nötigen Vorschriften in dem Telekommunikationsgesetz steht aus und ist noch lange nicht in Sicht. Statt dessen wollen sich die Bundesjustizministerin und der Bundesbeauftragte für den Datenschutz allenfalls auf einen „Quick Freeze plus“ einlassen und reagieren beleidigt, wenn sich Andere kritisch dazu äußern und weiterhin die Vorratsdaten fordern. So auch ich [29]:

"Quick Freeze" ist eine gute Methode, um eine laufende Kommunikation zu protokollieren. Sie ist keine Alternative zur Vorratsdatenspeicherung, weil sie eine laufende Überwachung voraussetzt. Wer sie als eine Alternative präsentiert, setzt einen flächendeckenden Überwachungsstaat à la Orwell voraus.

Die Verfolger von Urheberrechtsverstößen legen

---

25 ▸ Stuxnet-Code wird im Untergrund verkauft, Heise online 26.11.2010

26 ▸ CF, Versuch beim Skimming, 02.10.2010

27 ▸ CF, Newsletter #3, Vorratsdaten und Skimming, 07.03.2010; ▸ Kochheim, Zum Umgang mit Verkehrsdaten. Bestandsaufnahme und praktische Konsequenzen aus dem Urteil des BVerfG vom 02.03.2010, 08.03.2010

28 Gerüchteweise soll meiner Auffassung erhebliche Beachtung zukommen.

29 ▸ CF, Jetzt ist aber Schlüss! 05.10.2010

sich wie Straßenräuber auf die Lauer und protokollieren bevorzugt P2P-Netzwerke, um dann mit meist überzogenen Abmahn-Forderungen zuzuschlagen und abzuzocken. Wer das als Leitbild für die Strafverfolgung propagiert, lebt in einem anderen Rechtsstaat und unter einer anderen, nicht mehr freiheitlichen Verfassung als ich.

Binnen "drei bis sieben Tage", für die der Bundesdatenschutzbeauftragte zunächst die Speicherung zulassen wollte, merken Normalbürger in aller Regel nicht, dass sie betrogen, belogen, anderweitig bloßgestellt oder ihrer Identität beraubt wurden. Solange sie das nicht merken und anzeigen, weiß auch die Strafverfolgung nichts davon, dass möglicherweise eine Straftat begangen wurde.

Cyberfahnders Abgesang

Meine Ankündigung, den Cyberfahnder am 01.04.2011 einzustellen [30], hat bange Rückfragen ausgelöst. Ich habe am 24.10.2010 ua geschrieben [31]:

Die organisierten Strukturen der Cybercrime werden nicht oder allenfalls am Rande wahrgenommen. Dornröschens Attraktivität mag Blaublütler sportlich angereizt haben. Ich sehe jedoch weniger Bereitschaft, sich auf meine Warnungen einzulassen, sondern eher Widerstände, Bedenken und Unverständnis, wenn es um die Gefahren, Entwicklungen und Bekämpfung der organisierten Cybercrime geht. ...

Muss ich die infernale Komödie weiter beobachten? Für einen Gesetzgeber, der frei von Sachkenntnis ist - jedenfalls dann, wenn er sich medienwirksam äußert? In einem Justizapparat, der mir Anerkennung zollt, ohne daraus Konsequenzen zu ziehen? Ach, wir haben da so einen Idioten, der kennt sich ganz gut aus. Nö!

Am 01.04.2011 wird es den Cyberfahnder vier Jahre lang geben. Ich habe bewiesen, dass man ein solches Projekt durchziehen kann. So, wie es jetzt aussieht, wird es keinen Tag länger existieren!

So long! Fisch gab es nicht genug!

Ich weiß nicht, wie es danach weiter gehen wird. Das Engagement und den Aufwand, den ich bislang für den Cyberfahnder geleistet habe, werde ich jedenfalls ab dem genannten Datum nicht mehr aufbringen.

Dafür sind mehrere Gründe tragend:

① Die technischen und sonstigen Grundlagen der Cybercrime sind erarbeitet. Sie sind im ▸ Arbeitspapier Cybercrime zusammen gefasst.

② Auch die strukturellen Grundlagen habe ich erarbeitet und die Modelle von der modularen Cybercrime und den tatgeneigten Schwärmen entwickelt sowie das Entwicklungsmodell für die Cybercrime und den Cyberwar entworfen. Je mehr Fakten hinzu kommen, desto deutlicher zeigt sich, dass ich in den Grundlinien Recht behalte [32]. Vom Fachpublikum diskutiert und kritisiert werden sie nicht.

③ Der Cyberfahnder ist zu einem mahnenden Wachturm geworden, der meinem Eindruck nach nur lächelnd und gönnerhaft wahrgenommen wird. Um das fortzusetzen kann ich mir auch eine Kiste nehmen und Speaker spielen. Ich werde bislang dreimal in der akademischen Literatur der Rechtswissenschaften erwähnt, nicht aber diskutiert. Das ist angesichts der Bedeutung der Themen Skimming und Cybercrime zu wenig.

④ Es gibt aufmunternde E-Mails, Gästebucheintragungen und Gespräche, die mir zeigen, dass vor Allem die Praktiker in der Strafverfolgung den Cyberfahnder als Unterstützung schätzen und brauchen. Den damit verbundenen Anspruch kann ich im Rahmen eines Freizeitprojekts nicht erfüllen. Daneben gibt es Hilfsangebote, die sich auf die technische Unterstützung beschränken. Im Laufe der Zeit habe ich zwei Texte mit dem Ersuchen um Veröffentlichung erhalten, die beide keine Quellen auswiesen, so dass ich sie hätte ungeprüft verantworten müssen. Das habe ich verweigert.

⑤ Karaboga hat mir vor einem Jahr die Grenzen der kritischen Berichterstattung gezeigt, indem verhohlene Drohungen gegen meine Angehörigen

[30] ▸ CF, Statusbericht, 24.10.2010

[31] ▸ CF, Finale, 24.10.2010

[32] ▸ CF, hab ich es nicht gesagt? 27.11.2010

erfolgten. Eine engagierte Berichterstattung, muss ich daraus schließen, bedarf einer abschirmenden Umgebung, eines Unternehmens oder einer Organisation oder muss Bullet Proof sein. Das ist keine schöne Aussicht für die Meinungsfreiheit.

Die beiden Abmahnversuche aus dem vergangenen Jahr stecken auch noch als Stacheln in der Erinnerung.

⑥ Der Gesetzgeber verweigert die nötigen Instrumente für die Strafverfolgung und den Rechtsschutz im Übrigen. Das gilt besonders für die Vorratsdaten. Ich warte auf den Aufschrei, wenn der breiten Bevölkerung klar wird, dass ohne sie die Alltagskriminalität und berechtigte zivilrechtliche Ansprüche gegen Betrüger, Verleumder und Stalker nicht mehr verfolgbar sind [33].

⑦ Die Justizverwaltung nimmt die Cybercrime als besonderes Aufgabenfeld nicht wahr. Wollte man sie ernsthaft verfolgen, würde das mehr als Umschichtungen bei den Pensen verlangen. Dazu müssten zusätzliche Haushaltsmittel bereit gestellt werden und ein politischer Wille bestehen. Das ist nicht abzusehen.

⑧ Hingegen ist Fatalismus nicht nötig. Es liegt in der Natur der Kriminalität, dass sie immer wieder Lücken und neue Formen sucht, um Beute zu machen. Dennoch gibt es Wege und Mittel, sie zu bekämpfen. Das bedarf aber der richtigen Leute, die frei von anderen Lasten handeln können.

⑨ Der Cyberfahnder ist ein Hobby, das mich inzwischen so stark einnimmt, dass ich andere private Pflichten vernachlässige. Dem muss ich ein Ende bereiten!

Allen Freunden und Besuchern des Cyberfahnders wünsche ich eine schöne Adventszeit, angenehme Weihnachten und ein erfolgreiches und zufriedenes Jahr 2011.

Dieter Kochheim

PS: Gespannt bin ich darauf, wann die Ausgabe 1/2011 der c't erscheint.

[33] ▸ CF, Datenschatten in der Überwachungsgesellschaft, 27.06.2010