Eskalationen

Spätestens seit 2010 verschärfen sich die Auseinandersetzungen auf verschiedenen Feldern, die alle mit dem Internet in Verbindung stehen. Das gilt nicht nur für die Cybercrime, um die es gerade merkwürdig ruhig ist und die dennoch immer wieder neue Angriffsfelder für profitable Geschäfte erkundet, wie den zunehmenden Markt für internetfähige Mobiltelefone.

Auffällig sind die groß angelegten Spionageaktionen, für die **Aurora** vom Anfang 2010 und der erst jetzt bekannt gewordene **Night Dragon** stehen. Beide sind Beispiele für hochgradig professionell ausgeführte Angriffe über das Internet, die sich unmittelbar gegen Wirtschaftsunternehmen richten und dazu dienen, Betriebsgeheimnisse zu erkunden.

Stuxnet ist eine außergewöhnliche Malware, die der Sabotage dient. In ihr vereint sich professionelles Programmierwissen mit Detailwissen über die industriellen Steuerungsanlagen der Firma Siemens und Angriffswerkzeuge in einer Menge und Qualität, die bislang unbekannt waren.

Alle drei Beispiele zeigen, dass die Destruktionen im Internet und im Zusammenhang mit der Informationstechnik neue und äußerst gefährliche Formen angenommen haben.

McAfee und besonders der Leiter der französischen McAfee Labs, Paget, haben auf den zunehmenden **Hacktivismus** hingewiesen und dazu zunächst noch recht harmlose Beispiele wie das Verunstalten gegnerischer Webseiten – Defacement – und den groß angelegten DDoS-Angriff gegen Estland angeführt.

Das Beispiel **WikiLeaks** zeigt nicht nur, dass zivile Organisationen mit Nachdruck und einer gewissen Unbarmherzigkeit geheime und peinliche Informationen verbreiten – Whistleblowing. Auch die Gegenreaktionen sind bislang ungewohnt. Sie richten sich mit Sperren von Hostspeichern und Bankkonten existenziell gegen diese Organisation und ihre Repräsentanten. Das wurde im Herbst 2010 begleitet mit DDoS-Angriffen von WikiLeaks-Gegnern.

Das wäre nichts Neues und ist aus den Kämpfen zwischen verschiedenen Hackerboards schon bekannt gewesen.

Eine neue Qualität entfalteten hingegen die Sympathisanten des Hackerkollektivs **Anonymous**. Seine Gemeinde ist weltweit verbreitet und widmet sich verschiedenen und wechselnden politischen Zielen: Gegen Scientology, gegen WikiLeaks Gegner und für die Aufständischen in Ägypten. Die nachhaltigen Angriffe gegen Amazon und die Finanzunternehmen, die sich gegen WikiLeaks haben instrumentalisieren lassen, demonstrieren ebenso deutlich, dass die Hackergemeinde ihre eigenen Spielregeln einfordert und durchsetzt. Mächtig genug ist sie dazu.

Zwischen der Cybercrime und dem Internet-Mainstream sind Unternehmen entstanden, die mit den Methoden der Cybercrime auf dem regulären Markt gutes Geld verdienen. Das gilt einerseits für die kommerziellen Schwachstellen-Jäger und -Händler (Exploit-Händler). Die andere Seite stellen Unternehmen wie HBGary Federal dar, die existenziell bedrohende Angriffsstrategien entwickeln und alle Register des Social Engineering ziehen, um zum Beispiel die Anonymous-Aktivisten zu identifizieren und sie der persönlichen Verfolgung zuführen.

Das geschah im Stillen, bis HBGary Federal im Februar 2011 von Anonymous-Hackern gehackt wurde und diese peinliches Firmenmaterial veröffentlichten.

Seit dem späten Sommer 2010 werden intensive Diskussionen über **Kritische Infrastrukturen**, ihren Schutz und die Frage nach dem **Cyberwar** geführt. Auch hier stoßen stark gegensätzliche Positionen aufeinander.

Die deutsche Sichtweise sieht als kritisch vor allem die Kommunikationsnetze und ihren reibungslosen Betrieb an. Das wird besonders in den USA anders gesehen, wo auch breite Teile der produzierenden Industrie, das Verkehrswesen und überhaupt die Grundversorgung als kritisch eingestuft wird.

Diese Diskussion hat Ähnlichkeiten mit der um den Cyberwar. Während die militärisch und staatsrechtlich ausgerichtete Position nur „echte“ Kriegshandlungen dem Begriff unterwerfen will, spricht die Gegenposition von einem erheblich breiteren Ansatz, der auch den Hacktivismus und existenzielle Formen der Wirtschaftsspionage und -sabotage einbezieht. Das ist auch die von mir seit dem Sommer 2010 vertretene Position.

Spezial: Eskalationen

Mit dem vorliegenden Arbeitspapier gehe ich einen anderen Weg als mit den voraus gegangenen. Er ist für das Lesen am Bildschirm optimiert und kann als PDF-Dokument natürlich auch ausgedruckt werden. Die Anmerkungen sind, wo immer möglich, mit Hyperlinks versehen, die nur bei der Bildschirmausgabe funktionieren. Den Links ist das Zeichen „▸“ vorangestellt.

Inhaltlich befasst er sich mit allen Themen, die einleitend angeführt sind, und stellt einen Überblick über eskalierenden Aktivitäten im Zusammenhang mit dem Internet vor. Die Beiträge sind bereits im Cyberfahnder erschienen und wurden für diese Ausgabe überarbeitet und neu zusammen gestellt. Neu sind nur die Einleitung und der abschließende Beitrag über die Eskalationen in der dualen Welt.

Dieter Kochheim, 19.02.2011

Thema: Eskalationen
Autor: Dieter Kochheim
Version: 1.00
Stand: 19.02.2011
Cover: „Drei Damen“ (Vilnius, 2004), D. Kochheim
Impressum: ▸ CF, cyberfahnder.de

Auf den Seiten 4, 5 und 22 werden Bildzitate aus den Berichten und Whitepapers von McAfee verwendet, ohne die das Verständnis erschwert gewesen wäre.
Die Grafik auf Seite 31 stammt aus dem
- Air Force Doctrine Document 3-12, Cyberspace Operations, Lemay Center 10.09.2010.

Aurora

▸ CF 13.02.2011

Google und 30 andere Unternehmen waren Anfang 2010 heftigen Angriffen aus China ausgesetzt (1). Mit ihnen setzte sich nicht nur McAfees erster Quartalsbericht aus 2010 auseinander (2), sondern auch eine vollständige Studie (3). Sie beschreibt den Angriff so:

→ *1. Ein ins Ziel geratener Benutzer bekam aus einer „vertrauenswürdiger" Quelle einen Link in einer E-Mail oder in einer Sofortnachricht.*

→ *2. Der Benutzer klickte den Link an und gelangte so auf eine Webseite in Taiwan, die Schadcode in Form von schädlichem JavaScript-Payload enthielt.*

→ *3. Dieses schädliche JavaScript enthielt ein Zero-Day-Exploit für den Internet Explorer und wurde vom Browser des Benutzers heruntergeladen und ausgeführt.*

→ *4. Der Exploit lud dann von Servern in Taiwan einen als Bild getarnten Binärcode herunter und führte den schädlichen Payload aus.*

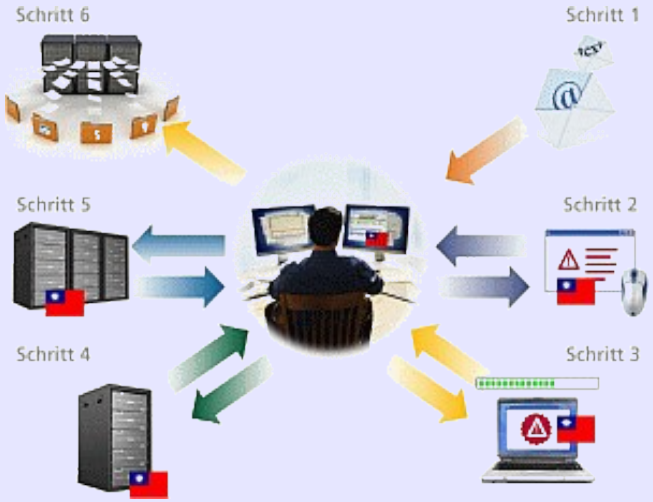
→ *5. Der Payload richtete eine Backdoor ein und verband sich mit einem Botnet in Taiwan.*

→ *6. Damit hatten die Angreifer vollen Zugriff auf die internen Systeme. Sie hatten es auf geistiges Eigentum und Systeme zum Software-Konfigurations-Management (Software Configuration Management, SCM) abgesehen, auf die sie nun durch die gefährdeten Systeme Zugriff hatten. Das kompromittierte System ließ sich zudem so manipulieren, dass die Angreifer noch weiter in das Netzwerk vordringen konnten.*

Die Studie analysiert eingehend alle Angriffsschritte. Das können wir uns hier ersparen.

Wichtig ist vielmehr, dass die Angreifer ganz gezielt und punktgenau das gegnerische System angegriffen und dazu Detailkenntnisse über die technische Ausstattung des Ziels genutzt haben. Noch professioneller handelten die Angreifer beim späteren Night Dragon.

Ich hatte zunächst wenig Verständnis für Googles beleidigt wirkende Flucht (4). Das Szenario, das McAfee hier beschreibt, weckt (wenigstens mein) Verständnis.



Grafik von McAfee (5)

(1) ▸ Verfassungsschutzbericht 2009. Tatort Internet, CF 26.06.2010

(2) ▸ Pedro Bueno, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar, Adam Wosotowsky, McAfee Threat-Report: Erstes Quartal 2010, McAfee Labs 12.05.2010

(3) ▸ Schutz für Ihre wichtigsten Ressourcen. Lehren aus „Operation Aurora", McAfee Labs 12.04.2010.
Die Beschreibung ist so knapp und präzise, dass man sie nicht sinnvoll mit eigenen Worten nacherzählen kann.

(4) ▸ Google in China, 28.03.2010

(5) Ebenda ▸ (3), S.3.

Night Dragon

▸ CF 13.02.2011

In einem nur in englischer Sprache verfügbaren White Paper berichtet McAfee über einen seit November 2009 offenbar von China aus geführten, koordinierten und gezielten Cyberangriff gegen globale Öl-, Energie- und petrochemische Unternehmen, dem McAfee den Namen Night Dragon gegeben hat (1). Mit den Angriffen sollen vor allem Produktions- und Förderdaten, Informationen über Vorräte, Vertragsangebote und Projektkalkulationen erlangt werden. Das Beispiel belegt, dass nicht nur die zerstörerischen DDoS-Angriffe gezielter werden, sondern auch die Hacking-Angriffe, die der Informationsbeschaffung und der Zerstörung dienen.

Bei dem Angriff geht es darum, den Fernzugriff auf die Computersysteme der angegriffenen Unternehmen mit entsprechenden Werkzeugen - Remote Access Tools - RAT - zu erlangen. Dazu werden Schwachstellen im Betriebssystem von Microsoft Windows und besonders in der Nutzerverwaltung und Rechtesteuerung - Active Directory - missbraucht.

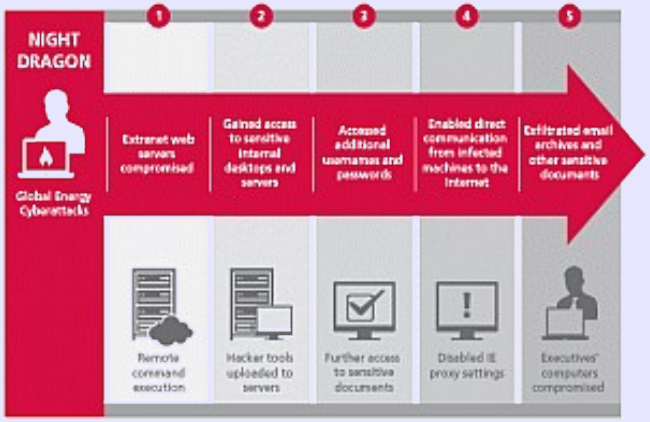
Zunächst wird der Webserver des Unternehmens mit SQL-Injection-Methoden angegriffen. Dieser Webserver befindet sich noch außerhalb der engeren Schutzzone und dient den Kundenkontakten. Aber auch dazu muss er auf Kundendatenbanken, Preislisten und andere interne Informationen zugreifen. Das macht das Gesamtsystem anfällig.

Die SQL-Injektion ist ein einfacher Kommando-String zur Steuerung von Datenbankfunktionen. Gelingt es damit, die Kontrolle über den Webserver zu erlangen, können Hackerwerkzeuge nachgeladen, Kontodaten und Zugangscodes ausgespäht oder protokolliert werden. Damit steht der Weg ins Innere des Unternehmensnetzes, alle Server und Desktoprechner offen.

Der Drache nutzt dazu verseuchte Webseiten, die der "eigene" Webserver den Mitarbeitern im Innern sendet, und E-Mail-Anhänge, die er auf dem firmeneigenen E-Mail-Server präpariert.

Um den Fernzugriff vom Command and Control-Server - C&C - des Angreifers durchzulassen, müssen nämlich die Sicherheitseinstellungen im Internet Explorer der firmeninternen Anwender und im Proxy-Server des Unternehmens abgeschaltet werden.

Der Night Dragon war offenbar erfolgreich. Über in China gehostete C&C-Server und Hostspeicher in den USA und den Niederlanden gelang der Eingriff gegen Unternehmen und gegen Führungskräfte in Kasachstan, Taiwan, Griechenland und den USA. Erlangt wurden neben sensiblen Unternehmensdaten auch urheberrechtlich geschützte und vertrauliche Informationen.



Grafik von McAfee (2)

Mit neu entwickelten und angepassten Software-Werkzeugen schaffte es der Drache, Firewalls und VPN-Tunnel zu durchdringen, um auf die Laptops der sich sicher glaubenden Mitarbeiter und Führungskräfte zu gelangen.

Das White Paper beschreibt und dokumentiert die Einzelschritte, die McAfee zur Analyse und Abwehr unternommen und entwickelt hat. Mein Überblick über die Funktionen und Wirkungen beansprucht keine Tiefe und Vollständigkeit. Dazu bin ich in der englischen Sprache viel zu ungeübt, um den Text binnen weniger Stunden völlig zu durchdringen und zu verstehen.

Das Szenario, das McAfee berichtet, ist hingegen nicht neu. Es enthält die Vorgehensweisen, die aus anderen Informationsangriffen bekannt sind. Ihre Kombination und Ballung ist jedoch einzigartig und dadurch tatsächlich neu.

Auch nicht neu, aber am Beispiel wieder aktuell, ist folgende Warnung: Sobald ein Angreifer den vollen Zugriff auf einen Rechner oder - damit verbunden - auf ein ganzes Rechnernetz erlangt, kann er nicht nur die gespeicherten vertraulichen Informationen stehlen, löschen oder durch falsche ersetzen, sondern auch computergestützte Anlagensteuerungen manipulieren. Er kann Kraftwerke, Förderbänder und Klimaanlagen steuern und abschalten und damit ein sehr reales Chaos veranstalten.

McAfees Bericht deutet das nur an, aber ich habe anhand der Wortwahl, der Textstruktur und den Auslassungen genau den Eindruck, dass das geschehen ist.

(1) ▸ Global Energy Cyberattacks: “Night Dragon”, McAfee Labs 10.02.2011;
▸ Stephen Shankland, Operation "Night Dragon": Hacker spionieren Ölindustrie aus, zdnet.de 10.02.2011.

(2) Ebenda ▸ (1), S.3.

Emissionsrechte

▸ CF 07.02.2010

Lizenzen zum Dreckverschleudern sind handelbar und Geld wert (1). Die Verteilung von Emissionsrechten reguliert die Deutsche Emissionshandelsstelle - DEHST.

Sie war jetzt das Ziel von Phishern, die eine Nachricht von ihr fälschten und lizensierte dreckschleudernde Unternehmen aus Sicherheitsgründen zur neuen Registrierung aufforderten (2). Kaum geschehen wurden die vorhandenen Emissionsrechte weltweit zum Verkauf angeboten und verkauft. Der Schaden beläuft sich auf mehrere Millionen Euro. ...

(1) ▸ Emissionsrechtehandel, Wikipedia

(2) ▸ Hacker legen Emissionsrechtehandel lahm, Heise online 03.02.2010

Stromnetz-Hacking

▸ CF 06.11.2010

Über das Internet tauschen Umspannwerke, Netzbetreiber und Kraftwerke Daten aus, *um Angebot und Nachfrage zu regulieren und damit auch den aktuellen Strompreis zu ermitteln* (1). In einer Amerikanischen Studie werden in diesem Zusammenhang *Szenarien entwickelt, in denen diese Daten manipuliert werden. Angreifer könnten die Kommunikationsleitungen zwischen Umspannwerken und Netzleitstellen anzapfen und falsche Informationen einschleusen*. Die Angreifer könnten *vorgeben, dass die Hochspannungsleitungen zwischen zwei Städten überlastet sind. Das würde die Leitstelle dazu veranlassen, Strom von entfernteren (und damit teureren) Kraftwerken anzufordern, was die Preise an diesem Netzknoten erhöhen würde. Mit diesen Informationen bewaffnet, könnte der Angreifer dann eine sichere Wette an einer Stromhandelsbörse abschließen – und anschließend kassieren*.

Solche Überlegungen sind originell, aber nicht überraschend oder spekulativ. Sie passen in die Reihe von Meldungen, die etwa Kursmanipulationen, automatisches Phishing oder spektakuläre Hacks betreffen.

(1) ▸ Kevin Bullis, Kasse machen mit Stromnetz-Hacks, Technology Review 13.10.2010

Stuxnet

▸ CF 16.02.2011

Die Stuxnet-Angriffe (1) begannen laut interner Protokolle im Juni 2009 mit gezielten Infiltrationen gegen die Laptops von Mitarbeitern von fünf Firmen, *die im Zusammenhang mit der iranischen Urananreicherungsanlage in Natanz* stehen. Symantec vermutet jedenfalls, *dass Experten der USA und Israels Stuxnet innerhalb von zwei Jahren gemeinschaftlich entwickelt haben* (2). Jedenfalls muss Stuxnet aus einem völlig anderen Umfeld stammen als übliche Malware (3). Bei tecchannel wird auch über die Symantec-Studie (4) berichtet: *Neben einer bereits früher dokumentierten Sabotagefunktion enthält Stuxnet noch eine zweite, komplexere, die jedoch deaktiviert ist. Ihre Aufgabe ist nicht endgültig geklärt, der Code scheint unvollständig zu sein. Er zielt auf Anlagensteuerungen des Typs Siemens S7-417. Der Sabotage-Code zeigt jedenfalls, das die Programmierer genaue Kenntnisse über die Struktur der Anlage haben, auf die der Angriff gerichtet ist.*

Stuxnet ist eine ungewöhnliche Malware (5).

→ Ihre Entwicklung begann wahrscheinlich im Jahr 2007. Sie ist nicht das Werk üblicher Cyberkrimineller, sondern von Profis aus dem gewerblichen Lager.

→ Sie verbreitet sich nicht über das Internet, sondern wird seit dem Sommer 2009 gezielt den Mitarbeitern von Firmen zugespielt, die an dem Bau der Atomanlagen im Iran beteiligt sind.

→ Sie verbreitet sich zwischen Endgeräten und in lokalen Netzwerken. Anders als die kriminelle Mal- und Botware aktualisiert sie sich nicht über das Internet. Aus gutem Grund: Sie ist für geschlossene Netze optimiert.

→ Sie verfügt über Tarnfunktionen (Rootkits), die noch bis zum Sommer 2010, als Stuxnet entdeckt wurde, unbekannt waren. Sie blieb äußerst lange unentdeckt.

→ Sie nutzt mehrere Exploits zum Angriff, die noch bis zum Sommer 2010 völlig unbekannt waren. Beides – Rootkits und Exploits – spricht dafür, dass alleine die Einkaufskosten (ohne Programmierung) sechsstellige $-Beträge verschlungen haben.

→ Ihre Angriffsfunktionen sind auf Anlagensteuerungen der Firma Siemens ausgerichtet, von denen mindestens zwei gefunden wurden. Eine dritte scheint noch unentwickelt geschlummert zu haben. An ihren Entwicklungen scheinen unabhängige Programmiererteams beteiligt gewesen zu sein.

→ Stuxnet ist das erste Beispiel für eine autonom handelnde Malware ohne Außensteuerung. Ihre Funktionen sind ohne tiefe Detailkenntnisse über die Prozesssteuerungssoftware von Siemens nicht programmierbar.

→ Stuxnet ist das erste Beispiel für eine destruktive Malware, die sich auf industrielle Steuerungsprozesse konzentriert.

(1) ▸ Stuxnet spielt erst noch wie Nachbars Kampfhund, CF 16.09.2010

(2) ▸ Stuxnet: Fünf Firmen als Sprungbrett missbraucht, Heise online 15.02.2011

(3) ▸ Stuxnet-Angriffe richteten sich gegen fünf ausgewählte Ziele, tecchannel 16.02.2011

(4) ▸ Updated W32.Stuxnet Dossier is Available, Symantec 11.02.2011

(5) ▸ Stuxnet, CF 20.11.2010

Stuxnet doch kein Meisterstück?
▸ CF 22.01.2011

Unter dieser Überschrift referiert Heise mehrere Experten, die Zweifel an der Genialität von Stuxnet anmelden (6). *Tom Parker ... halte die Fernsteuer-Funktion des Wurm für schlecht implementiert, weil etwa der Datenverkehr unverschlüsselt ablaufe. Zudem habe sich der Wurm über das Internet verbreitet, was dazu geführt habe, dass der Wurm unkontrolliert auch andere Systeme als das eigentliche Ziel befiel.* Nate Lawson hält dagegen die Tarnkappentechnik des Wurms für zu schwach.

Ich behaupte nicht, dass die Werkzeuge im Cyberwar klinisch sauber sein müssen und politisch korrekt keine Kollateralschäden anrichten können. Krieg in jeder Form ist schmutzig, so sehr sich die Beteiligten auch um eine Schadensbegrenzung bemühen mögen.

Die Einwürfe, dem Stuxnet-Datenverkehr fehle eine Verschlüsselung und seine Tarnung sei zu schwach, gehen aus mehreren Gründen fehl.

→ Der Wurm sollte sich eigentlich Anfang 2010 abschalten und wurde erst Monate später überhaupt entdeckt.

→ Weitere etliche Monate hat es gedauert, bis er geknackt wurde und seine Funktionen halbwegs ermittelt waren.

→ Es ist nur konsequent, keine Verschlüsselung zu verwenden, weil jedenfalls eine starke Verschlüsselung sehr schnell zur Überlastung der Kontroll-Server führen kann (7). Dann kann man gleich auf sie verzichten.

Man sollte den Wurm nicht kleinreden, auch nicht mit solchen Dummheiten: *Lawson hoffe, dass die Entwickler digitaler Waffen mehr auf der Pfanne hätten, als die Tricks, die bulgarische Teenager schon in den 90er Jahren zur Tarnung ihrer Viren eingesetzt hätten.* Zu fragen ist nicht nach dem Positiven, worauf Kästner bereits hinreichend geantwortet hat (8), sondern nach den Konzepten und Gegenmaßnahmen, die diese Experten jedenfalls schuldig geblieben sind.

(6) ▸ Ein Wurm im Cyberwar: Stuxnet doch kein Meisterstück? Heise online 19.01.2011

(7) ▸ Zombies im Labortest, 21.12.2010

(8) "Ja, wo bleibt es denn?"

Bedrohungen im 4. Quartal 2010

▸ CF 13.02.2011

Schon der Bericht von McAfee über das dritte Quartal 2010 (1) ließ sich überschreiben mit „Das Jahr der gezielten Angriffe“. Im vierten Quartal 2010 (2) setzten sich die gezielten Angriffe fort und wurden jetzt besonders auch mobile Endgeräte, allen voran Smartphones (3) mit dem Betriebssystem Android angegriffen. Während das Spam-Aufkommen auf den Stand von 2007 zurückging (4), nahmen die Malware-Varianten extrem zu (5), wie 2009 vorausgesagt, unter häufiger Ausnutzung von Adobes Portable Document Format - PDF (6). Die Besonderheiten des Quartals sind hingegen, wer hätte das vermutet, Hacktivismus, WikiLeaks und die Hacktivistengruppe Anonymous (7).

Cutwail und Bobax waren 2010 die aktivsten Botnetze (8), wobei Cutwail die Führung übernommen hat. In vielen Teilen der Welt war Rustock am weitesten verbreitet. Das gilt auch für die Malware im Übrigen: Ihre Form variiert in den verschiedenen Weltregionen: *Nutzer haben Vorlieben und Abneigungen, die mit ihrer Kultur und ihrem Land zusammenhängen. Internetkriminelle sind sich dieser Tatsache bewusst und greifen Nutzer daher in verschiedenen Ländern mit unterschiedlichen Methoden an.* (S. 6, 9)

Mehr als 20 Millionen neue Malware-Varianten wurden im vergangenen Jahr erfasst. Das entspricht fast 55.000 Malware-Bedrohungen pro Tag. Das sind mehr Bedrohungen als 2009, mehr als 2008 und erheblich mehr als 2007. Von den fast 55 Millionen Malware-Varianten, die McAfee Labs identifizierte und vor denen es Schutz bot, wurden 36 Prozent im Jahr 2010 geschrieben! (9), S. 7

Als Fahndungserfolge im vierten Quartal 2010 wurden gemeldet (10) (S. 19): Die russische Polizei verhaftete 50 Verdächtige, die 20 Millionen Rubel bei 17 Banken erbeutet haben sollen, mehrere Mitglieder einer Gruppe, die Geldautomaten mit Viren infizierten, und gegen einen der weltweit größten Spammer, Igor Gusev, wurde ein Strafverfahren eingeleitet. Die niederländischen Kriminalpolizei löste das Bredolab-Botnet auf. Deren mutmaßlicher Betreiber wurde in Armenien festgenommen.

In den USA beschlagnahmte die Behörde zum Schutz von Urheberrechten (National Intellectual Property Rights Coordination Center) 82 Domänen, die nachgemachte Waren vertrieben. Beim Verkauf von lächerlichen 30 Dumps wurde der Malaysier Lin Mun Poo verhaftet. Er soll über die Daten zu 400.000 gestohlenen Kredit- und Debitkarten verfügt haben. Der vermutliche Betreiber des für Spam-Kampagnen eingesetzten Mega-D-Botnetzes wurde in Las Vegas verhaftet.

Hacktivismus

Im vergangenen Quartal erfolgten mindestens 7 große Hacktivismus-Kampagnen (S. 19):

→ Anonymous: DDoS gegen vier große Urheberrechtsschutz-Organisationen und Anbieter von Erotikfilmen

→ Survival International: DDoS gegen Botswana wegen schwersten Menschenrechtsverletzungen

→ Vietnam: DDoS gegen regierungskritische Blogger

→ China: Hacking gegen Südkorea, um vertrauliche Informationen vom Auswärtigen Dienst und von Sicherheitsbeauftragten zu erlangen

→ Myanmar: DDoS gegen Zugangsprovider im zeitlichen Zusammenhang mit den Wahlen am 07.11.2010

→ China: DDoS gegen Phayul.com, ein führendes Nachrichtenportal der tibetanische Diaspora

→ WikiLeaks: Gegenseitige DDoS-Angriffe gegen Gegner und Unterstützer

→ Februar 2011, Anonymous: DDoS zur Unterstützung des Widerstandes in Ägypten (11)

(1) ▸ McAfee Threat-Report: Drittes Quartal 2010, McAfee Labs 08.11.2010

(2) ▸ McAfee Threat-Report: Viertes Quartal 2010, McAfee Labs 04.02.2011

(3) ▸ Smartphone-Zombies, 25.01.2011

(4) ▸ 95 Billionen Spam-Mails, 15.01.2011

(5) ▸ Wachstumsgrenze für Malware, 08.02.2011

(6) ▸ gefährliche PDF-Dateien, 09.05.2009

(7) ▸ Molotowcocktails im Internet, 05.02.2011

(8) ▸ mächtige Werkzeuge für die Cybercrime, 24.09.2010;
▸ Zheng Bu, Pedro Bueno, Rahul Kashyap, Adam Wosotowsky, Das neue Zeitalter der Botnets, McAfee Labs 19.08.2010

(9) Ebenda ▸ (2).

(10) Ebenda ▸ (2).

(11) Ebenda ▸ (7).

Betrug mit PayPal

▸ CF 12.09.2010

Über eine raffinierte Betrugsmasche berichtet Kossel in der jüngsten c't (1). Dabei geht es um das Zusammenspiel von PayPal und eBay und die Tricks eines Identitätsdiebes aus Litauen und um eine Spiegelreflexkamera für immerhin 858 €.

Der Betrüger *hatte sich per Phishing oder einem Trojaner die Zugangsdaten zu einem eBay- und dem dazugehörigen PayPal-Konto verschafft. Daraufhin tauschte er die Anschrift und die E-Mail-Adresse im eBay-Konto. Bei PayPal konnte er das aber nicht tun, da solche Änderungen dort ein Prüfverfahren in Gang setzen ... Beim Bezahlen gab der Betrüger an, nichtphysische Güter zu erwerben, die nicht verschickt werden. Dadurch teilte PayPal <dem Opfer> gar keine Versandadresse mit. Denn aus Datenschutzgründen erhält der Verkäufer nur die Informationen über den Käufer, die er für die Abwicklung des Geschäfts benötigt.* <Das Opfer> *vermisste diese Adresse nicht, sondern nutzte die Schnittstelle zwischen eBay und DHL Online Frankierung, die daraus einen Paketaufkleber generierte.*

Neben der Masche selber ist bemerkenswert, dass sich PayPal aktiv an der Aufklärung beteiligt hat. Das ist man von der Branche sonst nicht gewohnt.

(1) Axel Kossel, Verkäufer ohne Schutz, c't 20/2010, S. 76

Mobile Botnetze

▸ CF 25.01.2011

Als der Wurm "Sexy View" 2009 Smartphones infizierte und mit ihm versucht wurde, ein mobiles Botnetz aufzubauen, meldeten sich Experten mit der Meinung, dass sich damit kein richtiger krimineller Gewinn erzielen ließe. Bald verbreiteten sich jedoch die Handy-Viren und verhalfen einem alten Nummerntrick zu neuer Blüte, indem sie als Dialer Kostenfallen stellten. Im Oktober 2010 berichtete die c't über zunehmende Identitätsdiebstähle und Phishing im Zusammenhang mit dem Mobilfunk und im vergangenen Sommer versuchten russische Online-Kriminelle, böswillige Software auf die Geräte einzuschleusen, die dann teure Premium-SMS absetzten. Kurze Zeit später stahl ein trojanisches Pferd für Blackberry- und Symbian-Smartphones Bankdaten. Und in China kursierte Ende vergangenen Jahres ein Datenschädling, der Kontaktdaten von den Geräten abgriff.

In Russland wurde eine auf Java basierende Malware entdeckt, die unbemerkt teure SMS versendet. Sie greift auch andere Plattformen als nur Smartphones an.

Ein gutes Jahrzehnt für Internetkriminalität

▸ CF 13.02.2011

Ausgehend von Pagets White Paper "Cybercrime and Hacktivism" (1) aus dem März 2010 und eigenen Recherchen habe ich im November 2010 "Eine kurze Geschichte der Cybercrime" (2) abgeleitet. Die Zeit seit dem Jahr 2000 habe ich überschrieben mit: Kommerzielles Internet und organisierte Cybercrime (S. 17). Dieses Jahrzehnt hebt sich von den Entwicklungen aus der Vergangenheit dadurch ab, dass sich die Methoden und Formen der Cybercrime zunehmend professionalisiert, die Täter sich organisiert und sich die verschiedenen Formen der Kriminalität verwachsen haben (3).

Angereichert mit vielen Beispielen widmet sich jetzt auch McAfee dem zurückliegenden Jahrzehnt (4) und macht zunächst eine Bestandsaufnahme:

→ Die Zeit bis 2003 war geprägt von vereinzelten DDoS-Angriffen (5) und Malware (6) wurde bevorzugt per E-Mails verteilt, die mit einem Link zur Downloadseite des Angreifers versehen waren. Daneben entstanden die Makroviren, die in E-Mail-Anhängen eingebettet waren und noch heute beliebt sind. Die Angriffe waren lästig, brachten den Tätern aber noch nicht das große Geld.

→ 2004 und 2005 entstand die Adware, also lästige kommerzielle Werbung in Pop-ups, die über Downloads und Programmzusätzen verteilt wurde, und die Spyware, mit der Tastatureingaben und persönliche Daten ausgespäht wurden. Die Rootkits stellten Werkzeuge zur Tarnung von eingenisteter Malware und Abwehr von Sicherungen zur Verfügung, so dass damit verstärkt Onlinebanking-Daten ausgespäht werden und die ersten Botnetze entstehen konnten (7).

→ Zwischen 2006 und 2008 begannen sich die Täter verstärkt zu organisieren: *Einige hatten sogar eine Mafia-ähnliche Struktur mit bösartigen Hackern, Programmierern und Datenverkäufern, die Managern untergeben waren, die wiederum dem Boss untergeben waren, der für die Verbreitung von Malwarebaukästen im Internet verantwortlich war* (S. 5).

Die Bestandaufnahme bleibt an dieser Stelle etwas oberflächlich. Gemeint sind die Strukturen und Vorgehensweisen, die ich im Basar für tatgeneigte Täter (8) zusammengefasst habe (siehe Kasten rechts).

→ Die Zeit zwischen 2009 und 2010 überschreibt McAfee mit "Soziale Netzwerke und Manipulation" (S. 6) und spricht von "sozialer Manipulation". Dabei finden die Täter *heraus, welche Themen die Internetnutzer interessieren und entwickeln dann Angriffe mit populären Betreffzeilen als Köder*, um *Kreditkarteninformationen und andere persönliche Informationen zu stehlen* oder Malware zu verbreiten.

Zunehmend wurde auch Scareware eingesetzt, die dem Anwender vorgaukelt, dass sein PC mit einer neuen, weitgehend unbekannten Malware verseucht sei. Bestenfalls wurde ihm dafür ein teures, aber nutzloses Programm zum Kauf angeboten, schlimmstenfalls richtige Malware.

Der Begriff "soziale Manipulation" ist unglücklich gewählt. Es handelt sich um Formen des Social Engineerings (9) und sie sollten auch als solche bezeichnet werden.

Organisierte Cybercrime
im Cyberfahnder

- globale Sicherheitsbedrohungen, 27.07.2008;
- Der Basar, 11.04.2010
- Organisierte Internetverbrecher, 11.04.2010
- kriminelle Programmierer, 11.04.2010
- Operation Groups, 11.04.2010
- Koordinatoren, 11.04.2010
- Schurkenprovider, 11.04.2010

Schwachstellen

Die abschließenden Beispiele in McAfees Bericht sind beachtlich:

→ seit 2004 breitete sich der auf Spam-Mails spezialisierte Wurm MyDoom's sehr schnell aus, der verursachte Schaden durch verlangsamte IT-Systeme wird auf 38 Milliarden $ geschätzt

→ schon seit 2000 verbreitete der „I love you"-Wurm einen Virus, dessen Beseitigung und damit verbundenen Produktionsausfällen rund 15 Milliarden $ gekostet haben soll

→ Conficker verbreitete seit 2007 Keylogger und andere Spyware, um persönliche Daten auszuspähen; der Schaden wird auf 9,1 Milliarden $ geschätzt

→ der 2009 bekannt gewordene Stuxnet-Wurm wird als zielgerichtet und gefährlich bezeichnet; der von ihm ausgegangene Schaden ist noch unbekannt

→ dasselbe gilt für das seit 2007 aktive Zeus-Botnetz; die Malware ist auch darauf ausgerichtet, beim Online-Banking eingegebene Daten inklusive Passwörtern zu erfassen und persönliche Informationen erbeuten (S. 9).

Der Bericht schließt mit den verbreitetesten Cybercrime-Methoden,

→ der Scareware (10),
→ dem Phishing (11) nach Onlinebanking- und anderen persönlichen Daten,
→ den gefälschte Webseiten (12),
→ dem Online-Partnervermittlungsbetrug (13) und
→ dem Vorschussbetrug nach Art der Nigeria Connection (14).

Vorausschau

Die künftigen Schwerpunkte der Cybercrime sieht McAfee vor allen im Scamming, also dem Ausspähen persönlicher Daten durch geschickte Kontakte und gezielte Einsätze von Malware in sozialen Netzen, in den weiter verfeinerten Identitätsdiebstählen (15) und der Verbreitung von Malware und Botnetzen auf mobilen Endgeräten (16).

Fazit

Der Bericht über die Internetkriminalität in den letzten 10 Jahren zeigt nicht die gewohnte Güte und Tiefe der anderen Studien, die sich mit dem Thema befassen. Das gilt besonders auch für analytischen Aussagen, für die Paget Beispiel gebend ist (17), und für die begriffliche Klarheit. Einfach nur von Mafia-ähnlichen Strukturen zu reden, ohne klar zu sagen, was gemeint ist, oder neue Begriffe wie "soziale Manipulation" einzuführen, verschleiert eher die Phänomene, weil sie aus dem Zusammenhang mit bekannten Erscheinungsformen genommen werden. Darüber hat sich nicht zuletzt Muttik an anderer Stelle aufgeregt (18).

Trotz der Kritik ist der Bericht wertvoll, weil er die von mir entwickelten Modelle bestätigt (19) und mit weiteren Beispielen untermauert. Er ist kurz und lässt sich Dank seiner angemessenen Sprache schnell erfassen und lesen.

Die Veröffentlichungspolitik von McAfee begreife ich nicht. Ganz wichtige Studien aus der Vergangenheit sind nicht mehr verfügbar (20) und die wirklich wichtige Studie von Paget ist nicht in deutscher Sprache erschienen (21). Man könnte den Eindruck bekommen, dass der deutsche Sprachraum von McAfees kritischen und wichtigsten Analysen frei gehalten werden soll. Warum bloß?

(1) ▸ François Paget, Cybercrime and Hacktivism, McAfee Labs 15.03.2010;
▸ Strukturen der Cybercrime, CF 21.11.2010;
▸ Dieter Kochheim, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010
(2) ▸ Kochheim, Eine kurze Geschichte der Cybercrime, November 2010;
▸ Kochheim, Cybercrime und Cyberwar, November 2010 (Folienvortrag).
(3) ▸ Mafia, Cybercrime und verwachsene Strukturen, 20.10.2010
(4) ▸ McAfee, Ein gutes Jahrzehnt für Internetkriminalität. McAfees Rückblick auf zehn Jahre Internetkriminalität, McAfee 27.01.2011
(5) ▸ verteilter Angriff, CF 2007
(6) ▸ Malware, CF 12.05.2008
(7) ▸ Botnetze, CF 2007
(8) ▸ Basar für tatgeneigte Täter, 11.04.2010
(9) ▸ Fünf unwichtige Informationen ergeben eine sensible, CF 01.03.2009
(10) ▸ Scareware und organisierte Cybercrime, CF 15.08.2010
(11) ▸ Missbrauch fremder Identitäten, CF 22.11.2008
(12) ▸ Massenhacks von Webseiten werden zur Plage, CF 14.03.2008
(13) ▸ Ich Maria, die russische Frau, CF 02.12.2008
(14) ▸ Evergreen: Vorschussbetrug nach Nigeria-Art, CF 17.03.2008; ▸ (Fast) 30 Jahre Spam aus Nigeria! CF 2007;
▸ Manager entfernter Filialen, 25.04.2009.
(15) ▸ vom Kontoeröffnungsbetrug zum Identitätsglibber, CF 03.12.2010
(16) ▸ Smartphone-Zombies, CF 25.01.2011
(17) Ebenda ▸ (1).
(18) ▸ Zero-Day-Exploits und die heile Hackerwelt, CF 06.11.2010; ▸ Igor Muttik, Zero-Day Malware (engl.), McAfee 19.10.2010.
(19) ▸ Bestätigungen des Entwicklungsmodells von der Cybercrime, CF 21.11.2010
(20) ▸ McGau: McAfee hat das Threat Center aufgegeben, CF 14.12.2010
(21) Ebenda ▸ (3).

Luigi, das kostet Dich etwas!

▸ CF 14.02.2011

Verantwortungsvoll geht mit Sicherheitslücken nur um, wer sie sauber dokumentiert, auf dem Silberteller dem Hersteller übergibt, "Danke" sagt und dann die Klappe hält. So hätten das die großen Softwareanbieter gerne.

Uli Ries gibt in der jüngsten c't einen ersten Einblick in den offenen Markt, der um Exploits entstanden ist (1). Den Schwarzmarkt deutet er nur an. Dort werden fünfstellige und im Einzelfall auch 100.000 $ für einen Exploit gezahlt (2). Ohne ihn gäbe es aber keinen legalen Markt, auf dem immerhin 3.100 $ und mehr, die Rede ist von bis zu 40.000 $, für die Dokumentation einzelner Schwachstellen bezahlt wird. *Beim jährlichen Pwn2Own-Wettbewerb der Zero Day Initiative (ZDI) lobt der Veranstalter sogar Preisgelder von insgesamt 100.000 Euro aus.* (1)

ZDIs Mutterunternehmen ist HP Tipping Point. Mit dem Einkauf fremder Exploit-Beschreibungen von "White-Hat-Hackern" erspart es sich die eigene Suche und das Reverse Engineering (Rekonstruktion der Wiederholbarkeit eines Fehlers), um damit seine Intrusion-Prevention-Systeme aufzurüsten (Prozessüberwachung in einem Netzwerk). Das andere genannte Unternehmen ist iDefense, eine Tochter von Verisign.

Das französische Unternehmen Vupen behauptet von sich, es sei der *"Weltmarktführer bei der Schwachstellenforschung"*. Es kauft keine Exploits, sondern sucht sie selber und vermarktet sie mit seinem Threat Protection Program - TPP. Seine Marktstrategie ist lustig: Potenziellen Kunden wird eine Sicherheitsanalyse erstellt. Wenn der Kunde aber nicht zahlt, dann erhält er keine weiteren Informationen über ihre genaue Gestalt oder ihre Abwehr. In der Branche wird ein bisschen von Erpressung gemunkelt.

Die führenden Software-Anbieter, namentlich Microsoft und Adobe, weisen es weit von sich, für Exploits zu zahlen. Es bleibt der Eindruck, dass solche Geschäfte über Dritte oder durch Tauschhandel mit anderen wertvollen Informationen abgewickelt werden.

Solche Leckerbissen findet man selten, aber eben doch bevorzugt in der c't. Mir war zwar klar, dass die Software- und die Hersteller von Sicherheitssoftware nach Exploits jagen, nicht aber, dass sie auf dem grauen Markt sensible Informationen kaufen, um Exklusivrechte zu erlangen. Auch Vupen als grauer Jäger war mir völlig unbekannt. So wie Ries das Geschäftsmodell dieses Unternehmen beschreibt, bimmelt ein bisschen Mafia im Hinterkopf: *"Luigi, ich habe eine Information für Dich, die Du nicht ablehnen kannst. Aber Du weist ja: Das kostet Dich etwas".*

Im Gespräch mit heise Security erklärte Holden, dass Exploits für weitverbreitete Produkte wie Adobe Reader, Internet Explorer oder Windows zwischen 50.000 und 100.000 US-Dollar auf dem Schwarzmarkt bringen. "Was gerade verlangt wird, hängt immer vom Ziel der Angreifer ab ...“ (2)

(1) Uli Ries, Das Geschäft mit den Bugs. Sicherheitslücken als Handelsware, c't 5/2011, S. 82

(2) Teilweise werden astronomische Zahlen genannt, sechsstellige $-Beträge dürften jedoch im Raum stehen:
▸ Uli Ries, Spekulationen über Schwarzmarktpreise für Exploits, Heise online 16.02.2011.

IT-Söldner im Kampfeinsatz

CF 15.02.2011

Dossier gegen Anonymous

Die Security-Firma HBGary ist vor allem bekannt durch ihre Analyseprogramme, mit denen sich der Arbeitsspeicher von Windowssystemen zu forensischen Zwecken und zur Entdeckung von Malware analysieren lässt. Das Unternehmen hat eine Tochter, die HBGary Federal unter Leitung von Aaron Barr, die sich auch mit der Auswertung sozialer Netze (IRC, Facebook, Twitter) befasst (1).

Ausweislich eines jetzt veröffentlichten Dossiers (2) sammelte Barr Informationen rund um Aktivisten, die er der Anonymous-Bewegung zurechnet. Er dokumentiert insgesamt 10 Gruppen mit zusammen fasst 20.000 Mitgliedern (siehe Kasten rechts oben). In einem weiteren Teil konzentriert er sich auf Einzelpersonen. Aus Deutschland nennt er insgesamt 22 Personen mit so netten Namen wie Max Mustamaann, Karl Kot und Kerlchen Vom Hof. Aus der Schweiz stammt zum Beispiel Daniel Dusentrieb.

Das Dossier scheint auf solider Handarbeit zu beruhen und dokumentiert Fundstellen, die zugeordnet, bewertet und verbunden werden. Die Methode ist klassisch und dient zur Bestandsaufnahme. Wie bei allen Auswertungen im Zusammenhang mit dem Social Engineering (3) gilt auch hier (4):

Fünf harmlose Informationen bergen eine brisante.

Bevor Barr seine Ergebnisse an die US-Behörden verkaufen konnte, kam es jedoch ganz anders: Unbekannte brachen in mehrere Systeme ein und veröffentlichten nicht nur dieses Dossier, sondern auch HBGarys E-Mail-Archive und weitere Informationen. Heise online (5)

Anonymous

Anonymous machte auf sich zuerst 2008 aufmerksam, indem sich ein offenbar lockerer Verbund von Internet-Aktivisten gegen die Scientology aufstellte (6). Besonders bekannt wurde die Gruppe durch die Operation Payback (7). Sie unternahm DDoS-Angriffe gegen Gegner von WikiLeaks, die ihrerseits Angriffe gegen die Plattform gerichtet hatten, und gegen Unternehmen und vor allem Finanzunternehmen, die in den Verruf gekommen waren, die Arbeit von WikiLeaks durch Kontensperren und Abklemmen von Hostspeicher zu behindern (8). Schon vorher hatte das "kopflose Kollektiv", wie es sich selber nennt, Unternehmen angegriffen, die Urheberrechtsverletzungen verfolgen (9). Zuletzt wurde Anonymous durch DDoS-Angriffe zur Unterstützung des Widerstandes in Ägypten bekannt (10).

Das Anonymous-Kollektiv scheint als Ganzes ein lockerer Zusammenschluss zu sein, der sich zur Erreichung gemeinsamer Ziele verbindet.

Barr: Gruppen bei Anonymous

Operation Payback ITA	294	10.12.2010
Operation Leakspin	2.286	10.12.2010
Anonyswiss	386	11.12.2010
Operation Paperstorm	956	13.12.2010
Anonymous News Network	7.081	13.12.2010
Operation Darknet	259	14.12.2010
Operation Payback	811	16.12.2010
Crowdleak	811	26.12.2010
Anonymous – Operation Tunisis		05.01.2011
Operation Egypt	6.489	18.01.2011

Es besteht aus einzelnen Sympathisanten und kleinen stabilen Gruppen, wie in einem in der c't veröffentlichten Interview zu erfahren war (11). Die internen Diskussionen um die Effektivität von Widerstandshandlungen haben auch zur Gründung des subversiven Nachrichtenportals Crowdleaks (zunächst: Leakspin) geführt:

Operation Leakspin ist eine von verschiedenen Operationen, die von Anonymous-Mitgliedern gestartet wurde, die erkannt haben, dass DDoS auf Dauer kein Mittel ist. Oder zumindest kein effektives Mittel (12).

Jedenfalls hat Anonymous die öffentliche Diskussion um die Widerstandsformen im Internet angeregt (13).

Der Kampf gegen WikiLeaks

Die von den Anonymous-Hackern veröffentlichten Dokumente bergen Brisanz.

HBGary Federal sowie die Firmen Palantir und Berico sehen in WikiLeaks eine besondere Bedrohung, wie sich aus einer ebenfalls veröffentlichten, ganz neuen Präsentation ergibt (14). Sie geht zur Sache, schießt sich auf Assange ein und nennt weitere Namen (S. 3, 4), zeigt die Standorte der WikiLeaks-Infrastruktur (S. 10) und gibt heftige Handlungsempfehlungen (S. 14, siehe rechts), die mit demokratischen Spielregeln und Meinungsfreiheit nichts gemein haben. Schließlich kommt die Analyse (S. 19) und bieten sich die drei Unternehmen als Partner im Kampf gegen WikiLeaks an:

WikiLeaks ist keine Einzelperson und keine einzelne Organisation, sondern ein Netzwerk aus Personen und Organisationen, die nur deshalb zusammenarbeiten, um nicht nachverfolgbar massenhaft vertrauliche Dokumente zu veröffentlichen (15).

Aus dem veröffentlichten Material ergibt sich zum Beispiel auch, dass *HBGary unter Code-Namen wie Project C, Task Z, Task M Trojaner, Rootkits und andere Spionageprogramme im Wert von vielen 100.000 Dollar anbietet.* (16)

WikiLeaks

ist eine Organisation (17), die Geld damit verdient (18), dass sie vertrauliche Informationen verkauft und veröffentlicht. Sie entstand bereits 2006 und widmete sich zunächst bevorzugt regimekritischer Dokumente, die sich zum Beispiel gegen die Regierungen von China, Israel, Nordkorea, Russland, Simbabwe und Thailand wandten (19). Einen guten Überblick über die Veröffentlichungen bei WikiLeaks gibt die Wikipedia (20).

2009 gerieten zunehmend die USA in den Blickpunkt: Zunächst wurden Videoaufnahmen aus der Bordkamera eines Kampfhubschraubers über den Tod irakischer Zivilisten und Journalisten gezeigt (21) und dann folgten Schlag auf Schlag Dokumente aus (22)

→ dem ▸ Afghanistan-Krieg (Juli 2010),
→ dem ▸ Irak-Krieg (Oktober 2010) und
→ die ▸ diplomatischen Depeschen (November 2010).

Empfehlungen gegen WikiLeaks

von Palantir, HBGary Federal und Berico:

→ *Gießen Sie heißes Öl zwischen die befeindeten Gruppen. Desinformation. Erstellen Sie Nachrichten über die Aktionen, um sie zu sabotieren oder die gegnerische Organisation zu diskreditieren.*
Nutzen Sie gefälschte Unterlagen und beschweren Sie sich dann über die Fehler.

→ *Zeigen Sie die Mängel in der Sicherheit der Infrastruktur. Schreiben Sie entlarvende Geschichten. Wenn Sie Glauben finden, dass der Gegner unsicher ist, dann ist er fertig.*

→ *Cyber-Angriffe gegen die Infrastruktur zur anonymen Einsendung von Dokumenten. Dies würde das Projekt töten. ...*

→ *Medien-Kampagnen, um die radikale und rücksichtslose Natur der Wikileaks-Aktivitäten offenzulegen. Anhaltenden Druck. Tut nichts gegen die Fanatiker, aber sät Bedenken und Zweifel unter den Gemäßigten.*

→ *Sucht nach Lecks. Verwenden Sie soziale Medienprofile und identifizieren Sie riskantes Verhalten Ihrer Mitarbeiter.* (23)

Neue Qualität des Hacktivismus

McAfee hebt in seinem jüngst erschienenen Bedrohungsbericht für das 4. Quartal 2010 den Hacktivismus, WikiLeaks und die Hacktivistengruppe Anonymous besonders hervor, ohne die Vorgänge im einzelnen darzustellen und zu bewerten (24). Und tatsächlich heben sich die jüngsten Auseinandersetzungen ganz deutlich von den älteren Defacement- und Hacktivismus-Aktionen ab, über die Paget vor knapp einem Jahr dankenswerter Weise berichtet hat (25).

Kennzeichen für eine neue Qualität des Hacktivismus sind:

→ Noch keine zivile Organisation hat einen solchen Stepptanz auf den Füßen der USA veranstaltet wie WikiLeaks. Die schnelle Folge und Masse peinlicher und entlarvender Dokumente waren keine Nadelstiche mehr, die mit ein wenig Diplomatie kaschiert werden konnten, sondern schwere Perforationen.

→ Die DDoS-Angriffe gegen WikiLeaks blieben wirkungslos, weil ganz schnell mehr als 1.000 gespiegelte Mirrors entstanden (26). Daran scheitert jeder Gegner.

→ Neue Seiten zogen die Gegner von WikiLeaks auf, indem sie die existenziellen Grundlagen der Plattform und ihres Aushängeschilds Assange angriffen: Sperrung von Hostspeicher und Konten.

→ An dieser Stelle kommt Anonymous ins Spiel, indem seine Hacktivisten genau die Wirtschaftsunternehmen angriffen, die die Existenz von WikiLeaks bedrohten. DDoS war vorher nur als Instrument zur Erpressung und zum politischen Kampf gegen politische Gegner bekannt, nicht aber dazu, von Wirtschaftsunternehmen die Geltung von Spielregeln einzufordern.

→ Anonymous selber stellt eine neue Form des zivilen Widerstandes dar. Das Kollektiv besteht aus Personen und Gruppen, die weltweit verteilt sind und ihre Gegner und Angriffsmethoden sehr genau auswählen. Die breite Vielfalt ihrer Anlässe zum Hacktivismus sind ebenfalls noch ungewohnt.

Die verlorene Unschuld der Ökonomie

Ich wage zu bezweifeln, dass diese Botschaft bereits angekommen ist: Ein radikaler Teil der Internetgemeinde fordert die Einhaltung von Spielregeln ein! Unternehmen wie Amazon und große Finanzdienstleister können sich nicht mehr wie gewohnt selbstgerecht zurücklehnen, sich auf mehr oder weniger berechtigte AGB-Verstöße berufen, die ihnen so lange nicht aufgefallen sind, wie sie noch in Ruhe Geld verdienen konnten, oder gefahrlos politischem Druck aus dem Mainstream nachgeben. Die Angriffe von Anonymous machen sie zum Angriffsobjekt alternativen Wohlverhaltens. Das ist schmerzhaft!

Die Enthüllungen um HBGary Federal und Aaron Barr sind Symptome für eine weitere Verschärfung der destruktiven Auseinandersetzungen im Internet:

→ Zwischen Cybercrime und Hacktivismus haben sich Firmen etabliert, die dieselben Methoden nutzen, um gutes Geld zu verdienen. Sie suchen nach Exploits und lassen sich dafür bezahlen (27), betreiben Social Engineering gegen ausgesuchte Gegner (Dossier gegen Anonymous), entwickeln Strategien, die den militärischen Vorstellungen vom Informationskrieg gleichen (falsche Dokumente und Lügen gegen WikiLeaks), handeln ungeniert mit Überwachungstechnik (HBGary) und schrecken auch ihrerseits nicht vor DDoS-Angriffen zurück.

→ Die nächste Eskalationsstufe wäre die gezielte physische Vernichtung eines Gegners durch Söldner oder andere gedungene Mörder (28).

→ Der Angriff gegen HBGary Federal zeigt einen weiteren Aspekt der Eskalation. Die Spielereien, dass sich gegnerische Hackerboards nur gegenseitig behaken (29), sind vorbei. Jetzt müssen auch die gut verdienenden Profis damit rechnen, mit ihren Leichen im Keller an die Öffentlichkeit gezerrt zu werden. Durch Enthüllungsplattformen einerseits und professionelle Hacker andererseits.

Nun doch: Cyberwar?

Ich habe den Cyberwar als eine gezielte und zerstörerische Auseinandersetzung mit den Mitteln und gegen die gegnerischen Infrastrukturen der Netzkommunikation definiert. So verstanden umfasst der Begriff nicht nur militärische Akteure, sondern auch politische Aktivisten, Unternehmen, Terroristen und die organisierte Cybercrime. Er ist gekennzeichnet von dem 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 (30). Insoweit unterscheide ich zwischen dem Kalten und dem Heißen Cyberwar und habe behauptet, dass wir bereits eine kalte Phase erleben.

Diese Auffassung steht im Widerspruch zur militärisch und völkerrechtlich ausgerichteten Position (31), auch wenn die militärische Forschung dieselben Probleme und Bedrohungen beschreibt (32).

Der fehlende Beleg für meine Thesen sind die Wirtschaftsunternehmen gewesen, die sich an den handfesten bis hin zu vernichtenden Aktionen beteiligen. Diese Lücke schließen die Berichte über Exploit-Jäger und der Einzelfall HBGary Federal.

Außerdem sprechen die hier aufgezeigten Eskalationen eine deutliche Sprache. Das ist zwar noch kein Heißer Cyberwar, aber ... !

Die heutigen organisierten Konfrontationen im Internet kennen keine Regularien, weder völkerrechtliche noch zivilgesellschaftliche, keine Toleranz, keine Zurückhaltung und keine Verhältnismäßigkeit. Keine ihrer Parteien hat eine saubere Weste und keine kann für sich allein in Anspruch nehmen, "wir sind die Guten". Anonymous hat bewiesen, dass auch die Hacktivisten äußerst gut aufgestellt sind und die Netzindustrie nicht nur aus klinisch reinen Saubermännern besteht.

(1) ▸ Anonymous kompromittiert amerikanische Sicherheitsfirma, Heise online 15.12.2011
(2) ▸ Aaron Barr, Anonymous, 31.01.2011 (PDF)
(3) ▸ Fünf unwichtige Informationen ergeben eine sensible, CF 01.03.2009
(4) Siehe zuletzt ▸ Datenspuren. Das Ende des Privaten, CF 18.12.2010
(5) ▸ (1). ▸ Anonymous retaliates against HBGary espionage, Crowdleaks 08.02.2011.
Einzelheiten über den Angriff: ▸ Hintergründe zum Einbruch bei US-Sicherheitsfirma, Heise online 16.02.2011.
(6) ▸ Anonymous (Kollektiv). Entstehung, Wikipedia
(7) ▸ Operation Payback, Wikipedia
(8) ▸ Das Ende virtueller (T) Räume. Wikileaks, CF 09.12.2010; ▸ Nachtrag: Operation Payback, CF 11.12.2010
(9) ▸ Das Jahr der gezielten Angriffe. Internetkriminalität, CF 20.11.2010; ▸ Gegen Verfolger von Urheberrechtsverstößen, Wikipedia.
(10) ▸ Molotowcocktails im Internet, CF 05.02.2011
(11) ▸ Jan-Keno Janssen, "Anonymous verändert sich gerade dramatisch", c't 16.12.2010
(12) Ebenda ▸ (11)
(13) ▸ sie wollen doch nur spielen, CF 15.12.2010; ▸ Internet-Reset #2, 05.02.2011; ▸ Cyberspace und Cyberwar, 06.02.2011;
▸ Infokrieg bei Wikileaks, 10.02.2011; ▸ Geheimnisverrat von Wikileaks, 12.02.2011.
(14) ▸ Palantir Technologies, HBGary Federal, Berico Technologies, The WikiLeaks Threat, 09.02.2011 (PDF)
(15) Eigene Übersetzung. Im Original: untraceable mass document leaking.
(16) Zitat von Heise online ▸ (1).
Einzelheiten: ▸ HBGary INC. working on secret rootkit project. Codename: “MAGENTA”, Crowdleaks 14.02.2011
(17) Erste Erwähnung: ▸ Heimlichkeiten, CF 08.08.2010.
(18) ▸ Geschäftsmodell WikiLeaks, CF 25.12.2010
(19) Die sechs Länder werden hervorgehoben, weil sie den nationalen Zugang zu WikiLeaks gesperrt haben:
▸ WikiLeaks. Geschichte, Wikipedia.
(20) ▸ Veröffentlichungen von WikiLeaks, Wikipedia
(21) ▸ Gewaltsamer Tod irakischer Zivilisten und Journalisten durch US-Militärs, Wikipedia
(22) ▸ WikiLeaks, CF 09.12.2010
(23) Eigene Übersetzung
(24) ▸ Bedrohungen im 4. Quartal 2010, CF 13.02.2011; siehe auch GData:▸ Wachstumsgrenze für Malware, CF 08.02.2011.
(25) ▸ Mafia, Cybercrime und verwachsene Strukturen, CF 2010.2010; ▸ François Paget, Cybercrime and Hacktivism, McAfee 15.03.2010.
(26) ▸ Hacktivismus, CF 09.12.2010
(27) ▸ Luigi, das kostet Dich etwas! CF 14.02.2011
(28) ▸ universal soldiers, CF 10.01.2010
(29) ▸ Hacker cracken Carder-Forum, CF 23.05.2010
(30) ▸ Kommunikationstechnik und Cyberwar, CF 27.06.2010
(31) ▸ Spielregeln für den Cyberwar, CF 14.09.2010
(32) ▸ Bedrohungen gegen den Cyberspace, CF 06.02.2011

gewerbliche Unternehmen als Kritische Infrastrukturen

▸ CF 06.12.2010

Unter den jetzt bei Wikileaks veröffentlichten Dokumenten aus dem diplomatischen Depeschendienst der USA befindet sich auch eine Liste mit den ausländischen Kritischen Infrastrukturen aus 2008 (1), die einer besonderen Beobachtung bedürfen. Der Teil, der Deutschland betrifft, wird links zitiert. An erster Stelle stehen die Orte, an denen die wichtigsten Seekabel landen, in Norden und Sylt.

Ich sehe mich darin bestätigt, dass ich die Kommunikationsnetze und ihre internationalen Anbindungen in Bezug auf den Cyberwar hervorhebe. Bei TAT-14 (2) handelt es sich um ein ringförmiges Kabel, das maßgeblich auch von der DTAG betrieben wird und Europa mit Nordamerika verbindet. Diese Verbindung schafft auch AC-1 (3). Für beide Standorte gilt: Sie verfügen über Häfen und erfahrene Seeverbindungen. Genau dort, entlang den üblichen Schifffahrtsrouten, werden die Seekabel verlegt. In bekannten Gewässern, wo die verlegenden Schiffe ohne Überraschungen navigieren können. Dasselbe gilt für die Schiffe, die die Kabel wieder heben müssen, damit sie bei Bedarf geflickt werden können.

Die Exklusivität der Landungsstellen steht aber in Frage, weil ab Belgien und den Niederlanden auch starke Landverbindungen zur Verfügung stehen. Norden und Sylt dürften deshalb unter Sicherheitsgesichtspunkten zwar interessant, aber nicht kriegsentscheidend sein.

Mit der Liste setzt sich auch Rötzer in Telepolis auseinander (4) und betrachtet die Komponenten. Er bleibt dabei sehr locker.

Das geht mir zunehmend ab. Ich traue den US-amerikanischen Analysten viele Fehleinschätzungen und Übertreibungen zu. Das gehört zur Sichtung im Rahmen einer Analyse dazu und es wäre eher falsch, wenn in einer Feldstudie wichtige Betrachtungsobjekte fehlen würden. Wenn man sie nicht betrachtet, dann kann man sie auch nicht wieder zurückstufen.

Die Liste ist nun einmal in der Welt und dokumentiert die Betroffenheit der US-Administration an der Zulieferung und Zuverlässigkeit deutscher Industrie- und Gewerbestandorte. Das sollte Anlass dazu geben, sie auch hier als Kritische Infrastrukturen zu betrachten. Interessant ist nämlich, dass vor Allem spezialisierte, produzierende Unternehmen mit hohem Knowhow genannt werden. Als Kritische Infrastrukturen werden sonst vor Allem kommunikationsabhängige Strukturen angesehen, die örtlich verteilt sind. Der Blick aus den USA lenkt auch unsere Aufmerksamkeit auf industrielle Brain-Tanks

kritische Infrastrukturen in Deutschland

Germany: TAT-14 undersea cable landing, Nodren, Germany. Atlantic Crossing-1 (AC-1) undersea cable landing Sylt,
Germany BASF Ludwigshafen: World's largest integrated chemical complex
Siemens Erlangen: Essentially irreplaceable production of key chemicals Siemens, GE, Hydroelectric Dam Turbines and Generators
Draeger Safety AG & Co., Luebeck, Germany: Critical to gas detection capability
Junghans Fienwerktechnik Schramberg, Germany: Critical to the production of mortars TDW-Gasellschaft Wirksysteme, Schroebenhausen,
Germany: Critical to the production of the Patriot Advanced Capability Lethality Enhancement Assembly Siemens, Large Electric Power Transformers 230 - 500 kV Siemens, GE Electrical Power Generators and Components Druzhba Oil Pipeline
Sanofi Aventis Frankfurt am Main,

. . . . . .

von besonderer und vielleicht auch exklusiver Bedeutung.

Die nötige Kompetenz zur Analyse traue ich vor Allem dem Bundesamt für Verfassungsschutz (5) und Fraunhofer (6) zu. Von anderen Einrichtungen, mit denen ich zu tun gehabt habe, weiß ich, dass sie manchmal mit zu lauem Wasser hantieren.

Ich weiß ein wenig, wie das BKA in Bezug auf die Cybercrime und den Cyberwar aufgestellt ist. Beim BND und anderen Geheimdiensten fehlt mir das praktische Wissen. Ihre Erfolge werden auch nicht öffentlich bekannt - aus gutem Grund oder weil sie fehlen.

Die praktische Konsequenz aus der gleichzeitigen Betrachtung der Kritischen Infrastrukturen und der denkbaren Cyberwar-Strategien ist, dass wir uns darauf einlassen und zwingen müssen, verschiedene Blickweisen einzunehmen, um Risiken zu benennen, sie zu bewerten und ihnen zu begegnen. Der IT-typische und der Management-Blick sind zu häufig beschränkt auf einzelne Phänomene, wobei zu selten innerlich ein Schritt zurück getreten wird, um das Problem in seiner Umgebung zu betrachten.

Die Fragen, die beantwortet werden müssen, sind meistens ganz einfach: Was kann eine Technik, ein Unternehmen oder eine Struktur? Was passiert, wenn sie ausfallen?

CF 05.02.2011

In der jüngsten Ausgabe der c't berichtet Christiane Schulzki-Haddouti (7) ausführlich und hintergründig über die bei Wikileaks veröffentlichte Liste mit den ausländischen Kritischen Infrastrukturen aus 2008, von der hier berichtet wurde. Sie kritisiert zu recht, dass in Deutschland vor allem die kommunikationstechnischen Systeme als gefährdet angesehen und industrielle Fertigungsanlagen ausgeblendet werden. Das sieht die US-amerikanische Verwaltung anders, wie die Liste zeigt.

(1) ▸ Liste mit den ausländischen Kritischen Infrastrukturen aus 2008

(2) ▸ TAT-14 beschädigt? CF 24.03.2008

(3) ▸ AC-1, Wikipedia

(4) ▸ Florian Rötzer, US-Regierung listet die für das nationale Interesse kritische Infrastruktur im Ausland auf, Telepolis 06.12.2010

(5) ▸ Bundesamt für Verfassungsschutz

(6) ▸ Fraunhofer

(7) ▸ Christiane Schulzki-Haddouti, Eierlauf Kritische Infrastrukturen neu betrachtet, 't 4/2011, S. 68

kritische Infrastrukturen in Deutschland

Germany: Lantus Injection (insulin) Heyl Chemish-pharmazeutische Fabrik GmbH: Radiogardase (Prussian blue) Hameln Pharmaceuticals, Hameln,
Germany: Pentetate Calcium Trisodium (Ca DTPA) and Pentetate Zinc Trisodium (Zn DTPA) for contamination with plutonium, americium, and curium IDT Biologika GmbH, Dessau Rossiau, Germany: BN Small Pox Vaccine. Biotest AG, Dreiech,
Germany: Supplier for TANGO (impacts automated blood typing ability) CSL Behring GmbH, Marburg, Germany: Antihemophilic factor/von Willebrand factor Novartis Vaccines and Diagnostics GmbH, Marburg, Germany: Rabies virus vaccine Vetter Pharma Fertigung GmbH & Co KG, Ravensburg, Germany (filling): Rho(D) IGIV Port of Hamburg

Schutz Kritischer Infrastrukturen

▸ CF 13.02.2011

Mit einer werbend ausgerichteten Studie setzt sich McAfee mit den Kritischen Infrastrukturen in Unternehmen auseinander (1). Die betreffenden Branchen werden rechts aufgeführt. Diese Aufzählung ist fast deckungsgleich mit der der US-Air Force (2) und setzt sich damit einmal mehr von der zu engen deutschen Vorstellung ab. Die vorgeschlagenen Schutzmaßnahmen werden auf der folgenden Seite dargestellt.

Die zuletzt aufgeführte Maßnahme ist am schwierigsten zu realisieren: Wie schafft man Performance und Verfügbarkeit bei gleichzeitiger Absicherung und Abschottung? McAfee empfiehlt sein

Trusted Security-Modell

Ausgangspunkt ist ein „positives“ Sicherheitskonzept, bei dem alle nicht ausdrücklich zulässigen Handlungen verweigert werden. Daraufhin werden Reputationswerte auf Grundlage umfangreicher Verhaltensanalysen berechnet. Diese Kombination bietet die präziseste Echtzeit-Gefahrenabwehr auf dem Markt.

Kritische Infrastrukturen im Kreuzfeuer

▸ CF 13.02.2011

Den Faden nimmt eine Studie aus dem Dezember 2009 auf: Im Kreuzfeuer (3). Die drei Autoren setzen damit den Startpunkt in den Veröffentlichungen von McAfee für die Betrachtung, dass sich die Cybercrime tendenziell den Methoden des Cyberwar nähert.

Sie haben 600 Sicherheitsfachleute aus 14 Ländern zur IT-Sicherheit befragt. Das Ergebnis: Kritische Infrastrukturen stehen unter dauerndem Beschuss von DDoS-Attacken und Hacking-Versuchen. Sie berichten von langwierigen DDoS-Attacken, den ersten Anzeichen der Night Dragon-Angriffe aus dem September 2009 und von Manipulationen an ihren

Kritische Infrastrukturen nach McAfee

→ *Energiewirtschaft – Stromübertragungs- und Vertriebsnetze, Öl- und Gaspipelines, Wasserverteilung und -versorgung sowie radioaktive Stoffe und Kernkraftwerke*

→ *Transportwesen – Straßen-, Schienen- und Lufttransport, ÖPNV-Netze, Logistik und Gefahrguttransporte*

→ *Staatliche und kommunale Dienste – Wassersysteme und Müllentsorgung*

→ *Prozessfertigung – Chemische und petrochemische Abfälle und Sondermüll*

→ *Informations- und Kommunikationstechnik – Telekommunikation, Fernsehen und Radio*

→ *Notdienste – Rettungsdienste, Gesundheitswesen, Feuerwehr und Polizei*

→ *Bank- und Finanzwesen - Handelssysteme, Netzwerke für automatische Verrechnung und Geldautomatennetze*

Prozesssteuerungssystemen (Supervisory Control And Data Acquisition - SCADA; S. 10).

Soweit die heftigsten Angriffe zurückverfolgt werden können, kommt China ins Spiel. Natürlich können sich die Systeme, von denen aus der tatsächliche Angriff geführt wird, überall befinden, ohne den Standort des Hintermanns zu offenbaren. Die Häufung ist jedoch zu auffällig.

Die Studie zeigt die Anfänge, die McAfee dazu veranlasst haben, die permanenten Angriffe durch Hacking und DDoS gegen Unternehmen mit Kritischen Infrastrukturen und den zunehmenden Hacktivismus als Anzeichen für den Übergang von der lästigen über die schmerzhafte Cybercrime bis hin zum Cyberwar zu zeichnen. Sie beruft sich nicht nur auf Erfahrungen, sondern auch auf statistische Erhebungen. Diese Methode mag nicht wissenschaftlich genau sein, hilft aber, Erfahrungen zu erheben, zu ordnen und zu bewerten. Das ist der erste Schritt zu einer gesicherten Analyse, die wissenschaftlichen Ansprüchen standhält. Sozusagen: Feldarbeit. Auf sie bauen dann andere auf. Das gilt auch für den Cyberfahnder.

(1) ▸ McAfee, Fünf Möglichkeiten zum Schutz kritischer Infrastrukturen, McAfee 14.05.2009

(2) ▸ Grundversorgung als Kritische Infrastruktur, CF 06.02.2011

(3) ▸ Stewart Baker, Shaun Waterman, George Ivanov, In the Crossfire. Critical Infrastructure in the Age of Cyber War, McAfee 17.12.2009

(4) Siehe auch: ▸ Bestandteile eines professionellen Netzwerkes, 2007.

Schutzmaßnahmen nach McAfee (4):

→ *Echtzeitschutz. Laufende Überwachung des Datenverkehrs wegen der Zieladressen, Ports, Datenzugriffe von außen mit Firewalls und mit Virenscannern*

→ *Abtrennung und Abschirmung kritischer Infrastrukturen von verbundenen Netzwerken*
- → *Erste Schutzstufe: die Firewall*
- → *Zweite Schutzstufe: Intrusion Prevention (Prozessüberwachungen im internen Netz)*

→ *Kontrolle der Zugriffsberechtigungen und Netzwerkaktivitäten (siehe oben)*

→ *Schutz von Daten über kritische Infrastrukturen vor Datendiebstahl (Benutzergruppen, Zugriffsrechte, Separierung)*

→ *zuverlässiger Schutz ohne Beeinträchtigung von Verfügbarkeits-, Integritäts- und Zuverlässigkeitsanforderungen*

Konflikte im Internet

▸ CF 05.02.2011

Internet-Reset #2

Im Juli 2010 hat der BDK die Forderung nach einem Internet-Reset (1) erhoben, den ich für wenig sinnvoll halte [(2), siehe Zitat in der Mitte]. Jetzt will jedenfalls Österreich ernst damit machen. Sein *Bundeskanzleramt arbeitet seit "geraumer Zeit" an einem "Kill Switch" (Not-Aus) für das Internet* (3), um bei einer verheerenden Cyber-Attacke die nationalen Verbindungen zum Internet zu kappen. Das macht die Idee auch nicht besser.

Einen Mobilfunk- und Internet-Shot Down praktizierte gerade Ägypten (4), um sich seiner Bürgerproteste zu erwehren, ohne Erfolg (5). Google hat für Twitter einen *Microblogging-Dienst* per Telefon eingerichtet (6) und die Protestbewegung entwickelte Internet-basierte Dienste, um sich der Einkesselung durch die ägyptische Polizei zu erwehren [siehe links außen, (7)].

Auch Anonymous meldet sich wieder und *legt aus Protest Websites der ägyptischen Regierung lahm* (8). Diese offenbar locker und eher spontan organisierte Protestbewegung machte zuletzt wegen ihrer DDoS-Angriffe gegen Wikileaks-Gegner von sich reden (9).

Krankenhäuser, Polizei und andere Betreiber kritischer Infrastrukturen wären beim Reset ihrer Handlungsfähigkeit beraubt. Genau das will der Angreifer im heißen Cyberwar erreichen, um andere destruktive Aktionen durchführen zu können. Das Reset spielt ihm in die Hände. aus:

▸ Internet-Reset (2)

Molotowcocktails im Internet

"Es ist nicht korrekt, alles gleich als 'Krieg' oder 'Angriff' zu bezeichnen, was im Internet an schlechten Dingen passiert", betont James A. Lewis auf der Münchner Sicherheitskonferenz (10).

Gleichwohl mehreren sich die Beispiele dafür, dass sich der Protest und Widerstand (auch) in das Internet verlegt und neue, auch zerstörerische Aktionsformen entwickelt. Mit Angriffen auf gewerbliche Onlineshops und ihre Übernahme - Defacement - meldete sich jetzt überraschend die Berliner Hausbesetzerszene zu Wort (11). Auch Anonymous zeigt Bestand (siehe Meldung links) und scheint sich als dauerhafte, internationale Bewegung im Internet einzurichten (12).

Nach Lewis waren die Proteste, wie zum Beispiel gegen Estland (13), bislang eher harmlos. Die Cyber-Attacken könnten jedoch andere militärische Aktionen begleiten. Er verweist auf die israelische "Operation Orchard" aus dem September 2007, als der Luftangriff auf vermutete Atomanlagen mit einem Totalausfall der syrischen Radarabwehr verbunden war, auf die Sabotage durch chinesische Hackerangriffe vom Januar 2010 und schließlich auf Stuxnet.

Am bewussten Samstagnachmittag hatten sich also rund 500 Studenten, die von einer Demo gegen Einsparungen kamen, den Protesten vor der ägyptischen Botschaft angeschlossen. Dann hätten einzelne Studenten mit Sukey-Anbindung durch mitgehörten Polizeifunk und Beobachtung Hinweise auf die bevorstehende Einkesselung bemerkt und an das Sukey-Team weitergegeben, welches wiederum ihre Abonnenten informierte. Dann waren laut Sukey innerhalb von fünf Minuten auch praktisch alle Nicht-Abonnenten informiert. Bevor die Zugänge geschlossen waren, stoben die Studenten davon und es fand keine Einkesselung statt. (7)

Streit um den Cyberwar

Aus militärischer und völkerrechtlicher Sicht (14) mag es sein, dass die Analysten von McAfee zu locker mit dem Begriff "Cyberwar" umgehen. Kurtz (15) und vor allem auch Paget (16) betrachten in erster Linie die Entwicklungen der Cybercrime und stellen fest, dass sie sich nicht nur zunehmend organisiert und mit anderen Kriminalitätsformen verwächst, sondern auch politisch instrumentalisieren lässt.

Eher noch strenger als Lewis (siehe voherige Seite) grenzt Myriam Dunn Cavelty den Cyberwar von den zunehmenden Hakeleien im Internet ab (17). Sie hält den gezielten und kontrollierten Einsatz von Cyberwaffen für ausgeschlossen, unter Verweis auf Stuxnet für zu teuer und schließlich für kleine Kontrahenten zu riskant, weil die angegriffenen Militärmächte konventionell zurückschlagen könnten.

Damit wendet sie sich ausdrücklich gegen Toralv Dirro von McAfee (18), der ausgehend von den politisch motivierten Auseinandersetzungen im Internet und dem Erscheinen von Stuxnet schließt, dass künftig kriegerische Auseinandersetzungen von Cyberangriffen begleitet werden: *Angriffe auf Computernetzwerke als eine weitere Kriegswaffe anstelle eines reinen Cyberkriegs.* (19)

Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt heute immer mehr, weil manche Staaten kriminelle Organisationen als nützliche Verbündete betrachten. (15)

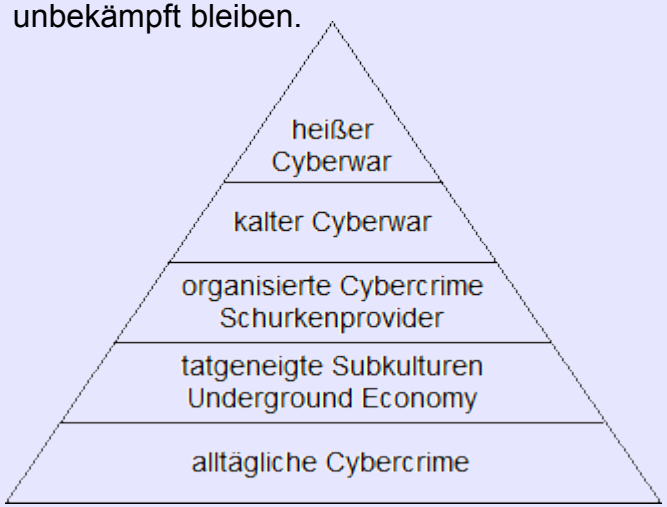
Unterstützt wird er in der interessanten Diskussion bei TheEuropean von Manfred Messmer (20), der besonders auf die Auseinandersetzungen um Wikileaks Bezug nimmt (21): *Kein Staat, kein Unternehmen, keine Rechtsordnung kann akzeptieren, dass ein anarchistischer Schwarm von ein paar Tausend Usern sich auf willkürlich ausgewählte Unternehmen, staatliche und private Organisationen stürzt und deren Webseite – das heißt heutzutage deren Geschäftstätigkeit – für Stunden oder gar Tage lahmlegt.*

Die Diskussion begann mit Raoul Chiesa (22), der als Opfer der Cybercrime einen Einzelnen oder ein Unternehmen sieht. Im Gegensatz dazu: *Cyberwar-Aktivitäten sind gezielte Attacken auf eine andere Nation. Diese Angriffe können entweder staatlich gefördert oder durch politische und religiöse Gruppen und Ideale getrieben sein. In jedem Fall ist beim Angriff auf einen Staat die Armee für die Verteidigung zuständig.*

Zuletzt hat sich Sandro Gaycken in die Cyberwar-Diskussion eingeschaltet (23) und er widerspricht Dunn Cavelty in allen drei Punkten: *... Schwache Staaten könnten Serien solcher Angriffe nutzen, um die Kräfte starker Gegner kontinuierlich zu schwächen. Es können damit gigantische Ablenkungen produziert werden. Wirtschaften können in langfristigen Operationen geschädigt werden. Es ließen sich Konflikte anheizen, andere Staaten agitieren.* Gaycken hat sich zum Thema Cyberwar schon bei Technology Review geäußert (24) und jüngst ein Buch dazu veröffentlicht (25).

Aber das Verunstalten von Webseiten ist kein Cyberwar. DDoS-Attacken, auch wenn Banken betroffen sind, sind kein Cyberwar. Das Ausspionieren von Regierungsgeheimnissen oder der Klau von Wirtschaftsgeheimnissen mithilfe von Computern ist kein Cyberwar. Elektronische Kriegsführung ist nicht Cyberwar. Das Verbreiten von halb wahrer oder nicht wahrer Information im Krieg ist kein Cyberwar. Nicht einmal die Sabotage einer Industrieanlage mithilfe von ausgeklügelter Malware ist Cyberwar. (17)

Die Diskussion um die richtigen Begriffe und Definitionen wird noch eine Weile andauern. Sie verbirgt eine Schwäche und gleichzeitig Gefahr: Während die einen - sozusagen die McAfee-Fraktion, der auch ich angehöre - Konflikte und Erscheinungsformen möglicherweise überdramatisieren, wiegeln die anderen - die "Militärs" - eher ab und reden die Probleme klein. Das kann dazu führen, dass die tatsächlichen Gefahren, die schon jetzt von (noch) kriminellen Angriffen ausgehen, unbetrachtet und vor allem unbekämpft bleiben.



Es ist, glaube ich, die Stärke meines Entwicklungsmodells, dass es mehrere Stufungen enthält und Differenzierungen ermöglicht und das auch für den Cyberwar selber (26). Es muss mit Beispielen angereichert werden, um sich als tragfähiges Modell erweisen zu können. Beispiele dafür sind die kurze Geschichte der Cybercrime (27) und die Bestätigungen des Entwicklungsmodells von der Cybercrime (28).

Cisco-Kaskade

▸ CF 04.09.2010

Durch einem Fehler im Cisco-Betriebssystem wurde am 27.08.2010 rund 1 % des Internets lahmgelegt. Das RIPE testete in Zusammenarbeit mit der Duke University das Routing mit erheblich erweiterten BGP-Daten, worauf die unter IOS XR laufenden Router fehlerhafte Daten vermittelten und ihre Gegenstellen die Verbindungen kappten. *Durch die Störung, die nur eine halbe Stunde dauerte, waren ... Netzwerke in über 60 Ländern nicht erreichbar. Zirka 3.500 der rund 330.000 sogenannten Routing-Präfixe sollen betroffen gewesen sein.* (29)

omnipotente Überwachung

▸ CF 29.03.2010

Totalitäre Staaten meinen, die Datenströme des Internets komplett überwachen zu müssen. Stieler protokolliert bei Technology Review den Erfahrungsbericht eines Insiders, der die Schwierigkeiten dabei beschreibt (30). Protokolle müssen nachvollzogen, fehlende Datenpakete rekonstruiert und besonders das Massenproblem bewältigt werden.

(1) ▸ Internet-Reset, CF 01.08.2010
(2) ▸ Internet-Reset. Fazit, CF 01.08.2010
(3) ▸ Österreich bereitet "Kill Switch" für das Internet vor, Heise online 01.02.2011
(4) ▸ Thomas Pany, "Historisch einmaliger Internet-Blackout", Telepolis 01.02.2011
(5) ▸ Horst-Udo Schneyder, Aufstand in Ägypten: 2 Millionen beim „Marsch der Millionen“ in Kairo, Weltexpress 01.02.2011
(6) ▸ Ägypten: Massenproteste gehenweiter, Heise online 01.02.2011
(7) ▸ Rainer Sommer, Anti-Einkesselungs-Netzwerk Sukey bewährt sich, Telepolis 05.02.2011
(8) ▸ Florian Rötzer, "Eure Schwestern und Brüder in der digitalen Welt stehen neben euch auf dem Platz", Telepolis 03.02.2011
(9) ▸ Das Jahr der gezielten Angriffe, CF 20.11.2010
(10) ▸ Peter Zschunke, "Cyberwar" nicht mehr nur Science-Fiction-Szenario, Heise online 02.02.2011
(11) ▸ Peter Nowak, Unterstützer von Berliner Hausprojekt "besetzen" Onlineshops, Telepolis 04.02.2011
(12) Siehe ▸ (8).
(13) ▸ kommerzielles Internet und organisierte Cybercrime, CF 03.11.2010
(14) ▸ Kriegsrecht im Internet, CF 14.09.2010;
▸ Bert Weingarten, [CYBERWAR & CYBER DEFENCE], PAN AMP 09.12.2009
(15) ▸ Paul B. Kurtz, Bericht zum Thema Virtuelle Kriminalität 2009. Virtueller Internetkrieg wird zur Wirklichkeit, McAfee 06.11.2009; siehe auch: ▸ Analysen zum Cyberwar, CF 11.01.2010
(16) ▸ Mafia, Cybercrime und verwachsene Strukturen, CF 20.10.2010; ▸ Dieter Kochheim, Cybercrime und politisch motiviertes Hacking. Über ein Whitepaper von François Paget von den McAfee Labs, 20.10.2010.
(17) ▸ Myriam Dunn Cavelty, So wahrscheinlich wie die Sichtung von E.T., TheEuropean 09.01.2011
(18) ▸ Toralv Dirro, Der heiße Draht, TheEuropean 07.12.2010
(19) Siehe hierzu auch: ▸ Bestätigungen des Entwicklungsmodells von der Cybercrime, CF 21.11.2010
(20) ▸ Manfred Messmer, Die Zeichen stehen auf Cyberwar, TheEuropean 19.12.2010
(21) Siehe auch ▸ Das Ende virtueller (T) Räume, CF 09.12.2010
(22) ▸ Raoul Chiesa, Katz und Maus, TheEuropean 06.12.2010
(23) ▸ Sandro Gaycken, Kabel-Gate, TheEuropean 23.01.2011
(24) ▸ Sandro Gaycken, David Talbot, Aufmarsch im Internet, Technology Review 08.10.2010
(25) Sandro Gaycken, Cyberwar. Das Internet als Kriegsschauplatz, open source press 2011
(26) Ausführlich: ▸ Kochheim, Cyberwar und Abgesang, Newsletter 28.11.2010.
(27) ▸ Eine kurze Geschichte der Cybercrime, CF 03.11.2010
(28) Siehe ▸ (19).
(29) ▸ Cisco-Router legen Internet teilweise lahm, tecchannel 01.09.2010
(30) ▸ Wolfgang Stieler, Mein Job beim Big Brother, Technology Review 29.03.2010

Bedrohungen gegen den Cyberspace

Andere reden über den Cyberwar, wir machen ihn!

▸ CF 06.02.2011

Während hierzulande die Experten noch über die Definition des Cyberwar streiten und darüber womöglich die tatsächlichen Bedrohungen gegen den Cyberspace kleinreden und übersehen (1), geht die Air Force der USA nicht gelassen, aber sehr offen mit dem Thema um. Ihr strategisches LeMay Center entwickelt und veröffentlicht militärische Grundlagen und Strategien (2) und bereits im Herbst 2010 erschienen die Lehren über Cyberspace-Operationen (3). Auf diese Veröffentlichung weist Dan Elliott hin (4) und auf ihn stieß ich Dank einer umfangreichen Cyberwar-Übersichtsseite bei Spiegel online (5).

Die Studie verzichtet auf den sonst üblichen militärischen Schmonsens von der Informationsbeschaffung, Sicherung eigener Informationen und der Verwirrung der Gegner durch falsche Informationen [Informationskrieg, (6)]. Statt dessen widmet sie sich ganz offen den destruktiven Akteuren im Cyberspace und den von ihnen ausgehenden Bedrohungen [S. 11 bis 13; siehe meine Übersetzungen auf den beiden Folgeseiten; (7)].

Die Beteiligten an nationalstaatlichen Bedrohungen sind die, die strenge Cyberwar-Theoretiker tatsächlich als kriegerisch anerkennen. Ihre Akteure sind Soldaten, allenfalls Söldner, Bürgerkrieger und Guerilla-Kämpfer.

Grenzüberschreitende Akteure sind solche, die nach Paget Hacktivismus betreiben und damit meistens politische Ziele verfolgen (8). Daneben stellt die Studie die kriminellen Organisationen und das sind genau die, die ich als Schurkenprovider, Malware-Firmen, Botnetz-Betreiber und Board-Betreiber beschrieben habe (9) und die McAfee Organisierte Internetkriminelle nennt.

Differenzierter geht die Studie mit den Einzelpersonen und kleinen Gruppen um, die Exploits erkunden, hacken und Malware schreiben. Damit sind wir wieder bei der untersten Stufe meines Entwicklungsmodells und der allgemeinen Cybercrime (10). Und genau so geht auch die Studie davon aus, dass Hacktivisten, kriminelle Organisationen und Nationalstaaten auf einzelne Hacker und Programmierer sowie auf Operating Groups (11) und Botnetzbetreiber zurückgreifen können, um ihre eigene Beteiligung zu verschleiern.

Strenge Cyberwar-Verfechter kennen nur die traditionellen und die asymmetrischen Bedrohungen. Erstere betreffen Kriegsziele, die mit verschiedenen Mitteln direkt angegangen werden. Irreguläre Taktiken entstammen der Guerilla und dienen dazu, falsche Aufmerksamkeiten zu schaffen und wichtige Verteidigungskräfte des Gegners ineffektiv zu binden.

Ein weiterer Verdienst der Studie ist es, dass sie die militärische Abhängigkeit von Netzinfrastrukturen und der Informationstechnik als gegeben ansieht und dafür einen - typisch amerikanischen - weiten Begriff von den Kritischen Infrastrukturen voraussetzt (12).

Akteure

nationalstaatliche Bedrohung

Am gefährlichsten ist die nationalstaatliche Bedrohung über den Cyberspace, weil sie Ressourcen und Infrastrukturen sabotieren und blockieren kann. Dazu gehört auch die Spionage, die von Gegnern und traditionellen Verbündeten gegen die USA betrieben wird. Nationalstaaten können solche Operationen selber durchführen oder Dritte damit beauftragen, um ihre Ziele zu erreichen.

Bedrohung durch grenzüberschreitende Akteure

Transnationaler Akteure sind formelle und informelle Organisationen, die nicht an nationalen Grenzen gebunden sind. Diese Akteure verwenden den Cyberspace, um mit ihren Zielgruppen zu kommunizieren, Anhänger zu rekrutieren und Aktionen zu planen, um das Vertrauen in die Regierungen zu destabilisieren und direkte terroristische Aktionen durchführen.

Bedrohung durch kriminelle Organisationen

Je nach dem, wie sie organisiert sind, handeln kriminelle Organisationen im nationalen Rahmen oder grenzüberschreitend. Sie stehlen Informationen zum eigenen Gebrauch oder um sie mit Gewinn zu verkaufen.

Bedrohung durch Einzelpersonen und kleinen Gruppen

Einzelpersonen oder Zusammenschlüsse von ihnen können sich illegale Zugänge zu Netzwerken und Computersystemen verschaffen. Sie sind besser bekannt als "Hacker". Ihre Absichten sind unterschiedlich.

Einige sind friedlich und nur auf der Suche nach Schwachstellen in der Informationstechnik. Manchmal suchen sie den Informationsaustausch mit den Besitzern, aber einige andere haben böswillige Absichten.

Andere Hacker haben politische Motive und nutzen den Cyberspace, um Ihre Botschaften bei ihren Zielgruppen zu verbreiten. Eine andere Art von Hacker sucht nach Ruhm und Ansehen. Sie brechen in gesicherte Systeme ein oder erstellen Malware, um Verwüstungen auf kommerziellen oder Regierungs-Systemen anzustellen.

Malware ist der Kurzname für "malicious software". Hacker können zu Cyberspace-Bedrohungen auch von anderen, zum Beispiel kriminellen Organisationen, eingesetzt werden, um verborgene Operationen gegen besondere Ziele auszuführen, ohne dabei selber in Erscheinung zu treten und die eigene Beteiligung abstreiten zu können.

Methoden

traditionelle Bedrohungen

Traditionelle Bedrohungen sind klassische militärische Konflikte und gehen normalerweise von anderen Staaten aus. Im Cyberspace nehmen solche Bedrohungen möglicherweise wegen des Einsatzes fortschrittlicher Technologien und Methoden ab. Traditionelle Bedrohungen richten sich im allgemeinen gegen die Cyberspace-Funktionen, die unsere Luft-, Land- , Seestreitkräfte und besondere Operationen im Weltraum nutzen. Sie sollen die militärische Handlungsfreiheit der USA einschränken und die Nutzung des Cyberspace verhindern.

irreguläre Bedrohungen

Asymmetrische Bedrohungen nutzen den Cyberspace, um mit unkonventionellen Mitteln traditionelle Vorteile zu erzielen. Diese Bedrohungen könnten sich auch gezielt gegen die US-amerikanischen Cyberspace-Fähigkeiten und gegen Infrastruktur-Einrichtungen richten. So könnten Terroristen den Cyberspace dazu nutzen, um Operationen gegen unsere finanziellen und industriellen Sektoren durchzuführen, während gleichzeitig andere körperliche Angriffe beginnen. Terroristen verwenden den Cyberspace auch, um anonym, ungleichzeitig und ohne Bindung an physische Standorte zu kommunizieren. Sie versuchen, sich mit leicht zugänglichen,

kommerziellen Sicherheitsprodukten und -dienstleistungen der Strafverfolgung in den USA und gegen militärische Operationen zu schützen. Unregelmäßige Bedrohungen durch Kriminelle und von radikalen politischen Akteuren nutzen den Cyberspace zu ihren eigenen Zwecke, um die Regierung, Verbündete oder gesellschaftliche Interessen herauszufordern.

katastrophale Bedrohungen

Katastrophale Bedrohungen betreffen den Erwerb, Besitz und Einsatz von Massenvernichtungswaffen [WMD (13) *] oder von Methoden, die ähnliche Wirkungen haben. WMD-Angriffe sind physische, sich fortbewegende (kinetische) Ereignisse. Sie erfordern profunde Kenntnisse über die Cyber-Strukturen, um in bedeutende Schlüsselsysteme für Systemsteuerungen, zum Beispiel industrielle Prozesssteuerungen wie SCADA* (14), *einzudringen, zu manipulieren oder zu zerstören. Gut geplante Angriffe auf Schlüssel-Knoten in der Cyberspace-Infrastruktur haben das Potenzial, Zusammenbrüche von Netzwerken und kaskadierende Effekte auszulösen, die kritische Infrastrukturen lokal, national oder möglicherweise sogar global beeinträchtigen können. Beispielsweise könnte ein elektromagnetischer Puls weiträumig die Cyberspace-Domäne beschädigen und Operationen in ihr verhindern.*

disruptive Bedrohungen

Disruptive Bedrohungen sind innovative und neue Technologien, die geeignet sind, die Kriegsführung und Abwehr der USA zu behindern oder zu unterlaufen. Globale Forschungen, Investitionen, Entwicklungen und industrielle Prozesse schaffen eine Umgebung, die den technologischen Fortschritten förderlich ist. Das DOD (15) *sollte auf innovative Durchbrüche der Gegner aufgrund der anhaltenden Verbreitung von Cyberspace-Technologien vorbereitet sein.*

natürliche Bedrohungen

Auch natürliche Gefahren können den Cyberspace stören oder beschädigen. Das sind zum Beispiel Überschwemmungen, Wirbelstürme, Sonneneruptionen, Blitze und Tornados. Diese Ereignissen haben oft höchst zerstörerische Wirkungen und die Verteidigung muss besondere Anstrengungen unternehmen, um ihre zentralen Cyberspace-Systeme zu bewahren oder wiederherzustellen. Diese Ereignisse ermöglichen es einem Gegner, die Verschlechterung von Infrastrukturen, die abgelenkte Aufmerksamkeit und die anderweitig gebundenen Ressourcen auszunutzen.

unbeabsichtigte Bedrohungen

Zufällige Bedrohungen sind nicht vorhersehbar und können viele Formen annehmen. Ein Bagger beschädigt das Glasfaserkabel eines Internetknotens, ein Software-Update weist Fehler auf oder neue Viren beeinträchtigen das Funktionieren des Cyberspace. Obwohl grundlegende Untersuchungen zeigen, dass die meisten Unfälle vermieden werden können, und Maßnahmen zur Unfallvermeidung eingeführt sind, sollte mit Unfällen gerechnet werden.

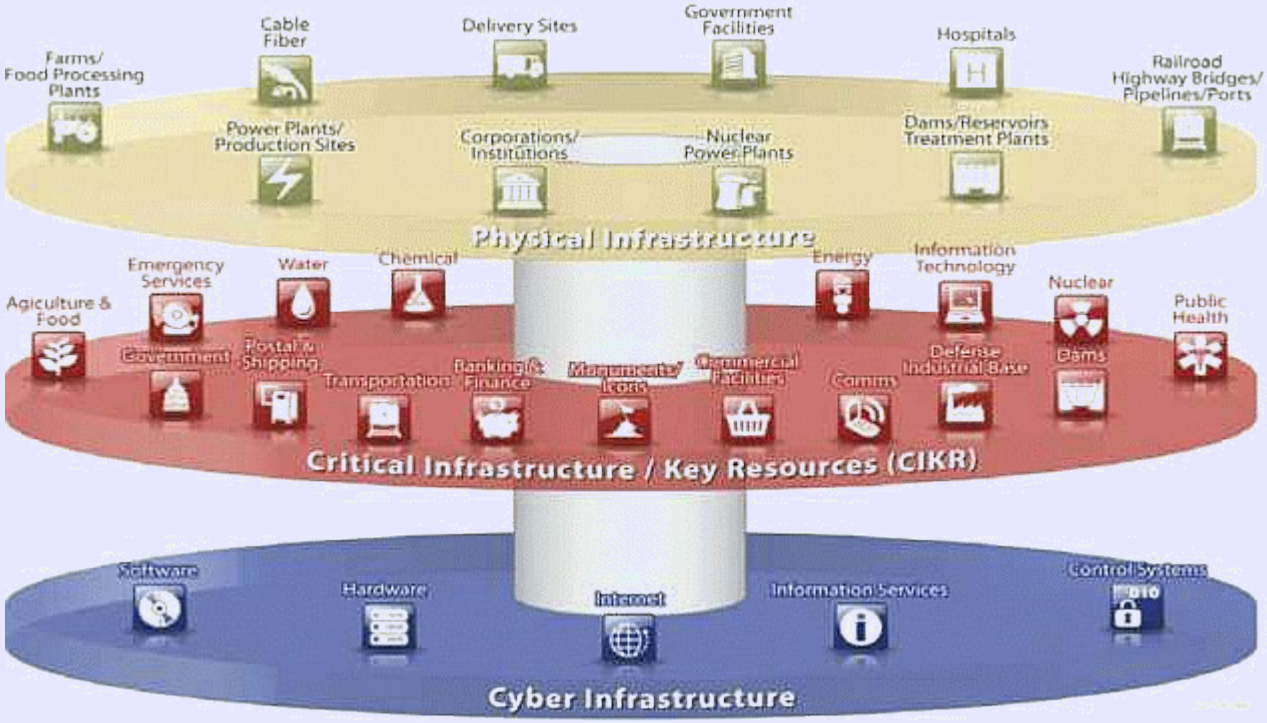
Grundversorgung als Kritische Infrastruktur

▸ CF 06.02.2011

Als Kritische Infrastrukturen betrachtet die Studie alle öffentlichen und gewerblichen Einrichtungen, die der Grundversorgung dienen (16). Davon hebt sie noch einmal die physikalische Infrastruktur ab (oberste Scheibe), auf der neben der landwirtschaftlichen Produktion und Energieversorgung auch der Verkehr (Eisenbahnen, Fernstraßen, Brücken, Pipelines und Häfen), die Kommunikationsnetze, das Transportwesen sowie die Krankenhäuser und staatlichen Verwaltungen angesiedelt sind.

Diese Betrachtung geht recht weit und weicht stark von der deutschen Sichtweise ab. Die hiesige tendiert dazu, nur die oberste Scheibe mit der physikalischen Infrastruktur als kritisch anzusehen.

Wenn man das Gefährdungspotenzial jedoch staffelt und differenziert betrachtet, dann ist amerikanische Sicht durchaus berechtigt. Was nutzen funktionstüchtige Krankenhäuser und Brücken, wenn es keine Rettungsfahrzeuge gibt, die die Kranken oder Verwundeten anliefern?



Hingegen ist es auch äußerst weise, in einem Krisen-, Katastrophen- oder Konfliktfall zu versuchen, das öffentliche Leben weitgehende aufrecht zu erhalten und zu sichern, weil sonst eine neue Front aus unzufriedenen, frierenden oder gar hungernden Bürgern entstehen kann.

Cyberspace und Cyberwar

▸ CF 06.02.2011

Die Studie spricht nicht ausdrücklich vom Cyberwar, sondern nur vom militärischen Umgang mit der Cyberspace-Domain als einem weiteren Einsatzgebiet und Gefechtsfeld, das neben dem Land, Luftraum, Meer und Weltraum zu betrachten ist.

Sie verweist auch auf Naturgefahren und Zufälle sowie auf unvorhergesehene technische Innovationen. Beachtlich finde ich auch, dass sie katastrophalen Bedrohungen durch Massenvernichtungswaffen eine besondere Aufmerksamkeit schenkt.

Ihr offener Umgang mit den Akteuren und den ihnen zuzutrauenden Aktionen ist richtig und verwirrend zugleich. Wenn eine Klimaanlage gehackt worden ist, dann ist es gleichgültig, ob der Angreifer gleich Lebensmittel in einem Kühlhaus vernichtet oder sein Wissen dazu nutzt, einen produzierenden Betrieb zu erpressen. Wenn das Militär auf Straßen, Krankenhäuser und Stromversorgung angewiesen ist, dann sind genau die Gefahren zu beleuchten, die mit ihrem Ausfall verbunden sind. Ob das alles schon Cyberwar ist oder nicht, ist gleichgültig. Niederschwellige Angriffe können nicht nur das öffentliche Leben beeinträchtigen, sondern damit auch die Verteidigungsbereitschaft insgesamt.

Das gilt auch unter strategischen Überlegungen. Ob ein Koordinator ein kriminelles, terroristisches oder militärisches Projekt plant und durchführt, ist zunächst gleichgültig, weil er sich im Zweifel derselben Botnetzbetreiber, Malwareschreiber, Zulieferer und sonstigen Hilfskräften bedient. Für bestimmte Projektziele werden sich Fachleute herausbilden, aber auch die rekrutieren ihre Gehilfen und Handlanger aus ihren sozialen Umfeldern, Internetkontakten und Boards wie alle anderen.

Die Studie gibt der McAfee-Fraktion neue Nahrung und Unterstützung gegenüber den kriegs- und völkerrechtlich ausgerichteten "Militärs". Dennoch mahnt sie auch stillschweigend, mit dem Wort "Cyberwar" etwas zurückhaltender und differenzierter umzugehen. In der Tat muss ich zugeben, dass ein Defacement für sich betrachtet keine kriegerische Aktion ist. Nur ihre Häufungen und ihr Zusammenwirken mit anderen Erscheinungsformen kann als Signal für eine Entwicklung verstanden werden, an deren Ende wirklich zerstörerische und gar tödliche Aktionen stehen.

Das zeigt einmal mehr, dass die analytischen und Gedankenmodelle aus der Militärwissenschaft, der Internet-Sicherheitsforschung und - das darf ich mir anmaßen - der strategischen Kriminalitätsbekämpfung abgeglichen und vereinheitlicht werden sollten. Alle drei Fachgebiete können voneinander lernen, die Erkenntnisse der jeweils anderen nutzen und im Dialog zu neuen Erkenntnissen gelangen. Das wäre dringend nötig. Die Justiz hält sich aber traditionell zurück und wird als Kompetenzpartner natürlich nicht wahrgenommen (17). Da hat es die Polizei leichter, die mit dem Wimpel mit der Aufschrift "Gefahrenabwehr" wedelt.

Erfrischend sind auch die klaren Worte der Studie, die sich vom traditionell gepflegten AbKüFi (18) der Bundeswehr abheben, zum Beispiel im Zusammenhang mit ihren technischen Informationsverarbeitungs- und Kommunikationsprojekten (19). Die Realisierung solcher Projekte mag tatsächlich anspruchsvoll sein, ihre theoretischen und handwerklichen Grundlagen sind das hingegen nicht. Das wird durch abgehobene Sprachungetümer, geheimbündlerischen Parolen, Abkürzungen oder angeblichen Fachbegriffen häufig genug verschleiert und mystifiziert. Das kennen wir auch zur Genüge aus dem IT-Bereich (20).

So entstehen Fachsprachen, die sich der sozialen Abgrenzung wegen bilden und nicht zur präzisen und zweifelsfreien Verständigung. Auch davon müssen wir weg, wie der Streit um den Begriff "Cyberwar" lehrt. Die einen verwenden ihn plakativ, um die aktuelle Bedrohungslage hervorzuheben, und die anderen reden mit ihrer Kritik an der Verwendung des Begriffes die Tatsachen klein, die zu der Bewertung

geführt haben. In der öffentlichen Diskussion sollten wir vielleicht von der Netztechnik lernen: Am Anfang verständigen sich die Komponenten händeschüttelnd (Handshake) über das Protokoll, mit dem sie sich miteinander verständigen wollen (21).

Das gilt zum Beispiel auch für die angeheizte Diskussion über die Vorratsdatenspeicherung ... aber das lassen wir jetzt!

(1) ▸ Streit um den Cyberwar, CF 05.02.2011
(2) ▸ Curtis E. Lemay Center for Doctrine Development and Education
(3) ▸ Air Force Doctrine Document 3-12, Cyberspace Operations, Lemay Center 10.09.2010
(4) ▸ Dan Elliott, US-Luftwaffe gewährt Einblick in Cyberwar-Strategie, Spiegel online 26.10.2010
(5) ▸ Krieg der Staatshacker, Spiegel online
(6) ▸ Informationskrieg, Wikipedia
(7) Es handelt sich um sinngemäße Übersetzungen von mir, die keinen Anspruch auf eine wortgetreue Authentizität erheben.
(8) ▸ Mafia, Cybercrime und verwachsene Strukturen, CF 20.10.2010
(9) ▸ Arbeitspapier Cybercrime, CF 22.08.2010
(10) ▸ Streit um den Cyberwar, CF 05.02.2011
(11) ▸ Operation Groups, CF 13.07.2008
(12) Siehe zuletzt: ▸ Kritische Infrastrukturen, CF 05.02.2011;
▸ gewerbliche Unternehmen als Kritische Infrastrukturen, CF 06.12.2010.
(13) WMD: weapons of mass destruction (Massenvernichtungswaffen)
(14) ▸ Supervisory Control and Data Acquisition, Wikipedia
(15) DOD: Department of Defense (Verteidigungsministerium)
(16) Grafik: ▸ (3), S. 4.
(17) An dem diskutierten Cyber-Abwehrzentrum *sollen unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) der Verfassungsschutz, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* beteiligt werden, nicht aber das BKA und die Justiz:
▸ De Maizière warnt vor "Cyberwar", Heise online 05.02.2011.
▸ Bundesregierung plant Cyber-Abwehrzentrum, Spiegel online 27.12.2010.
(18) AbKüFi: Abkürzungsfimmel
(19) ▸ Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr,
▸ Vorhaben und Projekte
(20) ▸ Zero-Day-Exploits und die heile Hackerwelt, CF 06.11.2010;
▸ Anglizismen ohne Sinn, CF 22.12.2010.
(21) ▸ Datenflusssteuerung, Wikipedia

Eskalationen in der dualen Welt

Die Cybercrime hat es vorgemacht. Zunächst mit Dialern und heute mit Onlinebanking-Malware und Würmern für den Identitätsdiebstahl oder für Botnetze hat sie das digitale Umfeld genutzt, um sehr reale Wirkungen zu erzielen. Gewinn. Ihn kann man in der digitalen Welt bewegen, wie die ▸ grauen Bezahlsysteme beweisen, aber nicht in Gänze für die Befriedigung aller natürlichen Bedürfnisse nutzen. Dazu bedarf es schon der Schnittstellen in der realen Welt, also zum Beispiel der von Paysafecard oder Webmoney gespeisten Kreditkarten auf Guthabenbasis. Mit ihnen kann die Beute am Geldautomaten an der nächsten Ecke realisiert werden.

Die digitale Netzwelt ist zum kommerziellen Marktplatz geworden und die Verlagerung von Geschäftsprozessen jeder Art lässt sich nicht mehr vermeiden.

Das sind die guten Gründe dafür, dass Paget und seine Kollegen bei McAfee davon ausgehen, dass die Erscheinungsformen der Wirtschaftskriminalität, vor allem der Geldwäsche, und der Cybercrime immer weiter zusammenwachsen werden. Der Trend zum Zusammenwachsen kommt aus beiden Richtungen. Die Cyber-Kriminellen entdecken immer häufiger die klassischen Formen der Beutesicherung für sich und in der traditionellen Sparte werden zunehmend die Vorteile der Internetkommunikation und der digitalen Zahlungssysteme erkannt.

Tor und andere Anonymisierer oder Proxy-Server stellen Techniken zur Verfügung, um digitale Kommunikationsbeziehungen zu verschleiern. Ohne sie könnte es Whistleblowing-Plattformen wie WikiLeaks nicht geben. Sie müssen die Wege verschleiern, auf denen ihnen geheime Dokumente zugespielt werden können.

Es ist vorauszusehen, dass die Security-Industrie Gegenstrategien entwickeln wird. Das werden zunächst solche Methoden sein, die McAfee im Zusammenhang mit dem Schutz von Kritischen Infrastrukturen vorgestellt hat, also der Zugriffsschutz. Ihre Alarmsysteme werden künftig auch auf ungewöhnliche Häufungen von Informationsabrufen, Kopien und mobilen Speichern reagieren, um Informationsabflüsse zu erkennen und zu verhindern. Dazu müssen nur die vorhandenen Systeme zur Intrusion-Prevention und Intrusion-Detection angepasst und sensibilisiert werden.

Darüber hinaus kann ich mir vorstellen, dass die schon bekannten Verfahren zur Einrichtung von Wasserzeichen verfeinert werden. Überall dort, wo Dokumente nicht nur Text, sondern auch Format-Kommandos enthalten, lassen sich auch aktive Funktionen einbinden, die Alarm geben können. Sie könnten ihre IT-Umgebungen dazu nutzen, um sich bei ihrem „Herrchen“ bemerkbar zu machen. Soweit zur Zukunftsmusik.

WikiLeaks bekommt die vertraulichen Dokumente nicht vor irgendwelchen Trenchcoatträgern in dunklen Ecken zugespielt, sondern über die Kommunikationsnetze. Das folgt aus seiner Tradition als Plattform, die weltweit Regimekritikern in totalitären Staaten die Veröffentlichung subversiver, peinlicher und auch gefährlicher Informationen ermöglicht.

Die Masse der als geheim angesehenen Informationen, die WikiLeaks 2010 veröffentlicht hat, übertrifft – jedenfalls quantitativ – alles vorher Bekannte. Damit hat sich sein Sprachrohr Assange, ungeachtet aller klebrigen Vorwürfe, die sonst noch im Raum stehen, zum Abschuss freigegeben. Der US-amerikanische Empörungs- und Verteidigungsapparat ist verlässlich und wird WikiLeaks vernichten. Begleitschäden wie der Abschuss von HBGary Federal sind dabei womöglich nur lästig und nicht einmal schmerzhaft.

Schon jetzt ist sicher, dass die Vernichtung von WikiLeaks kein bleibender Erfolg sein wird. Längst haben sich neue Whistleblowing-Plattformen gebildet und ihre Betreiber haben aus dem Fall gelernt. Sie werden mehr technische Sicherungen einbauen, auf schillernde und angreifbare Exzentriker wie Assange verzichten und an seiner Stelle projektbezogene Aushängeschilder auftreten lassen, die gleich wieder aus dem Verkehr gezogen werden. Die unvermeidbare Vernichtung von WikiLeaks wird die Subversion vorantreiben.

Das hat Anonymous bewiesen. Im Gegensatz zum typisch deutschen CCC-Verein, der sich als letzter Fahnenträger der akademischen Hackerkultur und Retter aller Freiheitsrechte versteht, oder der amerikanische Cult of the Dead Cow, der eigentlich lieber ein Motorradclub geworden wäre, ist Anonymous eine modulare Bewegung, die unerwartet ihre Schlagkraft bewiesen hat mit mächtigen DDoS-Angriffen und einer professionellen Hacking-Kompetenz, die alle gängigen Methoden erfolgreich anwendet. Anonymous präsentiert eine zivile Gegenmacht, die sich der Administration und dem kommerziellen Establishment erfolgreich entgegen stellt. Das ist keine kleine verschworene Gruppe, sondern eine weltweite Bewegung mit eigenen politischen und Moralvorstellung, die sich bislang als bemerkenswert stabil herausgestellt hat.

Ob man die WikiLeaks-Veröffentlichungen und die Anonymous-Aktionen vorbehaltlos befürworten kann, ist eine andere Frage. Ich neige bekanntlich zum abwägenden „Ja Aber“. Beide zeigen ungeachtet dessen einen selbstgerechten Freiheitsanspruch, der sich erfrischend von den Heimlichkeiten, Munkeleien und Seilschaften in der Tagespolitik und der Ökonomie im Mainstream abhebt.

Eine institutionelle Selbstgerechtigkeit kennen wir sonst nur aus der Wirtschaft und von ihren Verbänden. Sie stilisieren gelegentlich Software- oder Kunstdiebe zu blutrünstigen Piraten und Verbrechern, kümmern sich um ihr Kerngeschäft und halten sich in gesellschaftlichen und politischen Fragen ganz neutral. Das waren sie nie, weil jedenfalls ihre Verbände mit großem Aufwand Lobby-Politik betreiben.

Das Image als Saubermänner kratzen die Beispiele Stuxnet, Exploit-Händler und das Dreigestirn Berico-HBGary Federal-Palantir nachhaltig an. Wer sind denn die Geldgeber für Stuxnet? Woher stammen das Knowhow über industrielle Steuerungsanlagen und über Exploits, die noch nach drei Jahren völlig unbekannt waren? Woher kommen die Programmiererteams, die für mindestens zwei Jahre angeheuert wurden? Die Analysen der Sicherheitsunternehmen, allen voran Symantec, sprechen dafür, dass sie jedenfalls nicht aus der kriminellen Malwareszene kommen.

Der Cyberspace kennt – für sich betrachtet – keine zwingenden und justiziablen Regeln. Sie und ihre Sanktionen setzen gewöhnlich erst dann ein, wenn die Cyberrealität in die gewohnte Realität schwappt und in ihr Wirkungen hinterlässt. Beide Welten sind inzwischen so stark miteinander verwoben, dass sie sich nicht mehr – weder tatsächlich noch per bemühter Definition – voneinander trennen lassen.

Das bedeutet aber auch, dass wir die materielle und die digitale Welt als eine Einheit ansehen müssen. In der einen mag es abgelegene Bergdörfer ohne Zugang zu Kommunikationsnetzen und in der anderen hochgesicherte und abgeschottete Zirkel geben. Die großen Flächen in beiden sind aber schon heute Schnittflächen, die sich gegenseitig durchdringen.

Diese Erkenntnis hat mehrere Konsequenzen, die ich keineswegs abschließend anreiße:

→ Sicherheit ist unteilbar. Es gibt keine materielle Sicherheit, die von der digitalen unabhängig ist; und umgekehrt.

→ Moral und Recht sind unteilbar. Sie verlangen nach Pflichten und geben Schutz. Auch gegen haltlos spekulierende Cyberkämpfer aus dem Mainstream.

→ Die duale Welt kennt keine Nationalstaaten, keine bezöllnerten Grenzen und keine materiellen Schranken mehr. Ihr digitaler Teil durchdringt sie alle.

→ Grundbedürfnisse können nur in der realen Welt erlebt werden. Essen, Trinken, Abscheiden und Sex funktionieren nur bedingt, wenn man sie virtuell erledigen will. Das ist auch die Schwäche der digitalen Welt: Sie ist ein Parasit an der materiellen Welt, ohne die sie nicht existieren kann.

Wie geht es weiter?

Die Prognosen fallen mir schwerer als in der Vergangenheit, als ich mir eigentlich nur Gedanken über die Entwicklungen in der Cybercrime machen musste. Insoweit bin ich auch nicht unzufrieden, weil ich vieles im Zusammenhang mit der Cybercrime, ihren Organiationsprozessen und Entwicklungslinien entdeckt habe und durch neue Fakten bestätigen konnte.

Die neuen Prozesslinien, die von WikiLeaks, Anonymous und den falschen Saubermännern aus dem Mainstream ausgehen, nehme ich zunächst erst wahr und werde sie verfolgen, ohne schon jetzt erkennen zu können, wohin sie sich entwickeln werden.

Als Paget vor einem Jahr von der zunehmenden Gefahr des Hacktivismus sprach, hatte er nur wenige und eher harmlose Beispiele für das Defacement und die politisch motivierten DDoS-Angriffe zu bieten. Die jüngsten Entwicklungen haben ihm recht gegeben.

Mir geht es ähnlich: Ich habe zunehmend organisierte, nicht monolithische, aber modulare Strukturen in der Cybercrime vorausgesagt. Genau das trifft jetzt auch auf Anonymous zu.

Mangelnde Entrüstung

Es fällt leicht, sich über die Cybercrime zu entrüsten. Bei ihr haben wir auf der einen Seite die auf ihren kriminellen Gewinn bedachten Täter und auf der anderen Seite die Geschädigten. In diesem Bild reichen wenige Grautöne aus, um den Zwischenbereich zu zeichnen.

Beim Whistleblowing und beim Hacktivismus, bei den Gegenmaßnahmen aus der US-Verwaltung, den eingebundenen Unternehmen und schließlich den IT-Söldnern ist das schwieriger.

→ Kriminelle, Hacker und IT-Söldner nutzen dieselben Methoden, um ihre Ziele zu erreichen. Ob sie hacken, Malware einsetzen oder Social Engineering, sie unterscheiden sich nur wegen der Motive der Handelnden.

→ Die Motive der Verwaltungsleute und der IT-Söldner können für sich beanspruchen, auf böswillige Gefahren zu reagieren. Die Lehren aus dem letzten Golfkrieg und die Reaktionen auf den 11. September 2001 gebieten Vorsicht. Sie sind zu häufig aufgebauscht und mit falschen Informationen unterfüttert gewesen. Eine nüchterne Analyse ist gefordert.

→ Zu häufig sind gerade die, die sich im Recht der Entrüstung glauben, mit ihren Forderungen und Reaktionen weit über das Ziel hinaus geschossen. Säbelgerassel kennt keine Verhältnismäßigkeit.

→ Das gilt gleichermaßen für die Hacktivismus-Szene. DDoS und gezieltes Hacking sind keine einfachen Regelverstöße, sondern kriminelle Handlungen. Für sie mag es vereinzelt Rechtfertigungen geben, die im Ausnahmefall bis zur Notwehr, zur Nothilfe oder zur Wahrnehmung berechtigter Interessen reichen. Das kann ihre kriminelle Natur aber nicht ausräumen.

→ WikiLeaks und andere Whistleblower können für sich die Meinungs- und Pressefreiheit sowie die Forderung nach Informationsfreiheit in Anspruch nehmen. Auch diese Rechte sind nicht grenzenlos. Allein die Masse der von WikiLeaks veröffentlichten Dokumente spricht gegen eine verantwortungsvolle Auswahl und Bewertung.

→ Auch die kommerzielle IT-Branche hat ihre schwarzen Schafe. Ohne kriminelle Regelverstöße wie die von Anonymous kämen sie kaum ans Tageslicht.

Man mag mir widersprüchliches Verhalten vorwerfen, wenn ich einerseits die kriminelle Natur einer Methode benenne und andererseits ihre Früchte dennoch verwerte. Stimmt! Damit handele ich genau so wie die Finanzverwaltung und Strafverfolgung, die geklaute Daten über Steuersünder aus der Schweiz und aus Liechtenstein verwerten.

Dieter Kochheim, 19.02.2011