Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

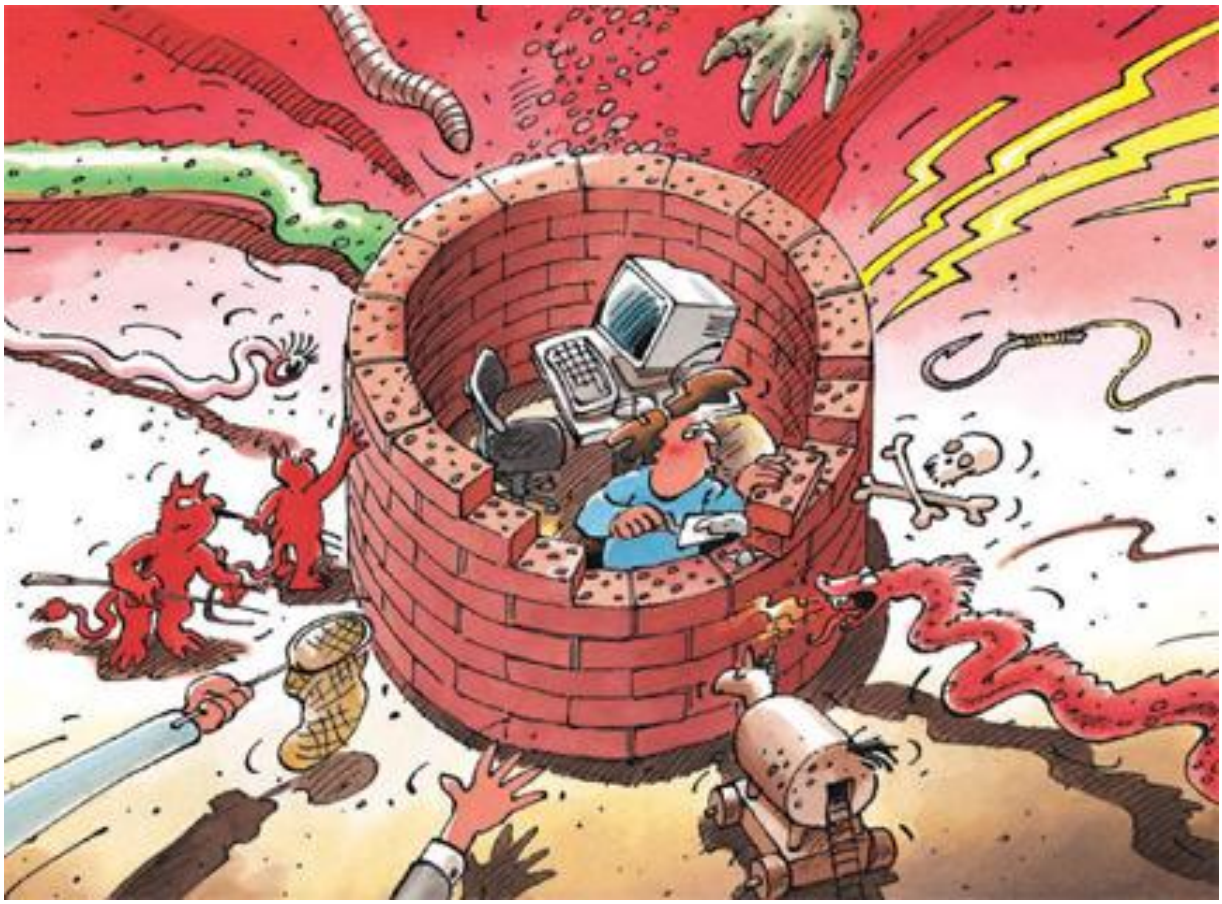
Informatikstrategieorgan Bund ISB
Dienst für Analyse und Prävention DAP

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2008/II (Juli – Dezember)



In Zusammenarbeit mit:

KOBIK
SCOCI
CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

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

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

The Swiss Coordination Unit for Cybercrime Control

Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2008/II 3

2 Einleitung 4

3 Aktuelle Lage IKT-Infrastruktur national 5

3.1 E-Banking-Trojaner – Weiterhin Verbreitung auf diversen Kanälen 5

3.2 Problematik der Botnetze 6

3.3 Gefälschte E-Mail mit Selbstmorddrohung versendet 7

3.4 Missbrauch von FTP-Konten 7

3.5 Finanzagenten verurteilt 8

3.6 Verschiedene Phishing-Angriffe gegen Schweizer Internetdienste 10

3.7 Verschiedene Angriffe auf Webserver 11

3.8 Revision Urheberrechtsgesetz in Kraft getreten 12

3.9 Pornoverbot auf Mobiltelefonen vom Parlament verabschiedet 13

3.10 Internet-Plattform für Pädophilie aufgedeckt 13

3.11 Verschiedene Sperren bei Grossfirmen 14

4 Aktuelle Lage IKT-Infrastruktur international 14

4.1 USA: Militär verbietet die Nutzung mobiler Speicher 14

4.2 Erfolge gegen Cyberkriminelle 16

4.3 Deutschland: Grosser Datendiebstahl bei der Telekom 16

4.4 EU: Plan zu einer umfassenden und gemeinsamen Bekämpfung der Internetkriminalität beschlossen 17

4.5 Deutschland: Vorratsdatenspeicherung auch für Internetprovider 17

4.6 Deutschland: Revidiertes BKA-Gesetz tritt in Kraft 18

4.7 Grossbritannien: Neues Cybercrime-Gesetz tritt in Kraft 18

5 Tendenzen / Ausblick 18

5.1 Allgemeine Entwicklung Cybercrime 18

5.2 Neue «Geschäftsmodelle» und «Services» verleihen der Cyberkriminalität 2009 neuen Schub 19

5.3 Umgang mit Datenmüll der Informationsgesellschaft 22

5.4 Zugangsdaten zu Internetdiensten zukünftig vermehrt im Visier der Cyberkriminellen 22

6 Glossar 23

7 Anhang 27

7.1 Endgültiges Löschen von Daten auf Datenträgern 27

7.2 Abschalten der AutoRun Funktion in Windows 30

7.3 Die Lücken in DNS und MD5 35

7.4 Providerdienste: Nach McColo weht der Wind von Osten 36

1 Schwerpunkte Ausgabe 2008/II

- **E-Banking-Trojaner – Weiterhin Verbreitung auf diversen Kanälen**
  Auch im zweiten Halbjahr 2008 gingen die Versuche, Schadsoftware gegen E-Banking zu verbreiten, weiter. Zu Beginn des Halbjahres wurden wiederum diverse Spam-Wellen beobachtet. Daneben wurde aber vermehrt auf Verbreitung via Drive-by-Infektionen, also die Infektion beim alleinigen Ansurfen einer Webseite ohne Benutzerinteraktion, gesetzt. Zudem tauchte am Ende des Halbjahres in der Schweiz eine neue E-Banking-Trojanerfamilie auf.
  ► Aktuelle Lage Schweiz: Kapitel 3.1

- **Finanzagenten verurteilt**
  Im letzten Jahr wurden einige Urteile gegen Finanzagenten gefällt. Das Bezirksgericht Zürich hat einen Finanzagenten wegen Geldwäscherei zu einer Strafe von 30 Tagessätzen und einer Busse von 500 Franken verurteilt. Zudem sprach das Gericht dem Geschädigten einen Schadensersatz in voller Höhe zu. In einem anderen Fall wurde der Beschuldigte zu einer Geldstrafe von 150 Tagessätzen und eine Busse von 1000 Franken verurteilt. Auch hier kommen Schadensersatzforderungen und Gerichtskosten dazu.
  ► Aktuelle Lage Schweiz: Kapitel 3.5

- **Verschiedenene Phishing-Angriffe gegen Schweizer Internetdienste**
  Letztes Jahr wurden verschiedene klassische Phishing-Versuche gegen Schweizer Dienstleister beobachtet. Beim Phishing sollen E-Mails mit gefälschtem Absender und Link das Opfer auf eine gefälschte Webseite locken sollen, damit es dort seine Logindaten eingibt. Allerdings ist der Anteil der Phishing-Versuche gegen Finanzdienstleister verschwindend klein. Eine Zunahme gab es bei Phishing-Versuchen gegen Auktionsdienstleister oder Inserateplattformen.
  ► Aktuelle Lage Schweiz: Kapitel 3.6

- **Angriffsvektor USB-Stick**
  Im November 2008 beschloss das US Strategic Command, dass Angehörigen der US Armee die Nutzung mobiler Speicher bis auf weiteres untersagt sei. Auslöser dafür war die rasche Ausbreitung eines Virus, welcher sich von mobilen Datenträgern auf angeschlossene Systeme kopierte. Auch der Wurm Conficker nutzte den USB-Stick als Verbreitungsvektor.
  ► Kapitel 4.1 und der Anhang (Kapitel 7.2) gibt Tipps im Umgang mit mobilen Speichermedien.

- **Umgang mit «Datenmüll» der Informationsgesellschaft**
  Heute befindet sich praktisch in jedem elektronischen Gerät eine Speicherkarte. Dadurch nehmen die unbewusst gespeicherten Daten stark zu, welche jede Person anhäuft. Das korrekte Löschen von Daten, wenn beispielsweise die Kamera, das Handy oder der USB-Stick den Besitzer wechselt, ist deshalb sehr wichtig. Im Anhang finden Sie wertvolle Tipps.
  ► Tendenzen, siehe Ausblick: Kapitel 5.3
  ► Anhang: Kapitel 7.1

2 Einleitung

Der achte Halbjahresbericht (Juli – Dezember 2008) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet einen Schwerpunkt im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

Gegenüber den letzten Berichten wurde die Kapitelstruktur vereinfacht. Sie besteht neu aus den Hauptkapiteln «aktuelle Lage national» und «international». Die bisherigen Kapitel über neue Gesetze, private, staatliche Aktivitäten, Studien und Statistiken zu IKT-Themen wurden in diese Kapitel integriert.

Ausgewählte Themen dieses Halbjahresberichtes sind in **Kapitel 1** angerissen.

Kapitel 3 und 4 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der zweiten Hälfte des Jahres 2008 aufgezeigt.

Kapitel 5 enthält Tendenzen und einen Ausblick auf zu erwartende Entwicklungen.

Kapitel 7 ist ein Anhang mit erweiterten technischen Erläuterungen und Anleitungen zu ausgewählten Themen des Halbjahresberichtes.

3 Aktuelle Lage IKT-Infrastruktur national

3.1 E-Banking-Trojaner – Weiterhin Verbreitung auf diversen Kanälen

Auch im zweiten Halbjahr 2008 gingen die Versuche, *Schadsoftware (Trojaner)* gegen E-Banking Kunden zu verbreiten, weiter. Die Angreifer versuchten, entweder durch Spam-Mails oder infizierten Webseiten (Drive-by) diese Trojaner zu verbreiten. MELANI hat gegen Ende des Jahres ganz klar eine Verlagerung von Spam auf Drive-by-Infektionen festgestellt.

Das Halbjahr begann mit diversen E-Mail-Wellen (mit dem Trojaner Namens WSNPoem), die das Opfer dazu verleiteten, auf einen Anhang zu klicken. Dabei waren vor allem jene E-Mails im Umlauf, welche vorgaben, dass ein Paket der Firma UPS nicht geliefert werden konnte. Man solle die Rechnung im angehängten Dokument ausdrucken, um das Paket abzuholen. Allerdings handelte es sich bei diesem Dokument im Anhang nicht um die erwartete PDF-Datei, sondern um eine ausführbare exe-Datei. Diese E-Mails waren sowohl in deutscher als auch in französischer Sprache verfasst, was darauf hindeutet, dass mittlerweile ein Grossteil der Schweiz im Visier von Cyberkriminellen ist.

"UPS colis postal"

"Bon matin,
malheureusement, nous avons manque de livrer le pli (votre colis postal), que vous avez envoyé le 1er juillet, parce que ladresse du Destinataire nexiste pas.
S'il vous plait, imprimez la facture envoyee en fichier joint a ce message, et venez chercher le pli a notre office a ladresse indiquee a la facture.
Consultant Esther Jennings,
UPS"

Beispiel einer französischsprachigen Spam-E-Mail mit einem Trojaner im Anhang

Am 28. August 2008 kam dann die vorerst letzte Welle dieser Trojanerfamilie, dieses Mal getarnt als Flugticket:

"Your Online Flight Ticket N 12557"

"Good morning,
Thank you for using our new service "Buy flight ticket Online" on our website.
Your account has been created:
Your login: xxxxx@xxxxxx.ch
Your password: passNFEC
Your credit card has been charged for $641.68.
We would like to remind you that whenever you order tickets on our website you get a discount of 10%!
Attached to this message is the purchase Invoice and the airplane ticket.
To use your ticket, simply print it on a color printed, and you are set to take off for the journey!
Kind regards,
Spirit Airlines"

Beispiel einer englischsprachigen Spam-E-Mail mit einem Trojaner im Anhang

Danach hörten die E-Mail-Wellen mit einen Schlag auf. Wie die holländische Staatsanwaltschaft zwei Monate später mitteilte, war exakt zu dieser Zeit ein erfolgreicher Schlag gegen E-Banking-Betrüger gelungen, bei der drei Personen verhaftet wurden. Die Vermutung liegt Nahe, dass es sich bei den Verhafteten um einen Teil der Verantwortlichen der oben genannten Angriffen gehandelt haben könnte. Weitere Informationen zu dieser Verhaftung sind in Kapitel 4.2 aufgeführt.

Im Dezember versuchten Cyberkriminelle, mit der neuen Trojanerfamilie Gozi alias Infostealer.Snifula in der Schweiz Fuss zu fassen. Mit einer Spam-E-Mail zweideutigen Inhalts[1] wurde versucht, potentielle Opfer auf verschiedene präparierte pornografische Internetseiten zu locken. In den Domänennamen dieser Seiten war dabei meist das Wort «Switzerland» enthalten, was zeigt, dass die Welle speziell auf die Schweiz ausgerichtet war. Auf der Internetseite wurde der Benutzer dann aufgefordert, ein so genanntes *Flash Plug-In* herunterzuladen und zu installieren, um die visuellen Inhalte auf der Internetseite betrachten zu können. Dahinter versteckte sich der E-Banking-Trojaner.

Die Verbreitung von Trojanern durch Drive-by-Infektionen nahm 2008 weiter zu. Dabei reicht es, dass das Opfer eine Website ansurft (Drive-by). Damit ist der Computer infiziert.
Um den Schadcode auf die Website zu laden, brauchen die Cyberkriminellen die dazu nötigen FTP-Konten. Diese besorgen sie sich durch Hacken und zwar in grossem Stil, wie die Ausführungen in Kapitel 3.4 zeigen.

Computerbenutzer sollten Verhaltensregeln im Umgang mit E-Mails sowie beim Surfen im Internet befolgen: Sie sollten Ihr Betriebssystem und die Applikationen auf dem aktuellen Stand halten sowie aktuelle Antiviren- und *Firewall*-Software einsetzen (siehe dazu die Empfehlungen auf der MELANI-Homepage).[2] Zudem hilft die Einschränkung von *ActiveX*, respektive *Javascript* sich vor Drive-by-Infektionen zu schützen. Schränken Sie die Ausführung von ActiveX Controls mittels Browsereinstellungen soweit als möglich ein. Verändern Sie die Sicherheitseinstellungen des Internet Explorers auf die Stufe «Hoch». Wie dies umgesetzt werden kann, ist auf Seite 5 und 6 der Anleitung «Sicherheitseinstellungen für Windows XP»[3] Schritt für Schritt erläutert. Für den Browser Firefox gibt es das Programm Noscript[4], mit welchem man Javascript für jede Internetseite individuell einschränken kann.

Unregelmässigkeiten bei der E-Banking-Sitzung sollten dem entsprechenden Institut umgehend gemeldet werden. Besondere Anzeichen sind dabei ein zweifacher Login-Prozess, eine plötzliche, von der Bank nicht kommunizierte Änderung des Login-Ablaufes oder der Abbruch nach der Eingabe der gesamten Login-Information.

3.2 Problematik der Botnetze

Bei Botnetzen handelt es sich um eine Ansammlung von Computern, die mit Schadsoftware infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Der amerikanische Provider McColo (Kapitel 7.4) beherbergte im letzten Jahr eine beachtliche Menge an *Command & Control Server*infrastruktur von grossen Botnetzwerken, weshalb er vorübergehend vom Internet getrennt wurde. Dies hatte auch Auswirkungen auf die Schweiz: ein Teil der E-Banking-Schadsoftware konnte nicht mehr weiter verbreitet werden.

[1] http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=de (Stand: 02.02.2009).
[2] Siehe: http://www.melani.admin.ch/themen/00166/index.html?lang=de (Stand: 02.02.2009).
[3] Anleitung auf http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=de (Stand: 02.02.2009).
[4] Addon Noscript für Mozilla Firefox https://addons.mozilla.org/de/firefox/addon/722 (Stand: 02.02.2009).

3.3 Gefälschte E-Mail mit Selbstmorddrohung versendet

In der Nacht auf den 5. August 2008 sind über 100'000 Spam-E-Mails an Schweizer E-Mail-Adressen versendet worden. Darin drohte ein junger Informatiker, seine Freundin, deren Liebhaber sowie sich selbst umzubringen. Besorgte Bürger, die diese E-Mail erhalten hatten, meldeten sich anschliessend bei der Kantonspolizei Zürich, welche den angeblichen Selbstmörder um zwei Uhr nachts aus dem Bett holte. Bei der E-Mail handelte es sich um eine Fälschung, die Drohung war nicht echt. Unter dem in der E-Mail angegebenen Link wurde auch keine Malware verteilt.

Nach Einschätzung der Melde- und Analysestelle Informationssicherung (MELANI) handelte es sich hier um eine relativ grossangelegte Racheattacke von Internetkriminellen gegen denjenigen Informatiker, der seit längerer Zeit Einzelheiten über E-Banking-Schadsoftware auf seiner Webseite abuse.ch publiziert. Dieser hatte kurz davor ein detailliertes Dokument veröffentlicht, das Zusammenhänge der Informatik-Infrastruktur der Täterschaft aufzeigte, welche auch für die E-Banking-Angriffe gegen Schweizer Finanzinstitute verantwortlich ist. Diese Veröffentlichung brachte wahrscheinlich das Fass zum Überlaufen und bewog die Täter, Gegenmassnahmen zu ergreifen. Die Einschüchterungsaktion begann mit einem grossen *Denial of Service*-Angriff auf die Webseite abuse.ch und wurde mit dem Versenden der besagten E-Mail weitergeführt.

In vielen Fällen wird die Internetkriminalität noch oft als eine rein virtuelle, unfassbare Sache oder aber als Lausbubenspielchen ein paar weniger Computercracks verstanden. Wie schon in den letzten Halbjahresberichten darauf hingewiesen, ist dem in keinster Art und Weise mehr so. Internetkriminalität wird von gut organisierten, teilweise über den ganzen Globus verstreuten Gruppierungen ausgeführt, welche alle klar den finanziellen Schnellgewinn im Auge habe. Dabei spielen auch in diesem kriminellen Umfeld der Markt und der Konkurrenzkampf: Die Angreifer vertiefen sich so lange in ein bestimmtes Geschäftsmodell, so lange Aufwand und Ertrag, Risiko und Gewinn noch stimmen. Im Falle der Vergeltungsmassnahme gegen den Schweizer Informatiker ging es den Angreifern ganz offensichtlich darum diesen Faktor, der sich nachteilig auf ihr Geschäft auswirkte, zu beseitigen.

3.4 Missbrauch von FTP-Konten

Die israelische Sicherheitsfirma Aladdin entdeckte im zweiten Halbjahr 2008 einen Server, auf dem sich über 200'000 FTP-Zugangsdaten zu öffentlichen Webservern befanden.

Inhaber einer Website benutzen in der Regel ein FTP-Konto bei einem Hosting-Provider, um Daten auf einen Webserver zu laden. 82'000 der durch diese Konten administrierten Webseiten waren bereits mit Malware infiziert worden. Zu den infizierten Websites gehörten auch solche von Rüstungsunternehmen, dem US Postal Service, verschiedenen Universitäten und Regierungen.

MELANI wurde über die betroffenen Schweizer Webseiten informiert: Die Angreifer waren im Besitz von insgesamt mehr als 3'000 Schweizer FTP-Benutzerkonten[5]. Auf über 130 Websites wurde ein unrechtmässiger Zugriff festgestellt. Die Angreifer platzierten auf diesen Webseiten eine sogenannte «Drive-by-Infektion», welche allein durch das Besuchen der Website

5 http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Windows&articleId=9116138&taxonomyId=125&pageNumber=1

eine Malware-Infektion des PCs ermöglicht. Dabei wurden vor allem Trojaner mit dem Ziel E-Banking-Sitzungen zu kompromittieren verbreitet. FTP-Daten kann man auf verschiedene Art und Weise sammeln: mit Hilfe von Malware - «Keylogger» genannt - die auf dem PC der Webadministratoren installiert werden, anhand der Beobachtung des Datenverkehrs zwischen Client und Server oder durch eine Sicherheitslücke beim Hosting-Provider. Das FTP-Protokoll weist viele Vorteile, aber auch einige Nachteile auf: Unter anderem die Tatsache, dass der Datenverkehr unverschlüsselt übermittelt wird und die Zugriffscodes infolgedessen abgefangen werden können.

Auch die Stiftung SWITCH, welche die Domänen «.ch» verwaltet, wurde informiert. Die Angaben wurden danach verschiedenen Providern zur Kenntnis gebracht. MELANI kontaktierte direkt die Inhaber der am meisten gefährdeten Websites, um die Gefahr so rasch wie möglich zu bannen.

Auf dieselbe Art wie der Firma Aladdin gelang es dem Betreiber des Swiss Security Blogs «abuse.ch», Ende 2008 einen Server zu entdecken, auf dem ungefähr 100 000 FTP-Konten abgespeichert worden waren. Diese Daten wurden anschliessend MELANI zugespielt, welche nach eingehender Analyse die Kontoinhaber über die zuständigen Hosting-Provider in der Schweiz oder über die zuständigen Stellen im Ausland verständigte.

3.5 Finanzagenten verurteilt

Immer wieder tauchen in der Schweiz E-Mails auf, welche für offene Stellen werben und grosse Gewinne versprechen. Dahinter stehen in der Regel Banden, welche mit Hilfe ahnungsloser Bürger, Gelder aus illegalen Geschäften transferieren wollen.

Dear Sir/Madam,

We're glad to offer you a position in our company Donation Europe. We are a charity organization in Central Europe. We help and support the community in Europe to help children of all ages. Donation Europe is an organization which supported by donations.

All information about us you can read at our website
You can earn money and help children with us. We are looking for freelance representatives in EUROPEAN COUNTRIES. Donation Europe receive donations in Europe, you have a possibility to become a Freelance representative? of our company. You do not need any funds to work and you do not need to find anybody. We hire people for freelance work. You can combine it with your full-time work, 2-3 hours a day are required from you. The salary is 450 - 2500 EUR per week. We have special offer for COMPANIES also. If you have an interest to our proposition and have a desire to help children send your reply to [e-mail at Yahoo]. Our manager will send you more information about the job and the terms of employment.

PLEASE REPLY TO [e-mail Yahoo] ONLY

Renee Johnson
Donation Europe.
Poland
Nowoursynowska st. 119,
02-776 Warsaw
Charity Registration No.: 101682
Company Registration No.: 2350841

Anwerbe-E-Mail der fiktiven Spenden-Organisation «Donation Europe», welches in grosser Zahl auch an Schweizer Bürger versandt worden ist.

Wer auf ein solches Angebot reagiert, erhält in der Regel innerhalb kurzer Zeit einen Geldbetrag auf sein Konto überwiesen. Nach Abzug einer Provision muss dieser Betrag dann, meist über die Geldtransfer-Firmen «*Western-Union*» oder «*Moneygram*», ins Ausland überwiesen werden. Die Gelder stammen immer aus illegalen Geschäften. Die Anbieter solcher Jobs nutzen ahnungslose Personen aus, um durch Betrug erwirtschaftetes Geld aus Onlinekanälen ins Ausland zu transferieren. Wer an solchen «Geschäften» und Transaktionen mitwirkt,

riskiert ein Strafverfahren wegen Geldwäscherei (Art. 305bis StGB). Nun wurden erste Gerichtsurteile gegen Schweizer *Finanzagenten* gefällt. Die zentrale Frage dabei ist, ob jeweils mit Vorsatz oder mit Eventualvorsatz gehandelt wurde und demzufolge der Tatbestand der Geldwäscherei auch in subjektiver Hinsicht erfüllt wurde. Eine bekannte Website, durch die im grossen Stil Finanzagenten in ganz Europa rekrutiert wurden, war «Donation Europe». Hierbei wurde den potentiellen Geldwäschern vorgegaukelt, dass sie Spendengelder via Moneygram nach Russland und in die Ukraine verschieben sollten. Die Gelder stammten aber in Wirklichkeit nicht von Spendern, sondern von E-Banking-Betrügereien.

«Donation Europe». Fiktive Spendenorganisation mit dem Ziel, Phishing-Gelder nach Russland und in die Ukraine zu transferieren.

Die Webseite (siehe Bild) machte in der Tat einen professionellen Eindruck. Ein Angeklagter, welcher sich auf ein solches Jobangebot gemeldet hatte, bestätigte, dass er die Homepage der Organisation «Donation Europe» angeschaut und diese seriös gewirkt habe. Trotzdem musste er den Vorwurf akzeptieren, dass er naiv gehandelt habe.[6] Der Angeklagte gab in der Untersuchung zu, dass er die Art und Weise, wie die Spenden gemacht wurden, schon als etwas merkwürdig empfunden habe. Dass er die Gelder per MoneyGram habe überweisen müssen, habe seine Zweifel noch gesteigert. Er habe telefonisch nachgefragt, weshalb das Geld nur über MoneyGram überwiesen werden solle. Er habe recherchiert und herausgefunden, dass MoneyGram - im Gegensatz zu anderen Geldtransferfirmen - weniger streng prüft, woher das zu überweisende Geld stammt. Das Gericht seinerseits begründete dann auch, dass es völlig unüblich sei, dass eine Hilfsorganisation ihre Spender auffordere, die Spenden auf das Konto einer fremden, der Hilfsorganisation nicht näher bekannten Person, einzuzahlen. Der Angeklagte hätte bereits aus diesem Grunde Zweifel haben müssen, dass es sich bei «Donation Europe» um eine seriöse Organisation handelte. Erst recht misstrauisch hätte ihn stimmen müssen, dass er für die Geldtransfers, die er für «Donation Europe»

[6] https://www.a-i3.org/content/view/1535/130/ (Stand: 02.02.2009).

auszuführen hatte, eine Provision von 10 Prozent der überwiesenen Geldbeträge für sich behalten durfte. Eine Provision in dieser Höhe steht nämlich in keinem Verhältnis zum geringen Arbeitsaufwand. Das Gericht kam zum Schluss, dass der Angeklagte an die Möglichkeit gedacht haben musste, dass es sich nicht um eine Hilfsorganisation, sondern um eine Organisation handelte, die kriminell erlangtes Geld über Finanzagenten verschiebe. Damit ist klar, dass der Angeklagte den Tatbestand der Geldwäscherei auch in subjektiver Hinsicht erfüllt hatte.
Dies sehen auch andere Gerichte so und haben ihre Urteile in ähnlicher Richtung gefällt. Das Bezirksgericht Zürich hat einen Finanzagenten wegen Geldwäscherei zu einer Strafe von 30 Tagessätzen verurteilt. Zudem sprach das Gericht der geschädigten Person einen Schadensersatz in voller Höhe zu. In einem anderen Fall hat das Bezirksgericht Arbon einen Finanzagenten zu einer Geldstrafe von 150 Tagessätzen und einer Busse von 1000 Franken verurteilt. Auch hier kommen Schadensersatzforderungen und Gerichtskosten dazu.

Die Urteile, die bis jetzt gefällt worden sind, zeigen deutlich, dass es sich hierbei keineswegs um Bagatelldelikte handelt. Auch wenn die Beschuldigten jeweils vorgegeben haben, nicht bemerkt zu haben, dass es sich um Geldwäscherei gehandelt hat. Angesichts der vielen Fragezeichen und Ungereimtheiten, die solche Jobangebote besitzen, muss der angeworbene Finanzagent früher oder später notgedrungen Verdacht schöpfen. Verdachtsmomente, wie beispielsweise der ungerechtfertigte Verdienst, sind genügend vorhanden. Überweist er den Betrag trotzdem, ist ein Vorsatz gegeben und eine Verurteilung die Folge. Naivität schützt in diesen Fällen vor Strafe nicht. Können die Gelder, die der Finanzagent überwiesen hat, nicht zurückgeholt werden, was nur selten der Fall ist, muss der Finanzagent ausserdem mit Schadensersatzforderungen in der Höhe von mehreren 10'000 Franken rechnen. In jedem Fall sind Angebote, welche Aussicht auf grosse Gewinne machen, mit Vorsicht zu geniessen. Eigene Bankkonten sollten nie Dritten zur Verfügung gestellt werden. Bei Verdacht auf Betrug oder Geldwäscherei sind die Behörden (lokale Polizeidienststelle oder die Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK) zu benachrichtigen.

3.6 Verschiedene Phishing-Angriffe gegen Schweizer Internetdienste

Letztes Jahr wurden verschiedene klassische *Phishing*-Versuche gegen Schweizer Internet-Dienstleister beobachtet. Phishing bedeutet das Versenden von E-Mails mit gefälschtem Absender und Link, welcher das Opfer auf eine gefälschte Webseite locken soll, um dort seine Logindaten einzugeben. Allerdings ist der Anteil der Phishing-Versuche gegen Finanzdienstleister verschwindend klein. Daneben gab es aber Phishing-Versuche gegen Auktionsdienstleister wie beispielsweise Ricardo[7] oder Inserateplattformen wie Autoscout24[8].
Im Falle von Autoscout24 haben Cyberkriminelle die Zugangsdaten dazu verwendet, Inserate von vertrauenswürdigen Autohändlern so zu manipulieren, dass ein Auto, das zuvor für 120'000 Franken angeboten worden war, plötzlich für nur 44'000 Franken zu haben war. Die Hacker hatten den Preis nach unten korrigiert. Bei diesem Schnäppchen mussten die potentiellen Opfer zuschlagen. Den kaufwilligen Autoscout24-Nutzern antworteten die Betrüger per E-Mail, dass sich die Autos in London befänden und dass zuerst die Kaufsumme oder eine Anzahlung auf ein ausländisches Konto einbezahlt werden müsse. In Tat und Wahrheit sahen die betrogenen Autokäufer das Fahrzeug jedoch nie.

[7] http://www.online-betrug.ch/?p=105 (Stand: 02.02.2009).
[8] http://www.tagesanzeiger.ch/digital/internet/story/19938467 (Stand: 02.02.2009).

Auch Provider stehen im Visier von Phishing-Betrügern. So warnte beispielsweise der Hosting-Provider Genotec im Oktober vor einer Phishing-Welle gegen die eigenen Kunden[9]. Die Motivation der Cyberkriminellen dürfte hier klar sein. Sie wollten die Kontrolle von möglichst vielen Webseiten erlangen um dort ihre eigenen Inhalte, wie beispielsweise Trojaner oder Kinderpornographische Seiten, zu hosten. Auch Bluewin-Kunden standen im Visier der Cyberkriminellen. Hier wurde versucht, die Zugriffsdaten von Bluewin-Mail zu erlangen. Mit diesen Angaben können beispielsweise die Daten aus Adressbüchern übernommen werden oder Spam-E-Mails versendet werden.

De : webmail.bluewin.ch <Suport@bluewin.ch> Date : 9 décembre 2008 10:53:21 GMT+01:00 À :
Objet : Confirm your

Dear bluewin.ch Subscriber,
To complete your bluewin.ch Account, you must reply to this email immediately and enter your password here (*********) Failure to do this will immediately render your email address deactivated from our database.

You can also confirm your email address by logging into your bluewin.ch Account at https://webmail.bluewin.ch
Thank you for using bluewin.ch!
THE bluewin.ch TEAM SUPPORT

Beispiel eines Phishing-E-Mails gegen Bluewin.ch

Die Uni Zürich[10] und Uni Basel[11] waren ebenfalls von Phishing-Attacken betroffen. Dabei wurde versucht, die Studenten zur Herausgabe der E-Mail Logindaten, respektive Uni-Logindaten zu bewegen, was in einigen Fällen auch gelang. Danach wurden E-Mail Accounts für Spam-Angriffe oder sonstige Betrügereien missbraucht. Die Folge war, dass die E-Mail Adressen beider Institute in die Blacklisten einiger Anti-Spamfirmen gelangten.

Nachdem in den letzten Halbjahresberichten eine Abnahme von Phishing-Versuchen gegen Finanzdienstleister verzeichnet worden war, gab es im zweiten Halbjahr 2008 eine erhebliche Zunahme an Phishing-Versuchen gegen Internetdienste jeglicher Art. Dabei ist alles von Interesse, was «nur» mit Login und Passwort und nicht mit einer *Zweifaktoren-Authentifizierung* geschützt ist. Die Cyberkriminellen haben gemerkt, dass sich auch damit Geld machen lässt und solche Daten ihnen Zugriff auf weitere, interessante Informationen und Rechte ermöglicht. Der Hinweis, niemals seine Logindaten anzugeben, behält also weiterhin seine Gültigkeit und ist auf sämtliche passwortgeschützen Dienstleistungen auszudehnen**.**

3.7 Verschiedene Angriffe auf Webserver

Verschiedene Hacking-Angriffe sorgten im zweiten Halbjahr für Aufsehen. So wurde die Webseite mit den Medienmitteilungen der Stadtpolizei Zürich verunstaltet. Es handelte sich dabei um ein sogenanntes *Webseiten-Defacement.* Der Angreifer hinterliess die Nachricht

[9] http://www.genotec.ch/desktopdefault.aspx/tabid-219/184_read-458/ (Stand: 02.02.2009).
[10] http://www.20min.ch/news/schweiz/story/24375194 (Stand: 02.02.2009).
[11] Siehe für die Mitteilung der Uni Basel:
http://www.unibasel.ch/index.cfm?uuid=21A8F3823005C8DEA3B81CC699203FF9&type=search&show_long=1
(Stand: 02.02.2009).

«Hacked by Burak». Ausserdem erschien eine Zeichnung von zwei jungen Männern, die einen dritten fesselten.[12]

Ebenso drangen Hacker in einen Webserver der Europäischen Organisation für Kernforschung (CERN) ein und veränderten die dazugehörige Website[13]. Die Hacker hinterliessen ebenfalls eine Nachricht und machten sich über die Computertechniker des Atomforschungszentrums in Genf lustig. Sie bezeichneten diese, angesichts der Sicherheitslücke, als «Schuljungen».

Bei einer solchen Verunstaltung erfolgt in der Regel kein Zugriff auf Daten; es werden Sicherheitslücken in der Server-Software bzw. in den Server-Anwendungen ausgenutzt. In beiden Fällen wurde der Angriff rasch entdeckt und es entstand kein Schaden.

An der Eidgenössische Technische Hochschule (ETH) versuchten die Hacker im Oktober in mehrere zentrale Server einzudringen. Durch die interne Überwachung konnten die Angriffe erkannt und Gegenmassnahmen ergriffen werden. Nach diesem Vorfall wurde ein neues Sicherheitskonzept überprüft.[14]

3.8 Revision Urheberrechtsgesetz in Kraft getreten

Am 1. Juli 2008 ist die Revision des Schweizer Urheberrechts[15] in Kraft getreten. Die wichtigsten Änderungen sind:

Die technischen Massnahmen (z.B. Kopierschutz auf Audio-CDs) sind neu geschützt. Wer Programme zur Umgehung dieser anbietet oder benutzt, macht sich strafbar. Weiterhin er-

[12] Weitere Informationen:
http://www.bluewin.ch/de/index.php/25,77047/Unbekannte_hacken_Internetseite_der_Stadtpolizei_Zuerich/
(Stand: 02.02.2009).
[13] Weitere Informationen: http://diepresse.com/home/techscience/wissenschaft/414065/index.do?from=rss
(Stand: 02.02.2009).
[14] http://www.infoweek.ch/security/hacking/articles/164957/ (Stand: 02.02.2009).
[15] Die wichtigsten Änderungen des Schweizerischen Urheberrechtsgesetzes:
http://www.ige.ch/d/jurinfo/j10300.shtm (Stand: 02.02.2009).

laubt ist aber das Erstellen einer privaten Kopie, auch wenn dies die Umgehung von technischen Schutzmassnahmen bedeutet.

3.9 Pornoverbot auf Mobiltelefonen vom Parlament verabschiedet

Nach dem Ständerat, hat sich am 25. September 2008 auch der Nationalrat dafür ausgesprochen, dass der Bundesrat - gegen seinen Willen - Gesetzesbestimmungen für ein Verbot von Pornografie und Gewaltdarstellungen auf Handys ausarbeiten muss.[16] Dies hat möglicherweise auch Auswirkungen auf die Verordnung über Fernmeldedienste. Anbieter von Diensten der Grundversorgung könnten allenfalls dazu verpflichtet werden, alle Verbindungen zu kommerziellen Mehrwertdiensten mit erotischen oder pornografischen Inhalten für Personen unter 16 Jahren zu sperren. Auch könnten Mehrwertdienstleister verpflichtet werden, keine erotische oder pornografische Inhalte an Personen unter 16 Jahren zu überlassen.

Die parlamentarische Debatte wurde ausgelöst durch die Motion Schweiger.[17] Der Bundesrat hat in seiner Antwort auf diese Motion vor allem darauf hingewiesen, dass bereits das Strafgesetzbuch ein Angebot von pornografischen Schriften und Bildern an unter 16jährige verbiete. Egal ob diese zu kommerziellen oder nicht kommerziellen Zwecken angeboten werden. Es bräuchte also nur eine konsequente Anwendung der momentanen Rechtslage und nicht eine neue, zusätzliche Bestimmung. Allerdings ist nun darauf zu achten, dass genau diese neue, geforderte Verordnung möglichst technologieneutral ausgestaltet wird. Denn im Fokus der Motion waren ganz klar die kommerziellen Wap- oder MMS-basierten Handy-Porno-Angebote. Mit der zunehmenden technischen Konvergenz werden Handys aber auch vermehrt zu vollumfänglich Internettauglichen Geräten. Die Inhalte, die mit solchen Smartphones abgefasst werden können, sind nicht mehr speziell aufbereitete Inhalte für Handys, sondern schlicht und ergreifend dasselbe wie für jeden anderen Computerbenutzer auf dem Internet. Ein Verbot von kommerziellen Handypornoangeboten, welches nicht technologieneutral ausgestaltet wird, könnte also zu einem Zeitpunkt in Kraft treten, an dem dieses Phänomen bereits nicht mehr wirklich existiert.

3.10 Internet-Plattform für Pädophilie aufgedeckt

Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) hat anhand von Internetrecherchen und Abklärungen eine Webseite für Pädophile aufgedeckt, die bei einem St. Galler Provider gehostet wurde. Es handelte sich dabei um eine Plattform, auf der pädophile Interessen diskutiert wurden. Sie bot den Benutzern Gelegenheit, sich näher kennen zu lernen oder sich auf privater Ebene zu vernetzen. KOBIK konnte feststellen, dass im Forum Tipps und Erfahrungen für den Umgang mit kleinen Mädchen oder Anweisungen für erste Kontaktnahmen mit Kindern ausgetauscht wurden. Die Recherchen ergaben auch, dass kinderpornografische Dateien über das Forum ausgetauscht wurden.

Die Angaben zu den ausländischen Teilnehmern und Betreibern des Forums wurde vom Bundesamt für Polizei (fedpol) direkt an die betreffenden Länder übermittelt. Es handelt sich

[16] http://www.heise.de/newsticker/Schweizer-Parlament-verabschiedet-Pornoverbot-auf-Handys--/meldung/116550 (Stand: 02.02.2009).
[17] Siehe Motion 06.3884 - Keine kommerzielle Pornografie auf Handys: http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20063884 (Stand: 02.02.2009).

um rund 600 Personen aus Deutschland, 40 aus Österreich und vier aus dem Fürstentum Liechtenstein. Die Erkenntnisse zu den Schweizer Benutzern wurden an die St. Galler Strafverfolgungsbehörden weitergeleitet, weil der Provider dort ansässig ist. Bis heute sind gegen 13 Schweizer Bürger Strafverfahren eingeleitet worden. Vier Personen wurden verhaftet wegen sexuellen Handlungen mit Kindern oder Herstellens pornografischer Bilder und Filme unter direktem Missbrauch eines Mädchens. Bei allen Verdächtigen wurden Hausdurchsuchungen vorgenommen und umfangreiches Material wie Computer-Festplatten und andere Datenträger beschlagnahmt. Die Auswertungen werden noch einige Zeit in Anspruch nehmen. Aufgrund erster Ergebnisse kann aber festgestellt werden, dass grosse Mengen an kinderpornografischen Bild- und Filmmaterialen sichergestellt werden konnten.[18]

3.11 Verschiedene Sperren bei Grossfirmen

Verschiedene grosse Firmen, darunter Banken und Versicherungen, haben im letzten Halbjahr den Zugriff auf Social-Websites wie Facebook gesperrt. Als Gründe werden sowohl die übermässige Benutzung während der Arbeitszeit angegeben als auch die Gefahr, dass Angaben von Mitarbeitenden auf diesen Seiten für *Social Engineering*-Angriffe missbraucht werden können. Persönliche Informationen auf Facebook können durchaus dazu verhelfen, ein gewisses Profil einer Person oder Personengruppe zu vervollständigen: Wer gehört zu wem? Wo arbeitet jemand? Was macht er in seiner Freizeit? Wo ist er gerade? usw. Diese Informationen können dann mit anderen, auf dem Internet verfügbaren Daten verknüpft und verwendet werden, um das Vertrauen dieser Person zu erschleichen und dadurch leichter an vertrauliche Daten zu gelangen.

Sperrungen von Internetseiten innerhalb von Unternehmen können aus verschiedensten Gründen verhängt werden. Zum Einen lässt sich somit ein möglicher Kanal zur Verbreitung von Malware unterbinden, zum Andern lässt sich aber gerade im Bereich der Web 2.0 Seiten wie Facebook unter Umständen die Arbeitsmoral schützen. Im Falle der Vorbereitung für *Social Engineering-Angriffe*, greift eine Sperrung einer Internetseite aber Umständen zu kurz. In der Regel spielt es keine Rolle, ob die Mitarbeitenden die Daten während der Arbeitszeit respektive zu Hause eingeben. Wichtig ist, dass Firmen integrale Richtlinien definieren, welche Art von Firmeninformation auf solchen Webseiten publiziert werden dürfen.

Auch Doodle, ein öffentlicher Terminplaner, wurde von einigen Firmen gesperrt. Hier mit dem Hintergrund, dass vertrauliche Daten, wie Geschäftstermine oder Kundennamen nicht auf öffentliche «unkontrollierte» Plattformen gelangen.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 USA: Militär verbietet die Nutzung mobiler Speicher

Im November 2008 beschloss das US Strategic Command, dass Angehörigen der US-Armee die Nutzung mobiler Speicher (USB-Sticks, CD, DVD etc.) bis auf weiteres untersagt sei.

[18] Siehe für die öffentliche Mitteilung der St. Galler Staatsanwaltschaft: http://www.staatsanwaltschaft.sg.ch/news/staatsanwaltschaft/2008/09/internet_plattform.html (Stand: 02.02.2009).

Auslöser dafür war die rasche Ausbreitung eines Virus, welcher sich von USB-Sticks auf angeschlossene Systeme kopierte.[19] Das US-Militär hat hiermit eine radikale Massnahme ergriffen. Es steht jedoch nicht alleine da, wenn es darum geht, sich mit den Gefahren zu befassen, welche der Gebrauch von externen Datenträgern mit sich bringt. Auch Symantec warnte beispielsweise in einem Bericht vor der Verbreitung von Schädlingen über USB-Sticks.[20]

Zurzeit bestehen insbesondere folgende zwei Möglichkeiten, wie sich ein Schädling mit Hilfe eines USB-Sticks oder einem anderen mobilen Speicher verbreitet: Einerseits kann sich eine Schadsoftware direkt von einem infizierten Computer auf einen angeschlossenen USB-Stick kopieren. Wenn nun ein Nutzer den USB-Stick an seinen Computer anschliesst und (unbewusst) die infizierte Datei abruft, dann kopiert sich der Schädling auf den betroffenen Computer. Für diesen Infektionsweg ist es nötig, dass der Nutzer das infizierte Programm manuell aktiviert. Die zweite Möglichkeit besteht darin, dass die Schadsoftware eine AutoRun-Funktion des Speichermediums kreiert oder modifiziert. Wenn nun ein Nutzer den mobilen Speicher an seinen Computer anschliesst, dann kann sich die Schadsoftware automatisch auf den betroffenen Computer kopieren.

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat im Sommer 2008 einen Bericht veröffentlicht, um Unternehmen über die Gefahren im Umgang mit USB-Sticks zu informieren und Tipps für einen sicheren Umgang aufzuzeigen. Nebst der oben beschriebenen Gefahr eines zusätzlichen Infektionswegs für Schädlinge, verweist der Bericht insbesondere auf die Risiken im Zusammenhang mit Verlust und Diebstahl von USB-Sticks. Die ENISA betont die Bedeutung einer Risikoeinschätzung sowie verbindlicher Richtlinien im Umgang mit mobilen Speichern.[21]

Die wichtigsten Tipps im Umgang mit USB-Sticks:

- Die AutoRun Funktion ausschalten. Dies hat zur Folge, dass immer zuerst manuell eingegriffen werden muss, um den Stick aufzurufen. Eine Anleitung hierzu finden Sie im Anhang.
- Den USB-Stick mit einem aktuellen Antivirenprogramm überprüfen.
- Vertrauliche Informationen müssen chiffriert gespeichert werden. Bei einem Diebstahl ist zwar der Stick verloren, die Information, respektive die Datei, ist jedoch geschützt.
- Jedes Unternehmen, egal ob kleiner, mittlerer oder grosser Betrieb, sollte den Einsatz von USB-Sticks zwingend in Richtlinien regeln. Diese Richtlinien müssen Anweisungen enthalten, unter welchen Voraussetzungen Sticks verwendet werden dürfen. Einige Sticks versuchen, Software auf dem Endgerät zu installieren. Mit der Abgabe von zentral beschafften Sticks, lässt sich dieser Umstand zumindest eingrenzen. Weitere Möglichkeiten sind die Beschränkung von Administratoren-Rechten oder die Deaktivierung der USB-Ports.

[19] http://blog.wired.com/defense/2008/11/army-bans-usb-d.html (Stand: 02.02.2009).

[20] https://forums.symantec.com/t5/blogs/blogarticlepage/blog-id/malicious_code/article-id/220 (Stand: 02.02.2009).

[21] http://www.enisa.europa.eu/doc/pdf/publications/Secure%20USB%20drives_180608.pdf (Stand: 02.02.2009).

4.2 Erfolge gegen Cyberkriminelle

Im zweiten Halbjahr 2008 konnten diverse Erfolge gegen Cyberkriminelle verzeichnet werden. So hat im Oktober die holländische Staatsanwaltschaft bekannt gegeben, dass eine Gruppe, welche für zahlreiche E-Banking Betrügereien - mutmasslich auch in der Schweiz - verantwortlich ist, in der Ukraine und in Russland verhaftet werden konnte.[22]

Der durch die Betrüger entstandene Schaden wird auf mehr als 100'000 Euro geschätzt. In mehreren Städten in der Ukraine und in Russland wurden Computer und andere Beweismittel sichergestellt. Bei den Verhafteten handelt es sich um drei Informatikstudenten. Nach der Festnahme von acht Verdächtigen in Deutschland durch das Bundeskriminalamt (BKA) im September 2007[23] ist dies der zweite grosse Schlag gegen E-Banking-Betrüger. Damals handelte es sich um zwei Frauen im Alter von 22 und 23 Jahren sowie um sechs Männer im Alter von 20 bis 36 Jahren aus Russland, der Ukraine und Deutschland.

4.3 Deutschland: Grosser Datendiebstahl bei der Telekom

Im Jahr 2008 sind weltweit zahlreiche Datenverluste bekannt geworden. Davon betroffen waren sowohl die Privatwirtschaft als auch Regierungssektoren.

In Deutschland hat insbesondere die Bekanntmachung der Telekom zum Verlust von mehr als 17 Millionen Kundendaten, die Debatte über Datensicherheit und Datenschutz erneut in Gang gebracht.[24] Die gestohlenen Datensätze sollen geheime Telefonnummern und Privatadressen von bekannten Politikern und Wirtschaftsführern umfasst haben. Die Daten wurden jedoch bereits im Jahre 2006 gestohlen. Damals wurden die Behörden eingeschaltet, die Öffentlichkeit über den Datenverlust jedoch nicht informiert. Die Daten sollen daraufhin im Internet in kriminellen Kreisen angeboten worden sein und im Oktober 2008 wurde der Fall

22 Pressemitteilung der holländischen Staatsanwaltschaft (in holländisch) http://www.om.nl/actueel/nieuws-_en/@149040/internationale/ (Stand: 02.02.2009).

23 http://www.heise.de/newsticker/BKA-verhaftet-Phisher-Gruppe--/meldung/95928 (Stand: 02.02.2009).

24 Siehe für die Pressemitteilung der Telekom:
http://www.telekom.com/dtag/cms/content/dt/de/595698?archivArticleID=572376 (Stand: 02.02.2009).

durch das Nachrichtenmagazin «Der Spiegel» publik gemacht.[25] Die Regierung entschied daraufhin, Gefährdungsanalysen für die betroffenen Prominenten zu erstellen.

Bei diesem Vorfall handelt es sich um ein besonders prominentes Beispiel von Datenverlust. Datenverluste und Datenpannen sind jedoch zahlreich und davon betroffen sind sowohl die Privatwirtschaft als auch Regierungssektoren. Die Gründe dafür sind vielfältig und umfassen internen und externen Diebstahl, Verluste und Diebstahl von digitalen Speichern (Laptops, USB-Sticks etc.), unbeabsichtigte Veröffentlichung und Verbreitung von Daten sowie Verlust von Daten durch externe Dienstleister (beispielsweise Beratungsfirmen).

Die zunehmende Ansammlung persönlicher Daten ist eine natürliche Begleiterscheinung unserer modernen Informationsgesellschaft. Gesammelte Daten und Informationen können gleichermassen als Wertschöpfungspotenzial wie auch als Risiko betrachtet werden. Somit steigt die Bedeutung eines sicheren, vertrauensvollen und geregelten Umgangs mit Daten. Ein klares Risikomanagement im Umgang mit Daten und Informationen ist für die Privatwirtschaft ebenso von Bedeutung wie für den öffentlichen Sektor[26].

4.4 EU: Plan zu einer umfassenden und gemeinsamen Bekämpfung der Internetkriminalität beschlossen

Ende November 2008 haben die Justiz- und Innenminister der Europäischen Union (EU), einen Plan zu einer umfassenden und gemeinsamen Bekämpfung der Internetkriminalität beschlossen. Die vorgesehenen operativen Massnahmen umfassen unter anderem eine europäische Plattform für Hinweise zu Internetstraftaten, ein effizienter Informationsaustausch zwischen Strafverfolgungsbehörden und Privatwirtschaft, der Einsatz grenzübergreifender Ermittlungsteams, eine bessere Koordination beim Blockieren und Schliessen von strafbaren Webseiten und Erstellung einer gemeinsamen schwarzen Liste sowie die Erleichterung von Ferndurchsuchungen (was Online-Durchsuchungen entsprechen dürften), sofern diese nach nationalem Recht vorgesehen sind.[27]

4.5 Deutschland: Vorratsdatenspeicherung auch für Internetprovider

Seit dem 1. Januar 2009 müssen in Deutschland alle Internet-Verbindungsdaten für ein halbes Jahr gespeichert werden, ohne dass ein konkreter Verdacht vorliegen muss. Die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung von Telekommunikation- und Internet-Verbindungsdaten ist in Deutschland bereits auf Anfang 2008 in nationales Recht umgesetzt

[25] http://www.spiegel.de/wirtschaft/0,1518,581938,00.html (Stand: 02.02.2009).

[26] Siehe zum Thema Unternehmen und ihr Umgang mit Informationen folgende im Auftrag von der Economist Intelligence Unit ausgeführte Studie: http://switzerland.emc.com/collateral/analyst-reports/economist-intell-unit-info-governence.pdf (Stand: 02.02.2009).

[27] Siehe für die Schlussfolgerungen des Rates Justiz und Inneres:
http://register.consilium.europa.eu/pdf/de/08/st15/st15569.de08.pdf
und für die Mitteilung der EU-Kommission:
http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=0&language=DE&guiLanguage=en (Stand: 02.02.2009).

worden.[28] Die Verbindungsdaten, welche beim Telefonieren im Fest- und Mobilnetz anfallen, werden bereits seit Anfang 2008 gespeichert. Für die Internetprovider galt eine Übergangsfrist, welche per Ende 2008 abgelaufen ist.[29]

4.6 Deutschland: Revidiertes BKA-Gesetz tritt in Kraft

Auf den 1. Januar 2009 tritt in Deutschland das geänderte Gesetz für das Bundeskriminalamt (BKA) in Kraft. Dieses Gesetz sieht neue Befugnisse im Kampf gegen den Terrorismus vor und ermöglicht unter Anderem heimliche Online-Durchsuchungen.[30]

4.7 Grossbritannien: Neues Cybercrime-Gesetz tritt in Kraft

In England und Wales ist auf den 1. Oktober 2008 der erneuerte «Computer Misuse Act» in Kraft getreten. Die wichtigsten Neuregelungen betreffen die Verschärfung des Strafmasses für unautorisiertes Eindringen in ein Computersystem sowie ein Verbot von *Denial-of-Service-Attacken (DOS)* und der Verbreitung von «Hacker-Tools».[31]

5 Tendenzen / Ausblick

5.1 Allgemeine Entwicklung Cybercrime

Auf der technischen Seite haben sich die Mittel der Cyberkriminellen im letzten Halbjahr nicht gross verändert. Zur Verbreitung von Schadsoftware werden Spam-E-Mails und Drive-by-Infektionen benutzt. In der Schweiz empfangene Malware-E-Mails sind neben Englisch auch in Deutsch, Französisch und Italienisch verfasst. Um an persönliche Daten zu gelangen, werden Trojaner und Phishing eingesetzt. Trojanische Pferde werden mittels *Root-Kit* Funktion versteckt. Phishing-Seiten werden auf *Fast-Flux-Netzwerken* gehostet. Botnetzwerke sind immer noch das wichtigste Mittel zum Zweck und sind immer noch in grosser Zahl vorhanden. *Sicherheitslücken* spielen bei der Verbreitung von Schadsoftware immer noch eine (zu) grosse Rolle, wie das jüngste Beispiel der Verbreitung des Conficker-*Wurmes* zeigt.

---

[28] Siehe den MELANI Halbjahresbericht 2007/2, Kapitel 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand: 02.02.2009).

[29] Siehe für ausführliche Informationen zum Thema folgende Seite vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Deutschland: http://www.bfdi.bund.de/cln_007/nn_533578/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html (Stand: 02.02.2009).

[30] Für den Gesetzestext siehe: http://www.bgblportal.de/BGBL/bgbl1f/bgbl108s3083.pdf; Siehe zur Debatte betreffend Online-Durchsuchungen in Deutschland auch den MELANI Halbjahresbericht 2008/1, Kapitel 7.1: http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (Stand: 02.02.2009).

[31] Siehe für den Rechtserlass: http://www.opsi.gov.uk/si/si2008/uksi_20082503_en_1; den Computer Misuse Act: http://www.opsi.gov.uk/acts/acts1990/UKpga_19900018_en_1.htm und den Police and Justice Act: http://www.opsi.gov.uk/Acts/acts2006/ukpga_20060048_en_1 (Stand: 02.02.2009). Siehe für weitere Informationen auch folgenden Artikel: http://www.theregister.co.uk/2008/09/30/uk_cybercrime_overhaul/ (Stand: 02.02.2009).

Was sich allerdings ändert sind die Geschäftsstrukturen der Cyberkriminellen: Es etabliert sich nach und nach eine richtige Dienstleistungsorganisation. Es sind nicht mehr eigenständige einzelne Gruppen, sondern vernetzte Strukturen, die sich auf die einzelnen Aufgaben konzentrieren. Der Informationsaustausch zwischen diesen Gruppen funktioniert scheinbar hervorragend. Jeder Cyberkriminelle sucht sich eine Nische und versucht anschliessend sein Produkt im «Markt» anzubieten. Dabei werden mittlerweile ganze Servicepakete angeboten (Kapitel 5.2)

Da die Problematik mittlerweile bekannt ist, könnte man annehmen, dass die Gegenmassnahmen relativ einfach durchgeführt werden können. Einzelne Erfolge wie die Verhaftung einer E-Banking-Betrügerbande (Kapitel 4.2) oder der Abschaltung des Providers McColo (Kapitel 7.4), stimmen hier zuversichtlich. Trotz dieser Erfolge ändert dies an der Dimension des Schadens, der tagtäglich angerichtet wird, nicht sehr viel. Die Täter vermögen sich den neuen Situationen jeweils bestens anzupassen. Fällt ein Glied weg, springt das nächste in die Bresche und versucht die Lücke so schnell wie möglich zu schliessen. Die Abschaltung von McColo hat beispielsweise nur zu einem kurzfristigen Rückgang der Spam-E-Mails geführt. In der ersten Februarwoche 2009 hat das durchschnittliche Spam-Aufkommen erstmals wieder das gleiche Niveau wie vor der Abschaltung des Spam-Hosters McColo erreicht.[32] Auch die Verhaftung der E-Banking-Betrüger brachte in der Schweiz nur eine kurze Erholung. Knapp 4 Monate später versuchte bereits eine neue Gruppe mit einer neue Trojanerfamilie sich zu etablieren.

Leider ist die Reaktion auf Seiten der Bekämpfung um einiges träger. Die Diskussion über die Verantwortung bei der Internetsicherheit ist in vielen Fällen noch nicht abschliessend geklärt. Je nach Fall und Ausgangslage liegt die Verantwortung bei der Strafverfolgung, bei den Providern, den Registrierungsstellen, den Webseitenbetreibern oder bei den Internetnutzern selber. Nicht selten könnten Angriffe durch die richtige Reaktion oder Vernetzung mehrerer dieser beteiligten Parteien gänzlich unterbunden werden. Insofern scheint es klar, dass alle, die Dienste im Internet anbieten oder Dienste nutzen, in irgendeiner Form verantwortlich sind. Leider wird aber noch in zu vielen Fällen auf ein Schwarzpeterspiel ausgewichen, statt die korrekten Lehren zu ziehen und damit eine Lösung zur erhöhten Internetsicherheit beizusteuern.

5.2 Neue «Geschäftsmodelle» und «Services» verleihen der Cyberkriminalität 2009 neuen Schub

In der Cyberkriminalität wurde im letzten Jahr das kommerzielle Modell Crimeware-as-a-Service (CaaS)[33] entwickelt. Die Cyberkriminellen, welche sich der technischen Schwierigkeiten mit der Server-Verwaltung, der Installation von Toolkits oder der Infizierung von Websites bewusst sind, können bei diesem Modell, einen entsprechenden Dienst «mieten». Über diese Plattformen erhalten sie die Daten (Kreditkarten, Zugangsdaten zu Bankkonten, Webservern usw.) direkt von anderen Internetkriminellen (Criminal-to-Criminal, C2C). Anschliessend können sie sich damit bereichern (u.a. Finanztransaktionen, Weiterverkauf von Daten oder Erwerb von Gütern). Dieses neue kommerzielle Modell wird im Laufe des Jahres 2009[34]

[32] Siehe auch: http://www.eleven.de/de/aktuell/pressemitteilungen/eleven-spam-aufkommen-hat-sich-von-mccolo-abschaltung-erholt-398.html (Stand: 02.02.2009).

[33] http://www.finjan.com/Pressrelease.aspx?id=1922&PressLan=1819&lan=3 (Stand: 03.02.2009)

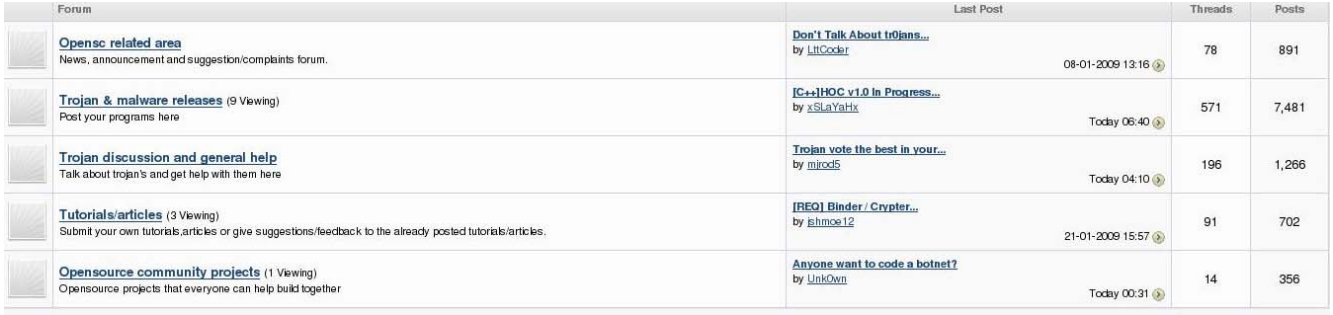
[34] http://www.finjan.com/GetObject.aspx?ObjId=641&Openform=50 (Stand: 15.01.2009, Studie kann ohne vorgängige Registrierung nicht heruntergeladen werden)

aufgrund diverser Faktoren wie der Wirtschaftskrise oder der Schwierigkeit, die Kriminellen aufzuspüren und sie strafrechtlich zu verfolgen, einen deutlichen Entwicklungsschub erleben.

Eine oft gestellte Frage ist die, ob der Zugang zu dieser Art von kriminellen Aktivitäten wirklich so einfach ist, wie in verschiedenen Studien dargelegt wird. Wie alle illegalen Tätigkeiten entsteht die Cyberkriminalität in einem immer wieder neuen und unbekannten Umfeld, um den Augen der Ordnungshüter, Forscher und sonstigen Security-Experten möglichst zu entgehen. Ein gewisser Grad an Anonymität wird beispielsweise dadurch gewahrt, dass man via *Internet Relay Chat Protokoll (IRC)*, kommuniziert. Es gibt Server mit nur einigen wenigen Kanälen, aber auch solche mit Zehntausenden von Kanälen. Auf Letzteren nehmen die Cyberkriminellen Kontakt miteinander auf, im vollen Bewusstsein dort unerkannter operieren zu können. Internetkriminelle bieten auf IRC-Kanälen ihre Dienste an, verkaufen diese und kaufen anderen solche ab[35]. Kriminelle bieten zwar branchenfremden Personen all-included-Dienste an, aber es ist auch sehr schwer, an neue Interessenten heranzukommen. Die IRC-Kanäle sind für Neulinge nicht leicht zugänglich, einerseits wegen technischer Anwendungsprobleme, andererseits wegen der ungeheuren Menge an Kanälen, die ein Server anbieten kann und der sich daraus ergebenden Schwierigkeit, das Gesuchte auch zu finden.

Was eignet sich da besser als ein webbasierter Dienst? Die erste Form eines solchen Dienstes war die Website 76service.com[36]. Die Abonnenten konnten die neusten gestohlenen Daten von einer Malware namens Gozi[37] herunterladen, nachdem sie sich ausgewiesen hatten. 76service.com machte Schule und generierte eine Vielzahl ähnlicher Dienste, die praktisch in Echtzeit die gestohlenen Daten, mit denen man Zugriff auf Bankkonten erhält oder Kreditkarten fälschen kann, zum Verkauf anboten[38].

Doch die Geschäftsmodelle der Cyberkriminellen führen noch weiter. Sie bieten ihre Dienste heutzutage nicht nur ganz offen an, auch die Tools werden neu über allgemein zugängliche Kanäle, wie beispielsweise über offene Foren, angeboten. Jeder der Erläuterungen zur Verwendung der gekauften Malware oder eine Hilfe für deren Weiterentwicklung benötigt, wird hier den idealen Support finden:



Forum	Last Post	Threads	Posts
Opensc related area News, announcement and suggestion/complaints forum.	**Don't Talk About tr0jans...** by LttCoder 08-01-2009 13:16	78	891
Trojan & malware releases (9 Viewing) Post your programs here	**[C++]HOC v1.0 In Progress...** by xSLaYaHx Today 06:40	571	7,481
Trojan discussion and general help Talk about trojan's and get help with them here	**Trojan vote the best in your...** by mjrod5 Today 04:10	196	1,266
Tutorials/articles (3 Viewing) Submit your own tutorials,articles or give suggestions/feedback to the already posted tutorials/articles.	**[REQ] Binder / Crypter...** by ishmoe12 21-01-2009 15:57	91	702
Opensource community projects (1 Viewing) Opensource projects that everyone can help build together	**Anyone want to code a botnet?** by UnkOwn Today 00:31	14	356

Für die verbreiteten und beliebtesten Kits wie El Fiesta oder IcePack wird die Malware oft zusammen mit den *Exploits* angeboten. Dabei handelt es sich meist um Raubkopien dieser Malware. Den Entwicklern solcher Crimeware ist es sogar gelungen, diese mit exklusiven

[35] http://www.symantec.com/content/de/de/about/downloads/PressCenter/20081124_UE_Report_Final.pdf (Stand: 17.12.2008)

[36] http://rbnexploit.blogspot.com/2007/10/rbn-76service-gozi-hangup-team-and-us.html (Stand:.02.2009)

[37] http://www.secureworks.com/research/threats/gozi/?threat=gozi (Stand:.02.2009)

[38] http://ddanchev.blogjspot.com/2008/12/zeus-crimeware-as-service-going.html

Benutzerlizenzen auszustatten, um das geistige Eigentum ihrer Arbeit zu schützen, wie bereits im ersten Halbjahresbericht 2008 von MELANI aufgezeigt worden war[39]

magicz
Junior Member

Zeus 1.1.0.0

my_poly_sploit ie6-ie7-op-firefox

icepack-ie7 mod

fiesta Sploit-pack

---

sell New version 700$ Sploit-Pack pri8 only

and Zeus 1.2.1.0 3000$

If someone of you interested in something, I say the prices of new things
I can help but not everyone can buy it pri8 only Zeus+Sploit-Pack

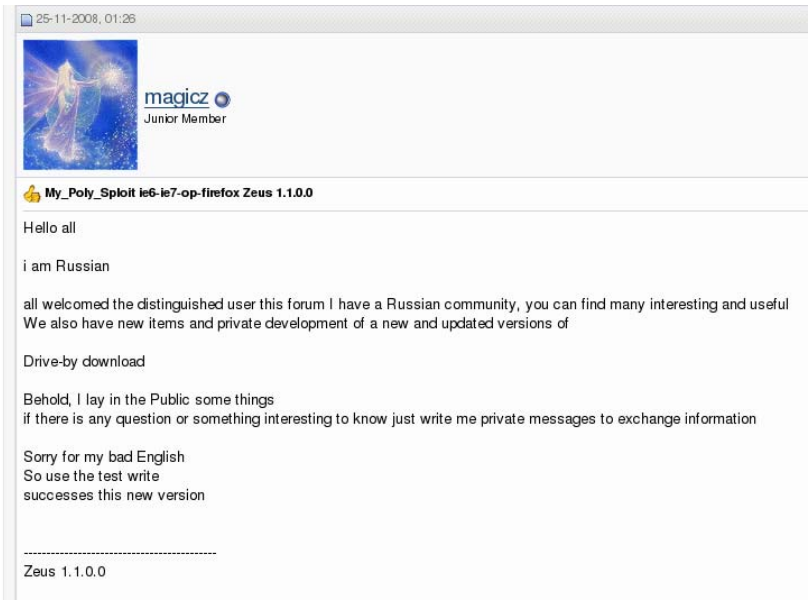
i create this topic

i russian man on Undegroun Scene

If anyone interested in new items that I can help you with this

PM me

Im Angebot steht aber nicht nur der Verkauf von Malware, es wird auch Support angeboten – es ist alles nur eine Frage des Preises.



25-11-2008, 01:26

magicz
Junior Member

My_Poly_Sploit ie6-ie7-op-firefox Zeus 1.1.0.0

Hello all

i am Russian

all welcomed the distinguished user this forum I have a Russian community, you can find many interesting and useful
We also have new items and private development of a new and updated versions of

Drive-by download

Behold, I lay in the Public some things
if there is any question or something interesting to know just write me private messages to exchange information

Sorry for my bad English
So use the test write
successes this new version

Zeus 1.1.0.0

[39] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=it ("Professionalisierung der Cyberkriminalität am Beispiel ZeuS", Stand: 12.02.2009)

Ob sich die Internetkriminalität in Richtung Outsourcing bewegt oder denjenigen vorbehalten bleibt, die zumindest einschlägige Grundkenntnisse besitzen - Eines ist sicher: In Zeiten der Wirtschaftskrise und angesichts der Schwierigkeiten bei der strafrechtlichen Verfolgung von Cyberkriminellen wird die Tatsache, dass die Mittel zur Begehung von Verbrechen auf Kanälen angeboten werden, die Internetusern offen und leicht zugänglich sind, dieser «Branche» im 2009 einen neuen Entwicklungsschub verleihen.

5.3 Umgang mit Datenmüll der Informationsgesellschaft

Der Speicherplatz auf elektronischen Geräten wird zusehends grösser. Ausserdem befindet sich heute praktisch in jedem elektronischen Gerät eine *Speicherkarte*. Die Menge an gespeicherten Daten, welche jede Person anhäuft, steigt kontinuierlich an. Um dem entgegenzuwirken, sollten nicht mehr benutzte Daten gelöscht werden.

Das korrekte Löschen von Daten ist allerdings vielen nicht klar. Gerade wenn man beispielsweise die Kamera, das Handy oder den USB-Stick weitergibt, ist das Löschen von Daten unabdingbar. Hierbei müssen einige Hinweise beachtet und ein Verfahren gewählt werden, das für das jeweilige Medium, für den Schutzbedarf der Informationen und für den konkreten Anwendungsfall geeignet ist.

Kapitel 7.1 im Anhang gibt hierzu einige praktische Tipps, welche sowohl im Privatbereich als auch in Firmen eingesetzt werden können. Zusammengefasst sind dies:

- Ein einfaches Löschen reicht nicht aus, die Daten können so wiederhergestellt werden.
- Die Löschmethode hängt von der Vertraulichkeit der Daten ab.
- Spezielle Lösch-Tools (Wipe-Tools) benutzen.
- Bei optischen Datenträgern am besten den Datenträger schreddern.

5.4 Zugangsdaten zu Internetdiensten zukünftig vermehrt im Visier der Cyberkriminellen

Nachdem klassisches Phishing in der Schweiz gegen E-Banking Kunden nur noch in geringem Ausmass eingesetzt wird, könnte man annehmen, dass dieses Problem nun der Vergangenheit angehört. Dass klassisches Phishing aber weiterhin ein Problem ist, zeigen Meldungen, die MELANI und KOBIK regelmässig erhalten. Für sämtliche Dienste im Internet werden Benutzernamen und Passwörter benötigt: So beispielsweise beim E-Mail-Konto, dem Zugang zu Website-Servern, Auktions- oder Trading-Plattform sowie zu E-Shops. Diese Daten werden zukünftig noch vermehrt ins Visier der Cyberkriminellen geraten. Im Gegensatz zu E-Banking-Konten fehlt hier meist eine Zwei-Faktoren Authentifizierung: Der Schutz beschränkt sich auf Login und Passwort. Ziel sind dabei in der Regel nicht die Inhaber der Konti. Die Konti sind nur Mittel zum Zweck und werden für die Durchführung einer Straftat missbraucht: Sei dies beispielsweise, um unter einer anderen Persönlichkeit aufzutreten, sei dies um ein hohes Rating eines Auktionskontos zu verwenden oder um Webseiten mit Drive-by-Infektionen zu versehen, die dann wiederum einen E-Banking-Trojaner verbreiten. Im letzten Fall wird also Phishing verwendet, um Malware zu verbreiten, die dann wiederum gegen E-Banking-Applikationen gerichtet ist.

Einzelne Sicherheitsaspekte dürfen in Zukunft nicht isoliert betrachtet werden, sondern müssen als Gesamtes gesehen und als Ganzes bekämpft werden. Jeder Einzelne, der entweder einen Internetdienst nutzt oder einen solchen anbietet, ist Teil dieser Internetsicherheit. Dieses Bewusstsein und auch die Verantwortung wird sich in den nächsten Jahren verstärken müssen. Besonders Provider werden in Zukunft vermehrt ins Visier der Cyberkriminellen rücken.

6 Glossar

Dieses Glossar enthält sämtliche *kursiv* hervorgehobenen Begriffe. Ein ausführlicheres Glossar mit weiteren Begriffen ist zu finden unter:
http://www.melani.admin.ch/glossar/index.html?lang=de.

ActiveX	Eine von Microsoft entwickelte Technologie, mit welcher es möglich ist, kleine Programme - so genannte ActiveX Controls - beim Anzeigen von Webseiten auf den Rechner des Besuchers zu laden, von wo sie ausgeführt werden. Sie ermöglichen es, unterschiedliche Effekte oder Funktionen umzusetzen. Leider wird diese Technologie häufig missbraucht und stellt ein Sicherheitsrisiko dar. Beispielsweise werden viele Dialer über ActiveX auf den Rechner geladen und ausgeführt. Die ActiveX-Problematik betrifft nur den Internet Explorer, da die anderen Browser diese Technologie nicht unterstützen.
Bot / Malicious Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. Sogenannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Botnetz	Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierten Rechnern bestehen.
CA	Certificate Authority (deutsch: Zertifizierungsstelle) Eine Zertifizierungsstelle ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht.
cc-TLD	Country Code - Top Level Domain Jeder Name einer Domain im Internet besteht aus einer Folge von - durch Punkte getrennten - Zeichen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Beispiel: Bei

	http://www.melani.admin.ch ist die TLD «ch». Ist diese TLD einem Land zugeordnet spricht man von einer ccTLD.
Command & Control Server	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Denial of Service (DDoS)	Denial-of-Service Attacke / Distributed-Denial-of-Service Attacke. Eine DDoS-Attcke hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Eine DDoS-Attacke ist eine Dos-Attacke, bei der das Opfer von vielen verschiedenen Systemen aus gleichzeitig angegriffen wird.
DNS-System	Domain Name System Mit Hilfe von DNS werden das Internet und deren Dienste benutzerfreundlich, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch). Der DNS-Dienst übersetzt dabei den Namen in die dazugehörende IP-Adresse.
Drive-by-Infektion	Infektion eines Computers mit Malware allein durch den Besuch einer Webseite. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausnutzen einer Sicherheitslücke.
Exploit-Code	(kurz: Exploit) Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Fast Flux	Fast Flux ist eine DNS-Technik, welche von Botnetzwerken verwendet wird um Phishingseiten oder Seiten, die Malware verbreiten, auf diversen Hosts zu verteilen und so zu verstecken. Fällt ein Computer aus, springt der nächste Computer in die Bresche.
Finanzagent	Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System - das heisst auf Ihrem Rechner - installiert.
Flash	Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash findet heutzutage auf vielen Webseiten Anwendung, sei es als Werbebanner, als Teil einer Website z.B. als Steuerungsmenü oder in Form kompletter Flash-Seiten.

Flash-Speicherkarte	Flash-Speicher sind digitale Speicherchips. Anwendung finden Flash-Speicher überall dort, wo Informationen auf kleinstem Raum gespeichert werden. Beispiele: USB-Sticks, Speicherkarten für Digitalkameras, Mobiltelefone, Handhelds, MP3-Player.
FTP-Kontodaten	File Transfer Protocol (FTP) ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Webseiten auf einen Webserver zu laden.
Hashfunktion MD5	Algorithmus welcher aus einem beliebigen Text eine immer gleichlange Zahlenfolge generiert. Hashfunktionen werden in drei Bereichen verwendet: • In der Kryptografie. • Bei Datenbanksystemen. Diese verwenden Hashfunktionen, um in grossen Datenbankbeständen effizient zu suchen. • Bei Prüfsummen. Jeder Datei kann ein Hashwert zugeordnet werden. Ein veränderter Hashwert deutet auf eine Manipulation hin.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) Die ICANN ist eine privatrechtliche Non-Profit-Organisation mit Sitz in der kalifornischen Küstenkleinstadt Marina del Rey. ICANN entscheidet über die Grundlagen der Verwaltung der Top-Level-Domains. Auf diese Weise koordiniert ICANN technische Aspekte des Internets, ohne jedoch verbindliches Recht zu setzen. Die ICANN untersteht dem US-amerikanischen Handelsministerium (Department of Commerce) und ist somit der US-Regierung unterstellt.
Internet Relay Chat (IRC)	Internet Relay Chat ist ein Dienst des World Wide Web. Er ermöglicht beispielsweise das Chatten in Echtzeit.
Javascript	Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Malware (Schadsoftware)	Setzt sich aus den englischen Begriffen «Malicious» und «Software» zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). (Auch: Malicious Code).
MoneyGram	MoneyGram International, Inc. ist ein US-amerikanisches Finanzunternehmen mit Sitz in Minneapolis, das international am Fi-

	nanzmarkt vertreten ist. Über eine MoneyGram-Filiale kann durch Einzahlung in einer Filiale ein Geldbetrag zwischen 2 Personen transferiert werden.
Peering	Unter dem Begriff Peering (engl. peer = gleichrangig) versteht man einen direkten Zusammenschluss von IP-Netzwerken, um Datenaustausch zwischen zwei Partnern (z.B. Providern) zu routen.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das E-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Plugin	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plugins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
Root-Kit	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.
Schadsoftware (Malware)	Setzt sich aus den englischen Begriffen «Malicious» und «Software» zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). (Auch: Malicious Code).
SHA	Secure Hash Algorithm. (engl. für sicherer Hash-Algorithmus), Der Begriff SHA bezeichnet eine Gruppe standardisierter kryptologischer Hash-Funktionen. Diese dienen zur Berechnung eines eindeutigen Prüfwerts für beliebige elektronische Daten.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.
SSL/TLS Serverzertifikat	Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht.
Trojanisches Pferd	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.

UDP	User Datagram Protocol UDP ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen.
Webseiten-Defacement	Verunstaltung von Webseiten.
Western-Union	Western Union ist der führende Anbieter von weltweitem Geldtransfer und bietet die Möglichkeit, schnell Geld rund um den Globus zu transferieren, Rechnungen zu bezahlen und Zahlungsanweisungen zu erwerben.
Wurm	Im Gegensatz zu Viren benötigen Würmer zur Verbreitung kein Wirtprogramm. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen, um sich selbständig von Rechner zu Rechner auszubreiten.
Zweifaktoren Authentifizierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z.B. Fingerabdruck, Retina-Scan, Stimmerkennung, usw.)

7 Anhang

7.1 Endgültiges Löschen von Daten auf Datenträgern[40]

Damit gespeicherte Daten nicht in falsche Hände geraten können, ist eine geregelte Vorgehensweise erforderlich, um Daten und Datenträger zu löschen oder zu vernichten. Bevor Datenträger wieder verwendet werden, müssen die gespeicherten Daten vollständig gelöscht werden. Dies ist insbesondere wichtig, wenn Datenträger an Dritte weitergegeben werden sollen.

Es gibt verschiedene Methoden, um Informationen auf Datenträgern zu löschen. Welche Methode gewählt werden soll, hängt hierbei wesentlich vom Schutzbedarf der zu löschenden Daten ab, aber natürlich auch von der Art der Datenträger. Folgende Datenträger werden heutzutage verwendet:

[40] Vorlage dieser Anleitung sind „Sicheres Löschen von Datenträgern“ https://ssl.bsi.bund.de/gshb/deutsch/m/m02167.htm und „Brennpunkt: Minianwendungen sicher nutzen“ http://www.bsi-fuer-buerger.de/brennpunkt/index.htm des Bundesamtes für Sicherheit in der Informationstechnik BSI in Deutschland.

- magnetische Speichermedien wie Festplatten, Disketten, Wechselplatten, Zip-Disketten, Magnetbänder,
- optische Speichermedien (z. B. CD, DVD),
- elektronische Speichermedien (z. B. Flash-Speicher oder Flash-Karten, wie USB- bzw. Memory-Sticks oder andere elektronische Speicherkarten).

Im Folgenden sind Hinweise und Empfehlungen für die wichtigsten Methoden zum Löschen und Vernichten von Datenträgern aufgeführt:

Löschkommandos

Löschkommandos sind vom Betriebssystem zur Verfügung gestellte Befehle und Funktionen, um Dateien oder Verzeichnisse zu löschen. Bei der Benutzung von Löschkommandos ist zu beachten, dass dabei in der Regel nicht tatsächlich die Datei-Informationen gelöscht werden, sondern nur der Verweis auf diese Informationen im «Inhaltsverzeichnis» des Datenträgers. Die Datei ist weiterhin vorhanden.

Formatieren

Bei Festplatten wird zwischen Low-Level-Formatierung, bei der Spuren und Sektoren auf der Platte neu erzeugt werden, und der logischen oder High-Level-Formatierung, die durch das Betriebssystem erfolgt, unterschieden. Eine High-Level-Formatierung ist als sicheres Löschverfahren ungeeignet, da dabei lediglich die Datei-Systemstruktur neu angelegt wird.

Für Festplatten konnte früher durch den Anwender eine sogenannte Low-Level-Formatierung durchgeführt werden, bei der die magnetischen Grundstrukturen neu geschrieben wurden. Bei modernen Festplatten kann dies in der Regel nur noch der Hersteller vornehmen.

Für wiederbeschreibbare CD-ROMs (CD-RW), Disketten oder ähnliche Datenträger muss beachtet werden, dass eine schnelle Formatierung die Daten nicht löscht. Eine komplette Löschung ist daher notwendig.

Überschreiben einzelner Dateien

Daten auf intakten Festplatten können mit spezieller Software durch Überschreiben vollständig und nicht widerherstellbar gelöscht werden. Dabei werden die Daten einmal oder mehrfach mit vorgegebenen Zeichen oder Zufallszahlen überschrieben. Die Datenträger sind nach dem Überschreiben weiterhin nutzbar. Die meisten dieser Tools bieten verschiedene Verfahren des Überschreibens an. Bekannte Methoden sind das sehr sichere Peer-Gutmann-Verfahren[41], das die Daten 35-mal mit wechselnden Zahlenfolgen überschreibt, allerdings auch sehr langsam ist. Das Russian GOST P50739-95 oder das DoD 5220.22-M (E)-Verfahren, welches die Daten 3 Mal überschreibt, was für den Privatgebrauch in den meisten Fällen ausreichend ist. Welches Verfahren Sie letztendlich anwenden, hängt jedoch von Ihren persönlichen Sicherheitsanforderungen ab.

Beispiele für kostenlose Programme, die Daten sicher löschen, sind «Eraser»[42] «Secure Eraser»[43] und «KillDisk»[44].

---

[41] http://de.wikipedia.org/wiki/Gutmann-Methode (Stand: 02.02.2009).
[42] http://www.chip.de/downloads/Eraser-5.8.6a_12994923.html (Stand: 02.02.2009).
[43] http://www.chip.de/downloads/Secure-Eraser_13008545.html (Stand: 02.02.2009).
[44] http://www.killdisk.com/ (Stand: 02.02.2009).

Fortgeschrittene Anwender können auch das Löschprogramm cipher.exe[45], das in Windows integriert ist, nutzen. Das Programm steht unter Windows XP und Vista zur Verfügung und löscht freigegebene Datenbereiche auf der Festplatte durch dreimaliges Überschreiben.

Und so benutzen Sie cipher.exe

1. Löschen Sie alle Dateien aus dem Papierkorb.
2. Gehen Sie auf Start/Ausführen und geben Sie in die Kommandozeile cmd ein. Es öffnet sich nun die Konsole.
3. Geben Sie das Kommando cipher.exe /w:C:\\ ein. C:\\ steht dabei für das Laufwerk, das bereinigt werden soll. Das Programm überschreibt nur freie Datenbereiche, d.h. Ihre Dateien werden nicht verändert! Drücken Sie <Enter>
4. Danach wird der Vorgang gestartet, was je nach Größe der Festplatte eine Weile dauern kann.

Hinweis: Bei der Benutzung dieses Tools sollte berücksichtigt werden, dass die Inhalte kleiner Dateien (unter 4 KB), die gelöscht wurden, unüberschrieben bleiben können, wenn sie direkt in der Master File Table (MFT), sozusagen dem Inhaltsverzeichnis der Festplatte, stehen. cipher.exe steht unter Windows XP Home Edition nicht zur Verfügung.

Physikalische Vernichtung von Datenträgern

Wiederbeschreibbare Datenträger, beispielsweise CD-RWs, können grundsätzlich durch vollständiges Überschreiben gelöscht werden. Theoretisch besteht jedoch die Möglichkeit, dass Spuren der alten Informationen verbleiben und rekonstruiert werden können. Bei erhöhtem Schutzbedarf müssen deshalb auch wiederbeschreibbare Datenträger mit geeigneten Geräten (Shredder) vernichtet werden, um die darauf gespeicherten Informationen unlesbar zu machen.

Optische Datenträger, beispielsweise CD-Rs, die nicht wiederbeschreibbar sind, können nicht gelöscht werden und müssen stattdessen mit geeigneten Geräten (Shredder) vernichtet werden, um die darauf gespeicherten Informationen unlesbar zu machen.

Bei defekten Festplatten, die nicht mehr überschrieben werden können, bleibt als Löschverfahren nur das Vernichten der Festplatten. Die Vernichtung kann durch Schreddern erfolgen, aber auch thermische Verfahren wie Verbrennen oder Einschmelzen sind geeignet. Magnetbandkassetten können wie Festplattenlaufwerke mechanisch oder thermisch vernichtet werden.

Löschgeräte für magnetische Datenträger

Löschgeräte dienen dazu, schutzbedürftige Daten, die auf magnetischen Datenträgern gespeichert sind, so zu vernichten, dass die Datenträger anschließend wiederverwendet werden können. Löschgeräte (Degausser) für magnetische Datenträger verfügen über einen starken Gleichfeld- oder Wechselfeldmagneten. Beim Löschen mit einem Löschgerät werden die Datenträger vom Magnetfeld des Gerätes durchflutet («Durchflutungslöschen»).

[45] Weitere informationen auf: http://support.microsoft.com/kb/315672 (Stand: 02.02.2009).

Allerdings ist zu beachten, dass Festplatten und verschiedene Magnetbänder nach dem Löschen nicht mehr verwendet werden können, weil mit den aufgezeichneten Daten auch die Servospur, mit der der Schreib-/Lesekopf gesteuert wird, gelöscht wird.

Mobile Speichergeräte, Kameras, Mobiltelefone, usw.

Ein besonderes Augenmerk sei auf Mobiltelefone und Kameras gelegt. Diese haben in der Regel eine kurze Lebensdauer und werden im Anschluss meist auch noch von Drittpersonen weiterverwendet oder weiterverkauft. Ausserdem können sich gerade auf diesen Speichermedien speziell vertrauliche Informationen wie persönliche Bilder oder Telefonnummern befinden, die man nicht gerne in fremde Hände gibt. Diese Speichermedien werden meist via USB an den Computer angeschlossen und erscheinen dort als Laufwerk. Anschliessend kann das Laufwerk mit den obengenannten Löschtools speziell überschrieben werden. Sollte sich das Gerät nicht an den Computer anschliessen lassen, bleibt nur die physikalische Vernichtung.

- Die Löschmethode hängt von der Vertraulichkeit der Daten ab.
- Ein einfaches Löschen reicht nicht aus.
- Die Daten können so wiederhergestellt werden.
- Spezielle Löschprogramme (Wipe-Tools) benutzen.
- Bei optischen Datenträgern am besten den Datenträger schreddern.

7.2 Abschalten der AutoRun Funktion in Windows

Die AutoRun-Funktion bei Speichermedien ist verantwortlich, dass beim Einlegen von Wechselmedien definierte Aktionen ausgelöst werden. Die Funktionen können die automatische Wiedergabe oder das Starten eines Kontextmenus sein. Während der automatischen Wiedergabe wird die Datei «Autorun.inf» auf dem Medium analysiert. Diese Datei legt fest, welche Befehle vom System ausgeführt werden. Viele Firmen nutzen diese Funktionalität zum Starten von Installationsprogrammen.

Typische Aktion beim Einstecken eines USB-Sticks

Die AutoRun Funktion in Windows birgt aber auch Gefahren. Immer mehr Schädlinge benutzen Flash-Speichermedien als Verbreitungsvektor. Hierbei spielt die AutoRun Funktion eine zentrale Rolle. Schaltet man diese aus, hat man schon einen erheblichen Sicherheitsgewinn. Leider ist das Abschalten nicht gerade einfach, und man muss in die Registrierungsdatenbank von Windows eingreifen. Nachfolgende Anleitung soll die nötigen Schritte dafür aufzeigen.

ACHTUNG: Die Deaktivierung der AutoRun-Funktionen funktioniert nur nach Installation eines Microsoft Windows Updates.[46]

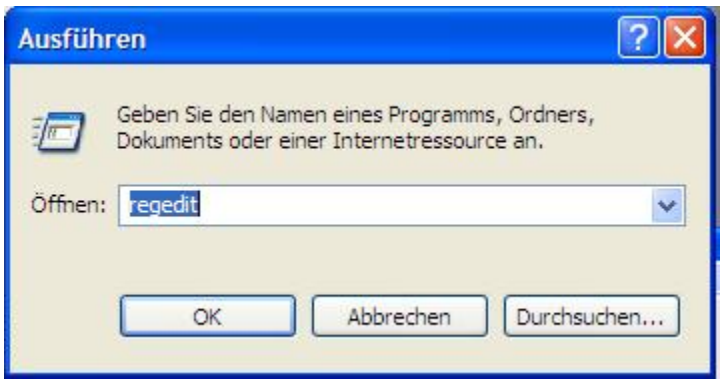
Update für Windows XP (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=c7dbcde3-7814-47c5-849e-e64ecfb35d74&displaylang=de
Update für Windows Server 2003 für Itanium-Systeme (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=99423caf-b52b-4ebc-b80c-94ee1ef9f66b&displaylang=de
Update für Windows Server 2003 x64-Edition (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=7b866fb7-9bb7-4fce-b395-d0a4ee38a115&displaylang=de
Update für Windows Server 2003 (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=32b845ac-7681-468c-812b-2dcebdae9b40&displaylang=de
Update für Windows XP x64-Edition (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=ca802f38-0566-4ac4-8808-6515623c35c5&displaylang=de
Update für Windows 2000 (KB967715)
http://www.microsoft.com/downloads/details.aspx?FamilyID=3c6039f1-d84d-4294-8457-35aa8b4dcab8&displaylang=de

Auf Windows Vista- und Windows Server 2008-Systemen muss das Update 950582 (Sicherheitsbulletin MS08-038 (http://www.microsoft.com/germany/technet/sicherheit/bulletins/ms08-038.mspx)) installiert sein, um die Registrierungs-Schlüsseleinstellungen zum Deaktivieren von AutoRun nutzen zu können.

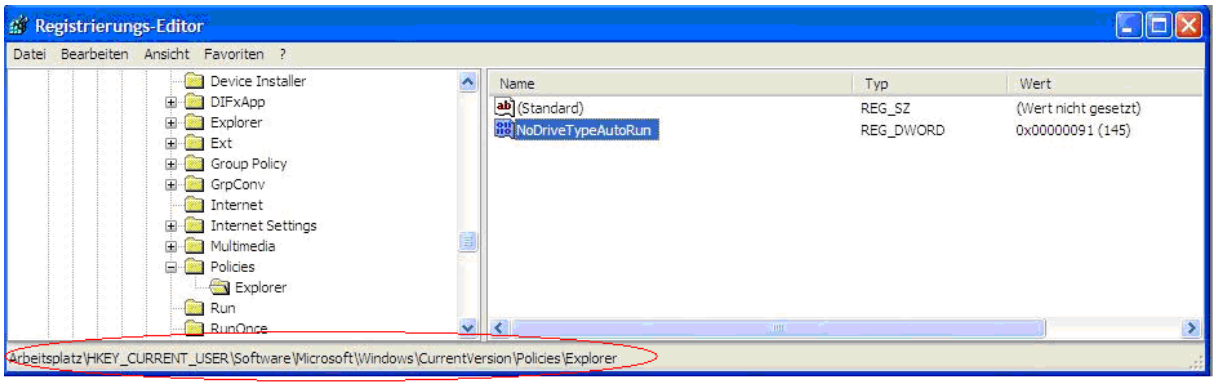
Sobald die Voraussetzungen erfüllt sind, führen Sie diese Schritte aus, um AutoRun zu deaktivieren:

Zuerst muss der Registrierungseditor gestartet werden. Hierzu geht man auf die Schaltfläche «Ausführen», tippt anschliessend «regedit» ein und drückt auf «Ok».

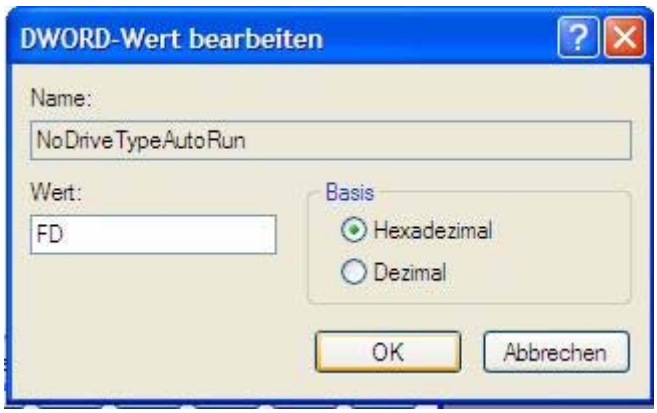
[46] Alle Informationen auf http://support.microsoft.com/kb/967715/ (Stand: 30.4.2009).



Nun muss man den entsprechenden Schlüssel «NoDriveTypeAutoRun» finden, der die AutoRun Funktion steuert. Hierzu startet man im Registrierungseditor die Suche.



Der Schlüssel (HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion \policies\Explorer\NoDriveTypeAutorun) wird so gefunden, ein entsprechender Doppelklick auf den Schlüssel öffnet das folgende Dialogfeld:



Wird der Hexadezimale Wert «FD» eingetragen, werden die AutoRun-Funktionen sämtlicher Laufwerke deaktiviert.

ACHTUNG: Diese Einstellung gilt nur für den aktuellen Nutzer.

Eine benutzerdefinierte AutoRun-Konfiguration können Sie mit Hilfe der Nachfolgenden Tabelle definieren. So können Sie genau bestimmen, welche Laufwerkstypen die AutoRun-Funktion verwenden sollen und welche nicht.

In der Tabelle sind die einzelnen Laufwerkstypen aufgeführt. Beachten Sie, dass USB-Sticks aufgrund ihrer Formatierung meist als Wechseldatenträger kategorisiert sind, USB-Festplatten hingegen als Festplatten.

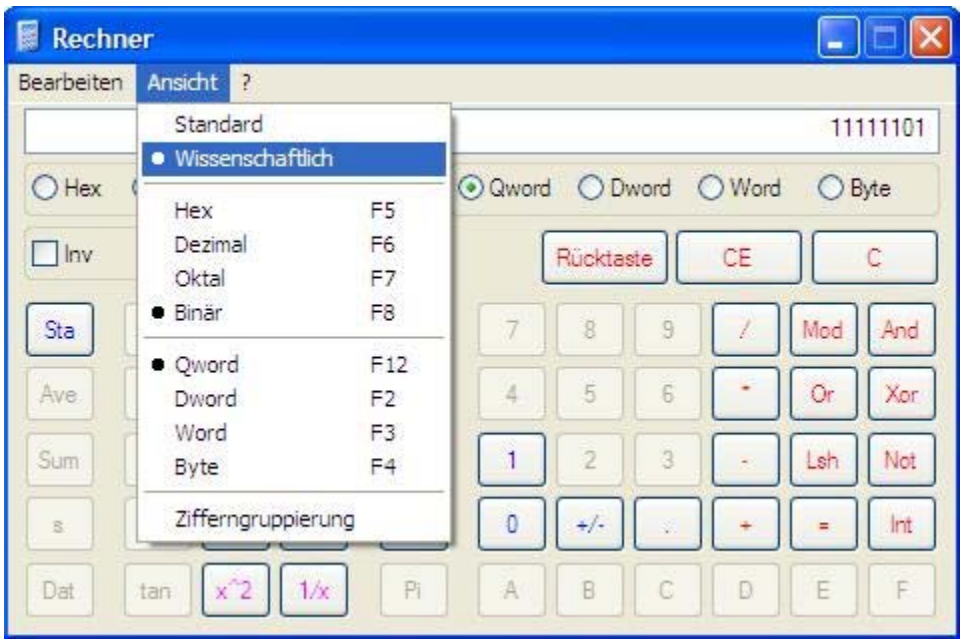
Falls Sie AutoRun aktivieren wollen, setzen Sie in der Spalte des entsprechenden Laufwerktyps eine « 0 ». Soll AutoRun nicht aktiv sein, setzen sie eine « 1 ». An den Positionen «Reserviert» und «Fremdes Laufwerk» sollte immer eine «1» stehen, bei «Laufwerk ohne Root» immer «0».

Diese Zahlen nacheinander aufgeschrieben ergeben den sogenannten Binärwert der gewünschten Konfiguration.

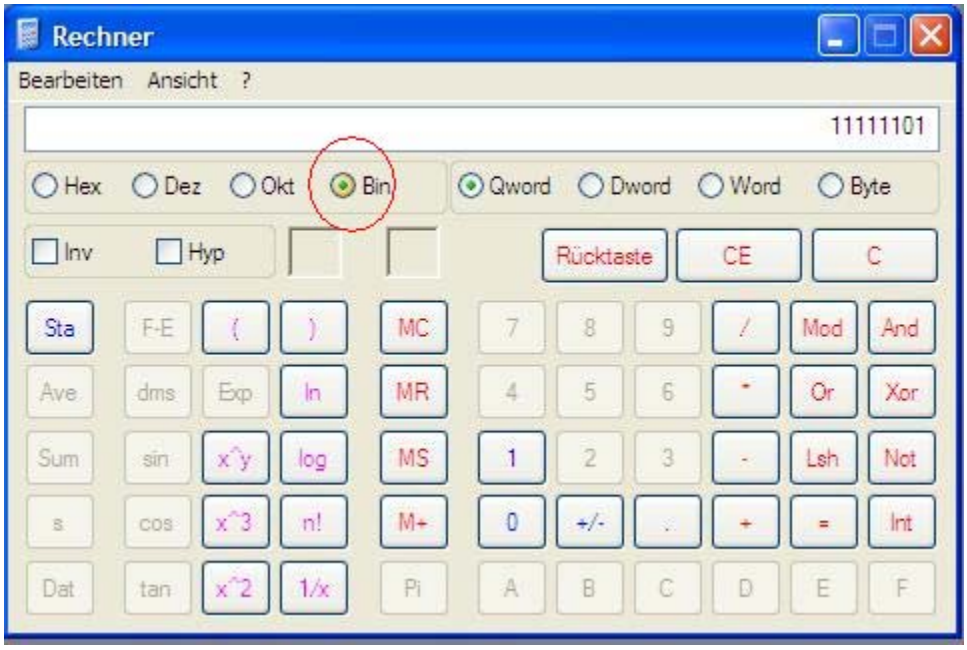
Reserviert	Ramdisk	CD-Rom Laufwerk	Netzlaufwerk	Festplatte	Wechseldatenträger	Laufwerk ohne Root	Fremdes Laufwerk	Binär-Wert
1	1	1	0	1	1	0	1	11101101
1	0	0	0	0	0	0	1	10000001
1						0	1	

Tabelle zur Generierung des Binärwertes der AutoRun-Funktion. Konfiguration 1 deaktiviert USB-Festplatten und -Sticks, Konfiguration 2 erlaubt AutoRun auf sämtlichen Laufwerkstypen. In der letzten Zeile können Sie Ihren eigenen Binärwert zusammenstellen.

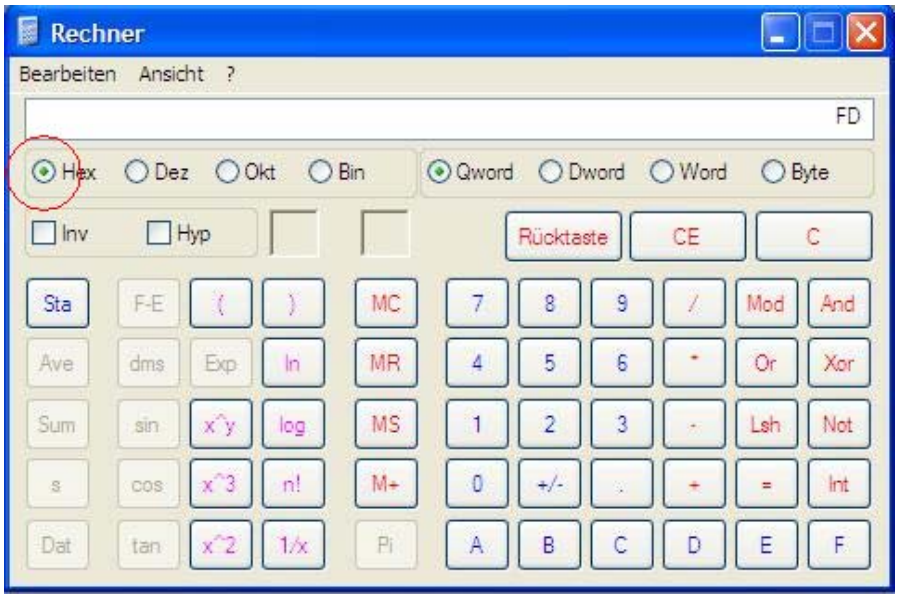
Anschliessend müssen Sie diesen Binärwert in einen Hexadezimalen Wert umrechnen. Sie können hierzu den Rechner im Wissenschaftsmodus starten.



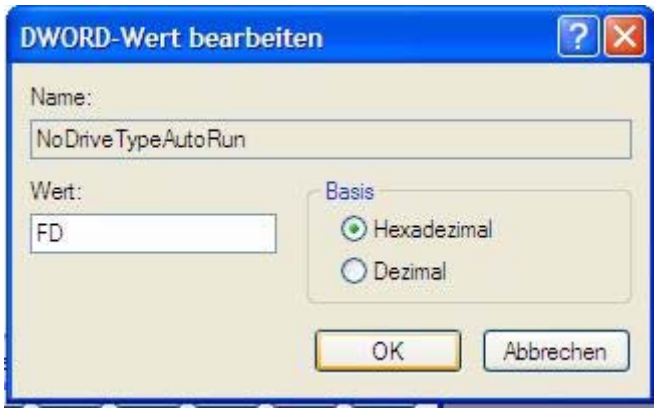
Anschliessend wählen Sie den Binär-Mode und geben den Binärwert ein, welchen Sie in obenstehender Tabelle generiert haben.



Wählen Sie nun den Hex-Mode, wird der binäre Wert automatisch umgerechnet.



Dieser Wert kann nun im Registrierungseditor eingegeben werden.



7.3 Die Lücken in DNS und MD5

Im Rahmen des 25. Chaos Communication Congress (25C3) hat eine internationale Forschergruppe - unter Mitwirkung der EPFL - gezeigt, wie bekannte Schwächen in der Kollisionsresistenz der kryptographischen Hashfunktion MD5 ausgenutzt werden können, um in den Besitz eines vertrauenswürdigen CA-Zertifikats zu gelangen (http://www.win.tue.nl/hashclash/rogue-ca/). Ein solches Zertifikat könnte z.B. eingesetzt werden, um beliebige SSL/TLS-Serverzertifikate für grossangelegte Phishing-Angriffe auszustellen. Im Wesentlichen müssen dazu zwei Zertifikatsanträge konstruiert werden: ein Antrag für ein Benutzerzertifikat und ein Antrag für ein CA-Zertifikat. Die Daten beider Anträge sind so gebildet, dass die Daten, die letztlich in die Zertifikate hineingeschrieben werden, unter MD5 kollidieren, d.h. beide Zertifikate haben den gleichen MD5-Hashwert und damit auch die gleiche Signatur. Wird das Benutzerzertifikat von einer vertrauenswürdigen CA signiert, kann mit Hilfe dieser Signatur ohne erneute Mitwirkung der vertrauenswürdigen CA das CA-Zertifikat ausgestellt werden. Dieses Zertifikat wird dann von handelsüblichen Browsern ohne Rückmeldung an den Benutzer akzeptiert.

Aus theoretischer Sicht ist das Forschungsresultat insofern interessant, als zum ersten Mal nachgewiesen worden ist, dass die seit 2004 bekannten Schwächen in der Kollisionsresistenz von MD5 für realistische Angriffe missbraucht werden können. Aus praktischer Sicht ist das Resultat weniger spektakulär, weil nur noch wenige CAs heute noch MD5 einsetzen. Dieser Trend weg von MD5 hin zu SHA-1 oder noch kollisionsresistenteren Hahsfunktionen (insbesondere SHA-2 und in Zukunft SHA-3) wird sich jetzt noch verstärken. Allerdings ist die Kollisionsresistenz der eingesetzten Hashfunktion nicht die einzige Achilles-Ferse beim Einsatz von Zertifikaten. So basieren viele Angriffe heute darauf, dass kein oder ein ähnliches aber falsches Zertifikat eingesetzt wird, und dass die Benutzer sich durch die entsprechenden Warndialoge der Browser durchklicken. Diese Angriffe sind bei deutlich niedrigeren Kosten für den Angreifer nicht viel weniger effektiv.

Anfang des Jahres 2008 entdeckte der Forscher und Spezialist für Computersicherheit Dan Kaminsky[47] eine gefährliche Lücke im DNS-System. Er kontaktierte darauf, die grössten Akteure in diesem Bereich (Microsoft, Cisco und andere), um gemeinsam mit ihnen eine Lösung für dieses Problem zu suchen. Nach sechsmonatigen Anstrengungen wurde am 8. Juli 2008 ein Patch veröffentlicht; es handelte sich hierbei um die grösste aktuelle Sicherheitsanpassung in der ganzen Geschichte des Internets.

Obwohl das DNS Cache Poisoning bereits in der Vergangenheit Probleme aufgeworfen hatte (‚die mit einem Algorithmus gelöst wurde, der die QID der Anfragen zufällig generiert), stiess Kaminsky auf eine viel besorgniserregendere Form von Cache Poisoning. Dieser Angriff konnte sich auch gegen die Authority Records richten, womit einem Cyberkriminellen potenziell ermöglicht wurde, den Informationsfluss (http, E-Mail und andere) durch eine bestimmte Zone (zum Beispiel einen Domainnamen) auf einen eigens präparierten Server «umzulenken». Zur Überwindung dieses Problems wurde die zufällige Generierung des Source ports (Ausgangstor UDP des Nameservers)[48] notwendig.

7.4 Providerdienste: Nach McColo weht der Wind von Osten

Es war der 11. November 2008 um 19:30 (EST), als laut CIDR-Bericht[49] der Provider Hurricane Electric (HE) das Routing für McColo (de-peered) unterbrach.

McColo[50] war ein amerikanischer Hostingprovider, der durch eine Vielzahl illegaler Aktivitäten, wie beispielsweise der Beherbergung von Webseiten, die Pharmaprodukte vertrieben oder von Command&Control (C&C) Servern der grössten Botnetze[51], traurige Berühmtheit erlangte. Aufgrund von Informationen, die von Informatiksicherheitsspezialisten und insbesondere vom Journalisten Brian Krebs der Washington Post[52] zusammengetragen und an

---

[47] http://www.doxpara.com

[48] Eine leicht verständliche Erklärung findet sich unter folgender Adresse (auf Englisch): http://www.unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html (Stand: 13.02.2009)

[49] http://www.cidr-report.org/cgi-bin/as-report?as=AS26780 (Stand: 17.12.2008)

[50] http://web.archive.org/web/*/http://www.mccolo.com/

[51] http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html (Stand: 17.12.2008), jüngster Bericht über McColo von Hostexploit.com: http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf (Stand: 17.12.2008)

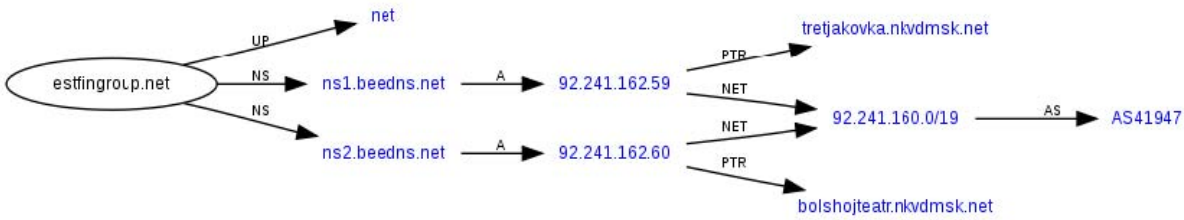
[52] http://voices.washingtonpost.com/securtiy/2008/11/major_source_of_online_scams_a.html (Stand: 17.12.2008)

den Upstream Provider HE von McColo übermittelt wurden[53], beschloss dieser seinem Kunden «den Stecker zu ziehen». Derselbe Krebs veröffentlichte am Tag darauf einen Artikel, in dem der drastische weltweite Rückgang des Spamvolumens aufgezeigt wurde[54].

Nachdem McColo vom Netz getrennt wurde, stellte sich die Frage nach den mittelfristigen Konsequenzen dieses Schrittes. Kurzfristig, das heisst in den Tagen nach dem Depeering, registrierten zwar verschiedene Quellen eine weltweite, spürbare Verringerung des Spamvolumens; mittelfristig, das heisst nach einigen Wochen, wurden jedoch neue Aktivitäten registriert[55]. Diese wurden nun nicht mehr im Westen (Vereinigten Staaten) sondern im Osten, beispielsweise in den Ländern Russland oder Estland[56] beobachtet.

Die Botnetze sind nicht die Einzigen, die in Russland und dessen Nachbarstaaten eine neue Heimat fanden. Ende November 2008 wurde die Schweiz von einer Spamwelle überrollt, in denen Personen für das Waschen von Geld angeworben wurden. Das zu waschende Geld stammte dabei von Schweizer E-Banking-Betrügereien[57]. Unterschrieben waren die E-Mails von der imaginären Firma *estfingroup.net*.

Die URL *estfingroup.net* weist als Name Server *beedns.net* unter den Adressen 92.241.162.59 und 92.241.162.60 auf. Das Routing dieser Adressen führt zu AS41947, das der Firma Webalta Wahome Networks gehört.



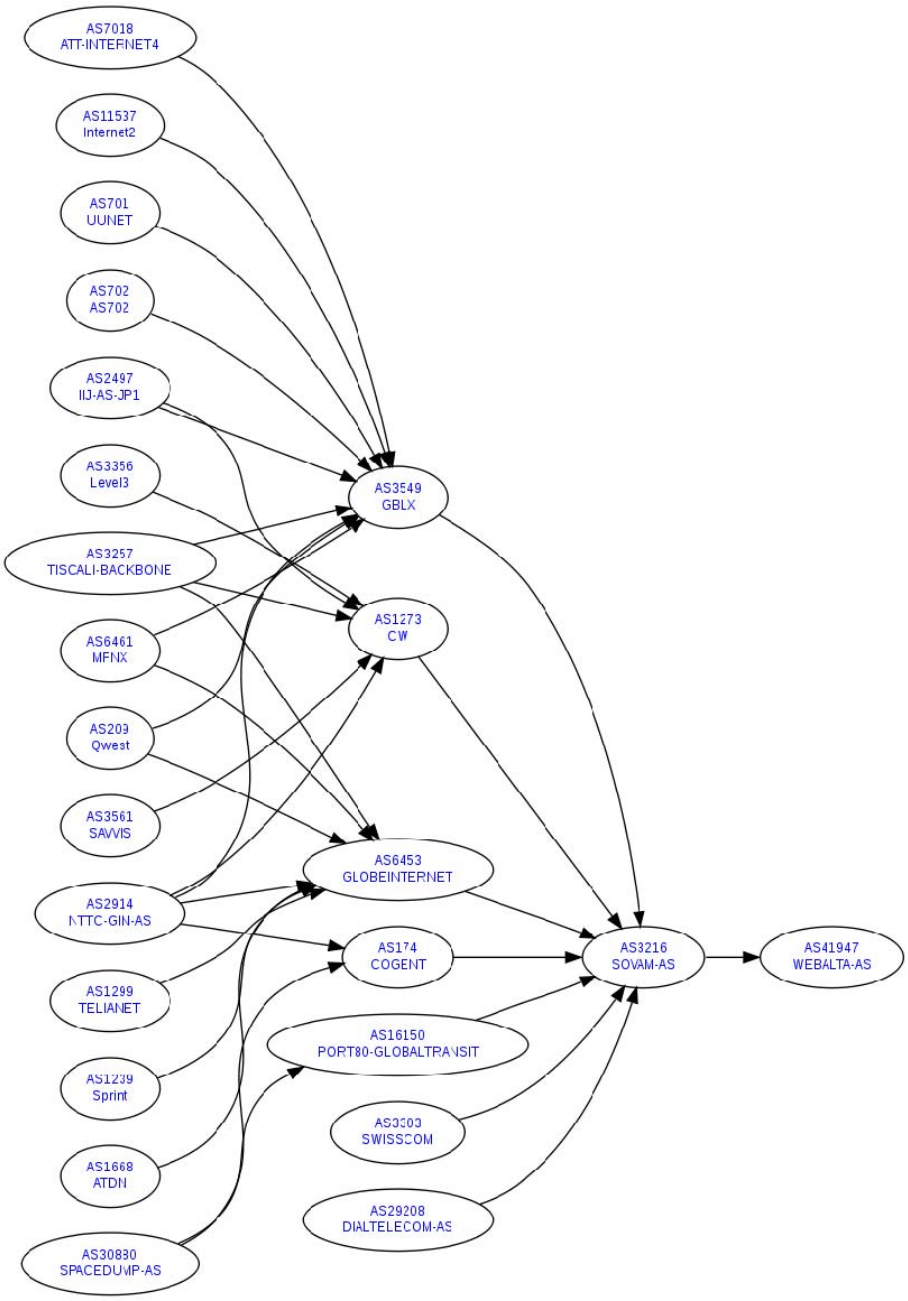
[53] http://www.secureworks.com/research/threats/warezov/ (Stand: 17.12.2008), http://blog.fireeye.com/research/2008/10/mccolo-hoting-srizbi-cc.html (Stand: 17.12.2008), http://www.threatexpert.com/report.aspx?uid=745bcad4-9f9d-4a32-ba95-7cb7d5fc14f8

[54] http://voices.washingtonpost.com/security/2008/11/spam_volumes_drop_by_23_after.html (Stand: 17.12.2008), http://www.securityfocus.com/brief/855 (Stand: 17.12.2008)

[55] http://www.theregister.co.uk/2008/11/18/short_mccolo_resurrection/ (Stand: 17.12.2008)

56 http://blog.fireeye.com/research/2008/11/rustocks-new-home.html (Stand: 17.12.2008) und http://blog.fireeye.com/research/2008/11/its-srizbi-trun-now.html (Stand: 17.12.2008)

[57] http://www.melani.admin.ch/dienstleistungen/archiv/01073/index.html?lang=de (Stand: 16.02.2009)



Webalta.ru ist ein russischer Service Provider, der zahlreiche kriminelle Aktivitäten beherbergt. Diese Firma besitzt gegenwärtig bei Spamhaus rund ein Dutzend SBL Advisories (SBL59981, SBL64756, SBL66771, SBL69825, SBL70442, SBL70445, SBL71946, SBL71948, SBL71955, SBL71957, 72319, SBL72604, SBL72607), vor allem für das Hosting von Botnet C&C, Drop-Servern verschiedener Malware, Spam-Versand und infizierten Website. Nach kurzer Suche stösst man auf verschiedene Ergebnisse in Bezug auf die kriminellen Domains, die auf Webalta untergebracht sind[58]. In der nachstehenden Liste werden einige Beispiele aufgeführt:

[58] http://www.spamhaus.org/sbl/sbl.lasso?query=SBL69825 (Stand: 16.02.2009), http://msmvps.com/blogs/hostsnews/archive/2008/11/10/1653730.aspx (Stand: 16.02.2009), http://www.forumpostersunion.com/showthread.php?t=3356 (Stand: 16.02.2009),

77.91.229.38 try-count .net
77.91.229.55 v2statscount .net
77.91.229.55 v2count .net
77.91.229.55 pluscount .net
77.91.229.55 newv2count .net
92.241.163.27 adv-a-v .com
92.241.163.27 a-a-v-2008 .com
92.241.163.27 aav2008 .com
92.241.163.30 wi-a-v .com
92.241.163.30 wav2008 .com
92.241.163.30 windows-av .com
92.241.163.31 uav2008 .com
92.241.163.32 spypreventers .com
92.241.163.32 sp-preventer .com
92.241.163.33 download.wi-a-v .com
92.241.163.33 download.wav2008 .com
92.241.163.33 download.uav2008 .com
92.241.163.33 download.adv-a-v .com
92.241.163.33 download.a-a-v-2008 .com
92.241.163.33 download.aav2008.com
92.241.163.33 download.windows-av .com
92.241.163.33 download.spypreventers .com
92.241.163.33 download.sp-preventer .com
92.241.163.34 secure2.softpaydirect .com
92.241.163.34 secure.softpaydirect .com
92.241.163.90 piterserv .com
91.208.0.220 rapidantivirus .com
91.208.0.223 microantivirus-2009 .com
91.208.0.223 microantivirus2009 .com
91.208.0.223 microantivir2009 .com
91.208.0.223 microantivir-2009 .com
91.208.0.223 micro-antivir-2009 .com
91.208.0.224 soft-traff6 .com
91.208.0.224 soft-traff5 .com
91.208.0.224 soft-traff4 .com
91.208.0.224 soft-traff3 .com
91.208.0.224 soft-traff2 .com
91.208.0.224 soft-traff .com
91.208.0.228 scanner.ms-scanner .com
91.208.0.228 scanner.msscanner .com
91.208.0.228 scanner.ms-scan .com
91.208.0.229 msantivirus-xp.com
91.208.0.239 winxsecuritycenter .com
91.208.0.240 download.vav2008 .com
91.208.0.240 vav2008 .com
91.208.0.241 winsafer .com
91.208.0.244 software-traffic .com
91.208.0.244 software-traff .com
91.208.0.246 scanner.vav-x-scanner .com
91.208.0.246 scanner.vav-scanner .com
91.208.0.246 scanner.vav-scan .com
91.208.0.246 scanner.vavscan .com
91.208.0.246 scanner-pwrantivirus .com
91.208.0.249 watcher-scan .com
91.208.0.249 scanner2.defender-scan .com
91.208.0.251 scanner.win-x-defenders .com
91.208.0.251 win-x-defenders .com
91.208.0.251 win-x-defender .com

Obwohl das Depeering von McColo von vielen als Erfolg gewertet wurde, bleibt noch viel zu tun. Wir haben aufgezeigt, wie es den Akteuren krimineller Aktivitäten gelang, sich innerhalb weniger Tage von einem herben Rückschlag zu erholen. Obwohl es selbstverständlich erscheint, muss man doch darauf hinweisen, dass die internationale Zusammenarbeit das einzige Mittel ist, um diese Art von Verbrechen zu bekämpfen. Initiativen wie diejenigen von ICANN, die dazu dienen, das bestmögliche Vorgehen bei der Bekämpfung illegaler Fast-flux-Netze[59] zu beurteilen, verdienen Unterstützung: Zusammenarbeit ist der einzige gangbare Weg.

[59] http://www.icann.org/en/public-comment/#ff-initial (Stand: 16.02.2009)