Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

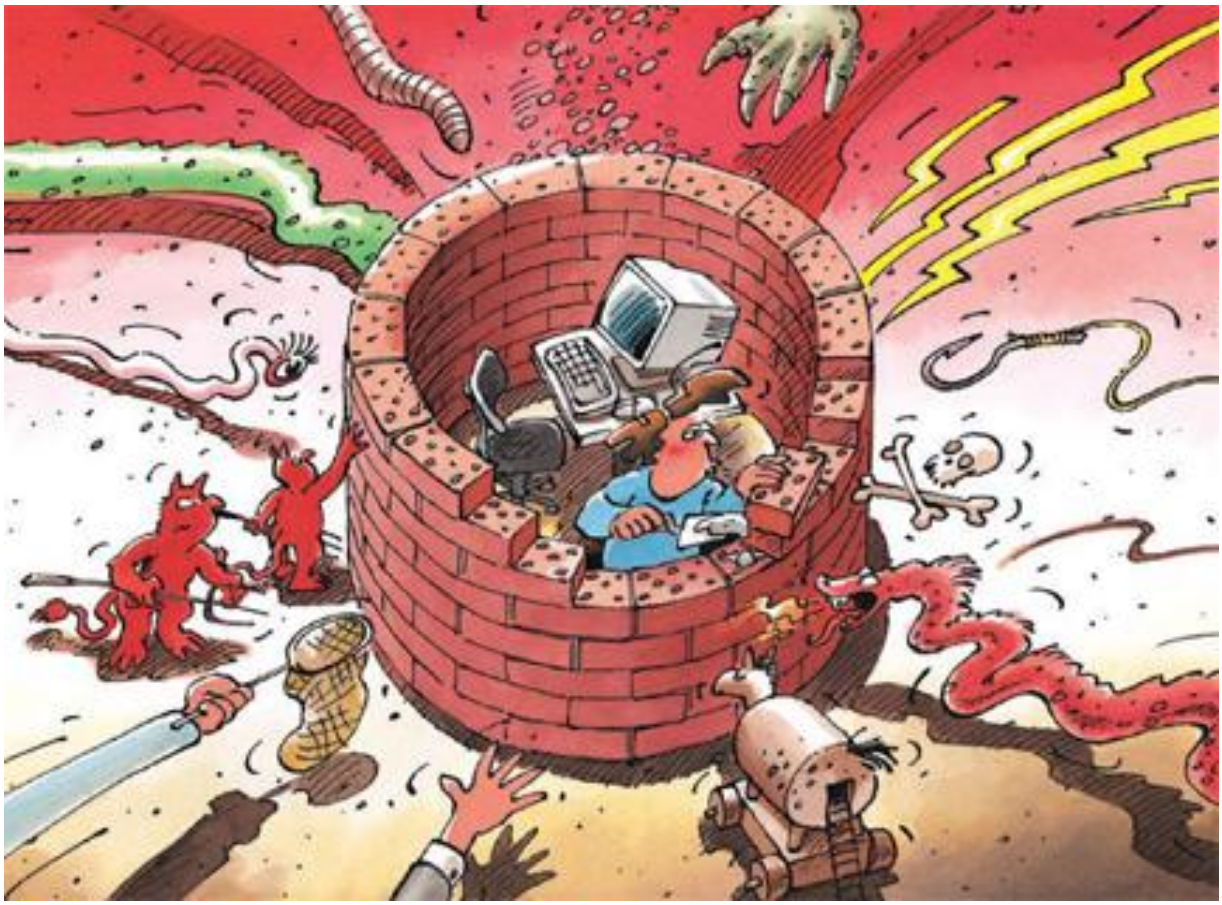
Informatikstrategieorgan Bund ISB
Dienst für Analyse und Prävention DAP

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2009/I (Januar – Juni)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2009/I

- **Drive-By Infektionen auf dem Vormarsch**
  Wie schon in den letzten Halbjahresberichten angedeutet, zeichnet sich eine Verlagerung der Angriffsvektoren (von E-Mails mit Anhang oder Links) zu Webseiteninfektionen – sogenannten Drive-By Infektionen – ab. Die klassischen Wege der Malware-Verbreitung funktionieren wohl deshalb nicht mehr so gut, weil die Anwender sensibler reagieren und seltsam anmutende Anhänge seltener geöffnet werden. Laut Angaben der Sicherheitsfirma Scansafe wurde 74 Prozent der Schadsoftware im dritten Quartal 2008 über Webseiten verteilt.
  ► Aktuelle Lage Schweiz: Kapitel 3.2
  ► Tendenzen 5.4
  ► Abwehrmassnahmen Anhang 7.2

- **Diskussion um Sicherheit von SCADA Systemen immer breiter geführt**
  Die Überwachung, Kontrolle und Steuerung von Industrieanlagen, von Systemen zur Verteilung lebenswichtiger Güter (Strom, Wasser, Brennstoffe, usw.) oder im Bereich des Transports und Verkehrs (Eisenbahnen, Verkehrsleitsysteme, Post, usw.) sind ohne den Einsatz von Informations- und Kommunikationstechnologie (IKT) seit Langem undenkbar. Die Entwicklung und der Betrieb entsprechender Überwachungs-, Kontroll- und Steuerungssysteme (engl. Supervisory Control and Data Acquisition, SCADA) hat lange Tradition. Die Diskussion um Sicherheit von SCADA Systemen wird deshalb immer breiter geführt. Es ist klar, dass solche Systeme für das Funktionieren unserer Gesellschaft zentral sind. Gefahren gehen aber nicht nur von Hacker-Angriffen (Sabotage), sondern auch von technischen Störungen aus.
  ► Aktuelle Lage Schweiz: Kapitel 4.3
  ► Tendenzen 5.2

- **Cloud Computing und das Information Ownership**:
  Am 17. Mai 2009 hat das Schweizer Wahlvolk mit denkbar knappen 50,1 Prozent der Einführung biometrischer Pässe zugestimmt. Neben datenschützerischen Bedenken schien dabei vor allem auch ein im Bereich der Informationssicherung fussendes Argument für den knappen Ausgang entscheidend gewesen zu sein.
  ► Tendenzen 5.1

- **Vorschussbetrug und Abofalle**
  Immer noch werden MELANI und KOBIK täglich verschiedenste Vorfälle betreffend Vorschussbetrug, angeblichen Lottogewinnen und Gratisangeboten gemeldet. Anscheinend ist diese Art von Internetkriminalität immer noch zu erfolgreich.
  ► Tendenzen 5.2

- **Conficker**
  Der Computer-Wurm Conficker war im vergangenen Halbjahr eines der IT-Hauptthemen in den Medien. Besonders rund um den 1. April 2009, dem Datum, an welchem sich der Wurm hätte updaten sollen, war das mediale Interesse enorm. Eigentlich hat niemand mehr mit einem solchen Wurmausbruch gerechnet, trotzdem war Conficker in der Verbreitung äusserst erfolgreich.
  ► Kapitel 4.2

2 Einleitung

Der neunte Halbjahresbericht (Januar – Juni 2009) 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 Themen 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.

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 ersten Hälfte des Jahres 2009 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

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

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

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Gozi - neuer Trojaner mit Spam-E-Mails verbreitet

Bereits im Dezember 2008 versuchten Cyberkriminelle mit der Trojanerfamilie Gozi alias Infostealer.Snifula in der Schweiz Fuss zu fassen. Es handelte sich dabei um die dritte E-Banking Trojanerfamilie, die Kunden von Schweizer Finanzinstituten im Visier haben.

Mit einer Spam-E-Mail zweideutigen Inhalts[1] wurde damals versucht, potentielle Opfer auf verschiedene präparierte pornografische Internetseiten zu locken. 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. In diesem Flash Plug-In versteckte sich der E-Banking-Trojaner.

Im Januar dieses Jahres wurden nun diverse Spamwellen beobachtet, welche die Verteilung des gleichen Trojaner-Typs zum Ziel hatten. Dabei wurde jeweils auf eine gefälschte Seite der Gratiszeitung «20 Minuten» verlinkt. Die Seite wurde 1 zu 1 vom Original kopiert und war demzufolge nur auf Grund der Webadresse als Fälschung zu erkennen. Auszüge des 20 Minuten-Artikels wurden auch im Spam-E-Mail verwendet. Aus diesem Grund war jener Teil des E-Mails auch in korrektem Deutsch. Die veränderten, respektive hinzugefügten Teile waren allerdings fehlerhaft.
Die Titel nahmen unter anderem Bezug auf die Ausdehnung der Personenfreizügigkeit auf Bulgarien und Rumänien. Da es sich dabei um spezifische Schweizer Themen handelt, lässt dies auf eine sehr gezielte Verbreitung der E-Mails schliessen.

Von: ZURICH Kontakt [mailto:alarm@20min.ch]
Betreff: ZURICH ALARM:2007 wurden erst 203 Einsteigerinnen aus den osteuropaischen Staaten registriert.

ZÜRICH

50 Prozent mehr Ost-Prostituierte
Die Zahl der Prostituierten aus Osteuropa wächst rasant: Von dort stammt fast die Hälfte der Frauen, die 2008 von der Stapo Zürich neu registriert worden sind.

Bis ins Einzelne> >
Mit den herzlichen Grüßen, Roseann Mansfield.

Spam E-Mail zum Thema Personenfreizügigkeit

[1] http://www.melani.admin.ch/dienstleistungen/archiv/01074/index.html?lang=de (Stand: 21.08.2009).

Gefälschte Seite der Newszeitung 20 Minuten. Um das Video zu sehen wird man aufgefordert, ein Flash Plug-In zu installieren.

Der 20 Minuten-Artikel, auf den das Spam-E-Mail Bezug nahm und dessen Text das Spam-E-Mail verwendete, wurde am Sonntagabend um 22:18 Uhr publiziert. Am Montagmittag wurden die Spam-E-Mails bereits versendet. Die Spamwellen wiederholten sich dann am Dienstag und Mittwoch. Der Inhalt war jeweils identisch, allerdings waren die Domänen, unter welchen die Seiten erreichbar waren, bei jeder Welle anders. Die Seiten waren auf einem so genannten «*Fast Flux Netzwerk*» gehostet, was bedeutet, dass eine Seite redundant auf mehreren Servern gespeichert ist[2]. Fällt ein Server aus, wird die Anfrage automatisch auf den nächsten weitergeleitet. So wird eine Deaktivierung erschwert und in der Folge die Zeit verlängert, in welcher ein Angriff erfolgreich ausgeführt werden kann. Registriert wurden die Domänen allesamt bei einem Registrar in China. Dieser Umstand gibt jedoch keine Hinweise auf die Herkunft der Täter.

Hierbei handelte es sich um die vorläufig letzten grossen E-Mail-Wellen, die E-Banking Trojaner verteilt haben. Anscheinend waren Kosten und Nutzen nicht mehr im Einklang, da die Ausbeute an kompromittierten Computern bei Spamwellen zu klein war. Insgesamt gingen die Angriffe mit E-Banking Trojanern ab Januar stark zurück. Die Angreifer wechselten vermehrt auf andere Geschäftsmodelle wie beispielsweise *Rogue-Software*. *Rogueware* ist eine Malware, die vorgibt, Schädlinge auf dem Computer gefunden zu haben, diese aber nur in seiner kostenpflichtigen Version entfernen zu können. Ausserdem wird vermehrt auf den Angriffsvektor *Drive-By Infektion* gesetzt. (Siehe hierzu Kapitel 3.2.) Erweiterte Informationen zu Fast Flux Netzwerken finden Sie im MELANI-Halbjahresbericht 2/2007.[2]

[2] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand:21.08.2009)

3.2 Drive-By Infektionen auf dem Vormarsch

Wie schon in den letzten beiden Halbjahresberichten angedeutet, zeichnet sich eine Verlagerung der Angriffsvektoren (von E-Mails mit Anhang oder Links) zu Webseiteninfektionen – sogenannten Drive-By Infektionen – ab. Die klassischen Wege der Malware-Verbreitung funktionieren wohl deshalb nicht mehr so gut, weil die Anwender mittlerweile sensibler reagieren: Es wird nicht mehr auf jeden, per E-Mail erhaltenen Link, geklickt und seltsam anmutende Anhänge werden weniger geöffnet. Laut Angaben der Sicherheitsfirma Scansafe[3] wurden im dritten Quartal 2008 bereits 74 Prozent der Schadsoftware über Webseiten verteilt. In einem Report der Firma Websense wird angegeben, dass 70% der 100 populärsten Seiten zumindest kurzzeitig Schadsoftware enthielten oder von Cyberkriminellen für deren Aktivitäten benutzt wurden.[4] [5]

Bei Drive-By Infektionen spielen Suchmaschinen eine nicht zu unterschätzende Rolle. Es wird unter Anderem versucht, Webseiten zu kompromittieren, welche bei populären Suchbegriffen ein hohes Ranking haben und zusätzlich schlecht geschützt sind oder Sicherheitslücken aufweisen. Manchmal enthält die Drive-By Infektion auch eine Auswertung des *Referrers*: Die Drive-By Infektion wird in diesen Fällen nur eingeblendet, wenn via eine Suchmaschine auf die betroffene Seite zugegriffen wird. Der Webseitenadministrator, der die Seite in den meisten Fällen direkt aufruft, entdeckt die Kompromittierung der Seite somit nur schwer. Bei der unter dem Namen Gumblar bekannt gewordenen Drive-By Attacke, die im Mai dieses Jahres beobachtet worden ist, manipuliert der Trojaner die im Browser des Opfers angezeigten Ergebnisse bei Google-Suchen. Das Opfer wird dadurch verleitet, auf andere gefährliche Seiten zu surfen und das Risiko einer weiteren Infektion wird drastisch erhöht.

Die Entwicklungen auf dem Gebiet der Drive-By Infektionen sind bemerkenswert (siehe Kapitel 5.4 Tendenzen). Was indes für jeden Drive-By Angriff identisch ist, ist die Tatsache, dass zuerst ein geeigneter Webserver gefunden werden muss, über welchen die Infektion verbreitet werden kann. Die Angreifer hacken sich deshalb in bestehende Webserver, um dort ihren schädlichen Code zu platzieren. Sie verwenden dazu gestohlene *FTP*-Passwörter oder nutzen Sicherheitslücken in der Server-Software aus. Besonders gefährdet sind hierbei die *Content Management Systeme (CMS)* – aber auch Foren und Gästebücher sowie die dazugehörigen Datenbanken bieten Angriffsflächen. Erwähnenswert ist hierzu, dass beim Ausnützen einer Sicherheitslücke meist nicht nur ein einzelner Webauftritt betroffen ist, sondern in der Regel auch noch andere Seiten, die auf diesem Webserver gehostet werden, in Mitleidenschaft gezogen werden.

Der Angriff selber erfolgt in mehreren Schritten. Auf der gehackten Seite befindet sich ein *Code*, der den Besucher im Hintergrund auf einen Drittserver umleitet. Dies geschieht in den meisten Fällen via *IFrame*, das oft über ein *Javascript* generiert wird. In Zukunft ist auch vermehrt mit automatischen Weiterleitungen, so genannten *META-Refreshes*, zu rechnen (siehe Tendenzen, Kapitel 5.4). Die Verschleierung mit Javascript hat zum Ziel, die Erkennung solcher Infektionen (beispielsweise durch Antivirenprogramme) zu erschweren. Mittlerweile werden aber auch direkt IFrames auf der Seite platziert, da dies auf Grund der breiteren Sensibilität auf Javascript als Angriffsvektor fast weniger auffällig ist. Sobald das Opfer umgeleitet ist, wird in mehreren Schritten geprüft, was für Programme auf dem

---

[3] http://www.scansafe.com/resources/global_threat_reports2/gtr_2008/Q3_2008_GTR.pdf (Stand: 31.08.2009).

[4] http://securitywatch.eweek.com/exploits_and_attacks/most_popular_sites_were_hacked_in_08.html (Stand: 31.08.2009).

[5] http://securitylabs.websense.com/content/Assets/WSL_ReportQ3Q4FNL.PDF (Stand: 31.08.2009).

Rechner installiert sind und ob es sich dabei um eine nicht aufdatierte Version handeln könnte, welche eine Sicherheitslücke aufweist. Ist dies der Fall, wird dem Computer eine auf dieses Sicherheitsloch zugeschnittene Malware präsentiert, welche das System in der Folge infiziert. Solche Sicherheitslücken betreffen keineswegs nur den Browser selbst, sondern insbesondere auch die dazugehörigen *Browser-Plug-Ins* wie Flash und Acrobat-Reader oder eine kritische Lücke im *ActiveX Control* Element usw. Sollte sich keine passende Sicherheitslücke finden, wird man schliesslich vielfach aufgefordert, das Schadprogramm manuell zu installieren.

Die Techniken, Drive-By Infektionen so lange wie möglich unerkannt auf einer Webseite platzieren zu können, verbessern sich in rasantem Tempo. Diese Entwicklung wird in Kapitel 5.4 aufgezeigt.

Um Ihren Computer gegen Drive-By Infektionen zu wappnen, lesen Sie das Kapitel „Browsereinstellungen zum Schutz gegen gängige Drive-By Infektionen“ im Anhang 7.2.

3.3 Missbrauch von Schweizer E-Mail-Konten

Im letzten Halbjahresbericht hat MELANI erläutert, dass Zugangsdaten zu Internetdiensten vermehrt im Visier der Cyberkriminellen stehen. Dabei ging es vor allem um das Platzieren von Drive-By Infektionen auf Webseiten, respektive den Missbrauch von Auktionskontos. Auch angesprochen wurden Phishing-Versuche gegen E-Mail-Dienstleister wie Bluewin, Hotmail usw. Nicht erläutert wurde, was mit einem gestohlenen E-Mail Konto alles angestellt werden kann. Viele werden sich sagen, dass es ihnen eigentlich egal ist, wenn ein Dritter auf ihre E-Mails zugreift, und dass die E-Mails, die sie erhalten, nicht wirklich vertraulich sind. Doch dahinter steckt mehr: Natürlich ist auch hier der Antrieb der Kriminellen das Geld. Ein realer Schweizer Fall zeigt, wie man mit gestohlenen E-Mail Logindaten zu Geld kommen kann:

Im Juni 2009 wurde mit gestohlenen Zugangsdaten auf ein E-Mail Konto eines Schweizer Bürgers zugegriffen und an all seine 350 Kontakte ein E-Mail versendet, dass er sich auf seiner angeblichen Reise in Afrika in Schwierigkeiten befinde. Sein Pass, das ganze Geld und auch sämtliche anderen Dokumente seien gestohlen worden. Um überhaupt aus dem Hotel abreisen zu können, benötige er dringend 1’000 Euro für die Hotelrechnung plus 100 Euro für die ausstehende Telefonrechnung. Der Betrag werde selbstverständlich vollumfänglich zurückerstattet, sobald er sich wieder in der Schweiz befinde. Das Geld solle via Western Union nach Abidjan an eine dem E-Mail-Empfänger unbekannte Person überwiesen werden. Die telefonische Erreichbarkeit sei auf Grund der Umstände nicht möglich.

In diesem Fall kam es dank der Skepsis der Adressaten, die vor einer allfälligen Überweisung unbedingt eine telefonische Bestätigung des angeblich in Not geratenen Freundes einholen wollten, sowie der Avisierung von Western Union zu keinem Schaden.

Fazit ist, dass nicht allein das E-Mail Konto einer Person von Interesse ist, sondern vielmehr die Kontakte, die eine einzelne Person unterhält. In Zukunft werden nicht nur E-Mail-Adressen gesammelt, sondern auch deren Kontakte zu anderen Personen akribisch genau aufgelistet. Das Ziel dabei ist, ein E-Mail auf ein potentielles Opfer so gut wie nur möglich zuzuschneiden. Da der entsprechende Aufwand gross ist, hat man dies bis anhin nur vereinzelt bei sehr gezielten Angriffen beobachtet. Werden diese Verknüpfungen aber automatisch und im grossen Stil zusammengetragen, verkleinert sich der Aufwand und es ist damit zu rechnen, dass diese Technik auch bei «ungezielten» Angriffen verwendet wird. Dies mit der immerwährenden Absicht, das Opfer zu verleiten, auf einen Anhang zu klicken oder eine andere Aktion auszuführen. Es gilt dann nicht mehr nur bei E-Mails von

unbekannten Personen kritisch zu sein, sondern auch bei bekannten Absendern Vorsicht walten zu lassen. Bei ungewöhnlichen Vorkommnissen – insbesondere wenn es um Geld geht – empfiehlt MELANI, die telefonische Erreichbarkeit zu überprüfen, durch Fragen, welche nur diese Person beantworten kann, ihre Identität zu verifizieren, oder die Glaubwürdigkeit der erzählten Geschichte mit gemeinsamen Bekannten zu besprechen.

3.4 Unterbruch von Internet und Telefon bei Cablecom

Ein *DDoS Angriff* gegen einen Cablecom Kunden führte am 19. Januar 2009 zu einer Störung auf dem Cablecom Netz während gut einer Stunde. Der Internetverkehr hatte sich um mehrere Gigabit/Sekunde erhöht. Internet- sowie Telefoniedienste im Grossraum Zürich und Umgebung, aber auch in anderen Regionen, waren deshalb eingeschränkt oder nicht verfügbar. Cablecom hatte in der Folge den Internetverkehr über eine alternative Internetanbindung in das internationale Netz umgeleitet. Danach konnte der angreifende Verkehr an den Eingangspunkten des Cablecom *Backbone* sowie des internationalen Internetbackbone unterbunden werden. Knapp ein Drittel der Kunden im Grossraum Zürich, rund 90'000 Anschlüsse, waren laut Angaben der Cablecom betroffen. Diese konnten zwischen 12.50 und 13.50 Uhr nicht oder nur erschwert telefonieren oder das Internet nutzen.

In der Schweiz sind schon verschiedene DDoS-Angriffe verzeichnet worden. Besonders oft werden Webseiten mit pornografischen Inhalten attackiert.[6] Im Dezember 2007 wurde beispielsweise die Website www.sexy-tipp.ch über ein *Bot-Netz* angegriffen (siehe[7]). Aber auch andere Websites, die mit dem Zürcher Bordellmilieu in Verbindung stehen, erlitten dasselbe Schicksal. Bei solchen Angriffen werden oft auch andere Webseiten, die auf dem gleichen Server gehostet werden, in Mitleidenschaft gezogen – meist wird jedoch das ganze Netz gestört. Ob es sich beim Angriff auf Cablecom um einen ähnlichen Hintergrund handelt, ist nicht bekannt. Cablecom hat bei der Polizei Anzeige erstattet.

3.5 Gezielte E-Mails mit Schadsoftware gegen grössere Firmen

Im ersten Halbjahr 2009 wurde eine sehr gezielte Angriffswelle[8] beobachtet, die gegen Kader von grösseren Firmen gerichtet waren. Die E-Mails waren in englischer Sprache verfasst und gaben vor, dass ein Zahlungsauftrag ausgelöst worden war und man das angehängte Dokument «details.rtf» nun auf seine Richtigkeit überprüfen soll. Beim Öffnen dieser Datei wurde dann die Schadsoftware installiert.

[6] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (Stand: 31.08.2009)

[7] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand: 31.08.2009)

[8] http://isc.sans.org/diary.html?storyid=6511 (Stand: 31.08.2009)

Ein Beispiel-E-Mail sieht folgendermassen aus:

Subject: Re: Wire Transfer <Vorname Name des Empfängers>

The wire transfer has been released.

BENEFICIARY : <Vorname Name des Empfängers>
ABA ROUTING# : XXXX92729
ACCOUNT# : XXX-XXX-XXX25
AMMOUNT : $19,438.16

Please check the wire statement attached and let me know if everything is correct. I am waiting for your reply.
Laura

Die Analyse der Malware hat ergeben, dass alle via Windows-Explorer besuchten Verzeichnisse, alle mit dem Browser besuchten Webseiten und alle eingegebenen Formulardaten aufgezeichnet und an diverse Server geschickt werden. Diese, in der Schadsoftware fix programmierten Server, konnten identifiziert und deaktiviert werden. International wurden ähnliche Wellen beobachtet. Wie viele dieser E-Mails versendet wurden, ist aber nicht bekannt. Die E-Mails waren dabei praktisch ausschliesslich an Mitarbeitende der Firmenkader gerichtet, was auf einen sehr gezielten Angriff schliessen lässt. Es gab anscheinend Ende Dezember 2008 schon andere Spam-Wellen[9] [10], die den gleichen Wortlaut enthielten. Diese hatten jedoch einen anderen Anhang (bank_statement.scr oder bank_statement.zip) und wurden anscheinend auch nicht so gezielt versendet. Wer hinter dieser Welle steckt und was für ein Ziel damit verfolgt wurde, ist nicht bekannt.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 IT-Spionage auf tibetische NGOs und das Büro des Dalai Lama

Am Wochenende vom 29. März 2009 berichteten mehrere Medien über eine kanadische-Studie zum Thema chinesische IT-Spionage mit dem Titel «Tracking GhostNet - Investigating a Cyber Espionage Network».[11] Dabei handelt es sich um die Resultate einer Untersuchung zu IT-basierten Angriffen auf vor allem tibetische Non Governmental Organizations und das Büro des Dalai Lama, welche weitere infizierte Systeme in über 100 Ländern zur Folge hatten. Darunter befanden sich auch Systeme in Unternehmen und Regierungsstellen.

[9] https://tools.cisco.com/security/center/viewAlert.x?alertId=17321 (Stand: 31.08.2009)
[10] http://fordhamsecureit.blogspot.com/2008/12/wire-transfer-phishing-email-sent-to.html (Stand: 31.08.2009)
[11] http://www.news.utoronto.ca/media-releases/international-affairs/information-warfare-monitor.html (Stand: 31.08.2009)

Bereits 2007 wurden vertrauliche Berichte des Chefs des britischen MI5 publik[12], in denen vor gezielten Spionageangriffen mit ausgeklügelten *Social-Engineering-Methoden* unter Einsatz von massgeschneiderten Trojanischen Pferden gewarnt wurde. Unter anderem seien *kritische nationale Infrastrukturen* und Regierungsstellen im Visier chinesischer Angreifer. Auch in der Schweiz haben sich seitdem solche Angriffe gegen Regierungsstellen ereignet. In diesen Fällen schickten die Angreifer präparierte Dokumente mit gefälschtem Absender an Schlüsselpersonen der betreffenden Unternehmen. Die Nachrichten waren auf die Empfänger zugeschnitten, was auf vorgängige nachrichtendienstliche Informationsbeschaffung hinweisen kann.

Bei diesen unter dem Titel «Ghostnet» bekannt gewordenen Angriffen, ist auf Grund der vorhandenen Informationen davon auszugehen, dass sie zum selben Fallkomplex gehören, wie die Angriffe auf staatliche Einrichtungen, kritische Infrastrukturen und Unternehmen, welche bereits seit einigen Jahren öffentlich gemacht wurden und bekannt sind. Der Ursprung dieser Angriffe wird in China vermutet.[13] Auch in der Schweiz sind im Rahmen der Ghostnet Nachforschungen infizierte Systeme gefunden worden. Allerdings handelt es sich bei diesen ausschliesslich um Vertretungen ausländischer Gruppen und Regierungen in der Schweiz. Schweizer Unternehmen und Regierungsstellen waren nicht Teil des Ghostnet.

4.2 Conficker

Der Computer-*Wurm* Conficker (auch bekannt unter dem Namen Downadup) war im vergangenen Halbjahr eines der IKT-Hauptthemen in den Medien. Besonders rund um den 1. April 2009, dem Datum, an welchem sich der Wurm hätte updaten sollen, war das mediale Interesse enorm.

Bereits seit dem 21. November 2008 ist die erste Version dieses Windows-Wurms im Umlauf. Anfangs war die Verbreitung noch gering. Dies änderte sich ab dem Jahreswechsel jedoch drastisch. Zur Verbreitung nutzt der Wurm dabei eine Sicherheitslücke im Microsoft Windows Server Dienst (MS08-067), zu der es allerdings seit Ende Oktober 2008 ein Sicherheitsupdate gibt. Bedroht waren demzufolge vor allem Firmen und Privatpersonen, die dieses Update nicht installiert hatten. Der Wurm kennt jedoch noch weitere Möglichkeiten, um sich zu verbreiten: Er probiert eine Liste von einfachen Passwörtern[14] durch, um sich auf Netzwerkfreigaben zu kopieren oder versucht sich auf mobile Speichermedien wie *USB-Sticks* oder Digitalkameras zu kopieren. Sobald man einen infizierten USB-Stick in einen Rechner einsteckt, öffnet sich ein Fenster, in dem der Wurm ein Standard-Icon zum Öffnen von Verzeichnissen erzeugt. Das Icon steht allerdings nicht im Bereich « Optionen », sondern unter «Programm starten». Klickt man darauf, wird der Wurm auf diesem Computer installiert. Insgesamt soll Conficker mehrere Millionen Rechner infiziert haben.

Ist der Wurm erst einmal installiert, stoppt er die Windows-Update-Prozesse und erstellt einen lokalen Webserver. Danach versucht er sich weiter zu verbreiten und sich zu tarnen, um ein Entfernen zu erschweren. Er kann beliebige Dateien nachladen und ausführen. Schliesslich blockiert er auch den Zugriff zu vielen Security-Seiten und Antiviren-Update-Diensten.

Besonders der Update-Mechanismus und das magische Datum (1. April 2009), an welchem sich der Wurm hätte aufdatieren sollen, sorgte für grosses Medieninteresse. Der Update

[12] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html (Stand: 31.08.2009)
[13] http://www.melani.admin.ch/dokumentation/00123/00124/00161/index.html (Stand: 31.08.2009)
[14] http://blog.namics.com/2009/02/die_aktuelle_li.html (Stand: 31.08.2009)

Mechanismus generiert nach einem Algorithmus Domänennamen, zu denen er dann Kontakt aufzunehmen versucht, um ein entsprechendes Update entgegenzunehmen. Conficker.C konnte theoretisch 50'000 Domainnamen pro Tag generieren, mit welchen er hätte Kontakt aufnehmen können. Schlägt der Kontaktversuch fehl, wartet der Wurm 24 Stunden und generiert wiederum 50'000 neue Domainnamen. Wie bei vorangegangenen Würmern ging es den Autoren in den ersten Monaten vor allem darum, das Botnetzwerk zu installieren und zu schützen (Konsolidierung des Netzes) und weniger das Botnetz für irgendwelche aufsehenerregende Aktionen zu verwenden. Dafür spricht auch, dass die Programmierer des Wurms modernste, zum Teil erst wenige Wochen alte Algorithmen verwendeten. Die eingebaute Verschlüsselungstechnik, welche gebraucht wird, um sich vor Missbrauch durch andere Hacker zu schützen, wurde erst im Herbst 2008 entwickelt. Deshalb konnte auch davon ausgegangen werden, dass am 1. April das Internet nicht gross beeinträchtigt werden würde. Erst am 7. April 2009 bemerkte das Sicherheitsunternehmen Trend Micro eine erhöhte *P2P-Aktivität* von Conficker.C, womit der Wurm sich in die Conficker.E-Variante wandelte. Auch dabei war die Hauptmotivation des Wurmes, seine Spuren zu verwischen. So blockierte er Seiten, die Wurmentfernungs-Programme anbieten. Zusätzlich trat er unter einem zufälligen Dateinamen auf und löschte alle seine Spuren auf dem Wirts-PC. Über die genaue Motivation der Conficker-Autoren lässt sich nur spekulieren. Beweggrund könnte beispielsweise der Aufbau eines *Botnetzes* zur Vermietung an andere Kriminelle sein. Bekannt ist, dass Conficker.C das Programm SpywareProtect2009, eine *Scareware*, installiert[15].

Im Ausland waren zahlreiche Firmen- und Regierungsnetzwerke von diesem Wurm betroffen, so beispielsweise das Spital und die Landesregierung Kärnten[16] sowie die Deutsche Bundeswehr[17]. Auch in der Schweiz wurden Firmennetze durch diesen Wurm für einige Stunden lahmgelegt. In der Schweiz waren rund 1'000 *IP-Adressen* bekannt, hinter welchen sich infizierte Rechner befinden. Die meisten infizierten Computer standen jedoch in Russland, Brasilien, China und Indien.

Problem zertifizierte Systeme

Auffällig war insbesondere, dass der Wurm vor allem Netzwerke im Gesundheitswesen[18] befiel. Der Grund dürfte hier darin liegen, dass gerade in diesen Netzwerken viele zertifizierte Computersysteme stehen (beispielsweise Steuergeräte von Untersuchungsapparaten), die nicht einfach ohne Weiteres gepatched werden können. Sind diese zusätzlich mit dem Internet verbunden, sind sie ein einfaches Ziel für den Wurm. Ein anderes Problem ist das Verwenden persönlicher Laptops und USB-Geräten in Firmennetzwerken. Hierbei kann sich eine Infektion vom privaten Computer auf das Firmennetzwerk übertragen. Der Wurm nutzt diese Problematik perfekt aus.

Eigentlich hat niemand mehr mit einem solchen Wurmausbruch gerechnet. Nach Einführung von WindowsXP mit Service Pack 2, welches eine Firewall enthält und die neuesten Updates regelmässig einspielt, sollte eigentlich jedermann vor dieser Art Wurm geschützt sein. Die Realität sieht allerdings anders aus. Eine These besteht darin, dass es sich bei den meisten kompromittierten Computern vor allem um nicht offizielle Windows-Versionen gehandelt hat,

[15] http://www.heise.de/security/Deckt-der-Conficker-Wurm-jetzt-seine-Karten-auf--/news/meldung/136083 (Stand: 31.08.2009)

[16] http://www.heise.de/security/Conficker-in-Kaernten-Nach-der-Landesregierung-nun-die-Spitaeler--/news/meldung/121570 (Stand: 31.08.2009)

[17] http://www.netzwelt.de/news/79475-conficker-bundeswehr-kaempft-gegen-computerwurm.html (Stand: 31.08.2009)

[18] http://diepresse.com/home/techscience/internet/sicherheit/473436/index.do (Stand: 31.08.2009)

bei denen die Benutzer die Kontaktaufnahme mit dem Windows Update-Server bewusst nicht in Anspruch genommen haben.

Wieder einmal zeigt es sich, wie wichtig der Grundschutz eines Computers ist. Hierzu gehören die Aktualisierung des Betriebssystems und deren Applikationen, eine Firewall sowie eine aktualisierte Antivirensoftware. Da in vielen Firmen die Updates nicht immer sofort eingespielt werden und zuerst auf Kompatibilität mit den anderen Programmen getestet werden muss, kann beim Installieren eine Verzögerung entstehen, welche aber so kurz wie möglich gehalten werden sollte. Mit der Verbreitung von USB-Sticks, Digitalkameras, Handys und *MP3 Player* wird der Infektionsweg über mobile Speichermedien an Bedeutung gewinnen.

4.3 SCADA

Die Überwachung, Kontrolle und Steuerung von Industrieanlagen, von Systemen zur Verteilung lebenswichtiger Güter (Strom, Wasser, Brennstoffe, usw.) oder im Bereich des Transports und Verkehrs (Eisenbahnen, Verkehrsleitsysteme, Post, usw.) sind ohne den Einsatz von Informations- und Kommunikationstechnologie (IKT) seit Langem undenkbar. Die Entwicklung und der Betrieb entsprechender Überwachungs-, Kontroll- und Steuerungssysteme (engl. *Supervisory Control And Data Acquisition, SCADA*) hat lange Tradition. Ursprünglich hatten SCADA-Systeme nur wenig Ähnlichkeit mit herkömmlicher IKT: Sie waren von den Computernetzwerken isoliert, benutzten proprietäre Hard- und Software und setzten zur Kommunikation mit dem Zentralrechner eigene Protokolle ein. Die breite Verfügbarkeit vergleichsweise günstiger Geräte mit eingebauter Schnittstelle zum *Internet-Protokoll (IP)* hat in den letzten Jahren in diesem Bereich grosse Veränderungen gebracht. Sensoren, Maschinen und Schalter verfügen heute immer häufiger über eine eigene IP-Adresse und nutzen das normale Internet-Protokoll zur Kommunikation mit dem Zentralrechner. Den Vorteil des Einsatzes kostengünstiger herkömmlicher IKT erkauft man sich damit, dass SCADA-Systeme nun grundsätzlich den gleichen Bedrohungen ausgesetzt sind, wie wir sie vom Internet her kennen; Schadsoftware sowie «Hacker» halten Einzug. Die Diskussion um die Sicherheit von SCADA-Systemen wird deshalb immer breiter geführt, wie untenstehende Beispiele zeigen. Bei den Angriffen auf diese Systeme, welche für das Funktionieren unserer Gesellschaft zentral sind, geht es aber nicht nur um Hacker-Angriffe (Sabotage) sondern auch um technische Störungen, die den Ausfall wichtiger Systeme zur Folge haben können, wie das Beispiel der *ETCS*-System-Störung der SBB im Sommer 2009 zeigt.

Störung im ETCS hatte Beeinträchtigung im Bahnverkehr zwischen Mattstetten-Rothrist und im Lötschbergtunnel zu Folge

Die Abkürzung ECTS[19] steht für European Train Control System. Auch hierbei handelt es sich um ein SCADA-System. Zielsetzung von ETCS ist die Schaffung einer harmonisierten europäischen Zugbeeinflussung. Die Standardisierung bezieht sich insbesondere auf die Informationsübertragung zwischen Fahrweg und Fahrzeug. Die über die Komponenten des ETCS zu übertragenden Informationen können meist aus den vorhandenen Sicherungsanlagen gewonnen bzw. erzeugt werden.

Auf den Neubaustrecken Mattstetten-Rothrist, im Lötschberg-, sowie im noch nicht fertiggestellten Gotthard-Basistunnel kommt das ETCS-Level 2 zum Einsatz. Bei

[19] http://mct.sbb.ch/mct/etcs-technologie-funktionsprinzip.htm (Stand: 31.08.2009)

Geschwindigkeiten von über 160 km/h ist es dem Lokführer nicht mehr möglich, die Signale visuell zu erkennen. Dem Lokführer werden deshalb die Fahrerlaubnis und der Fahrbegriff im Führerstand angezeigt. Ausser einigen Merktafeln kann daher auf eine Aussensignalisierung verzichtet werden. Die Gleisfreimeldung und damit die Zugvollständigkeitsüberwachung sind aber weiterhin streckenseitig vorhanden. Alle Züge melden automatisch, in regelmässigen Abständen ihre genaue Position und Fahrrichtung an die Streckenzentrale. Die Bewegungen der Züge werden von der Streckenzentrale dauernd überwacht. Die Fahrerlaubnis wird, zusammen mit Geschwindigkeitsangaben und Streckendaten, laufend via *GSM-R* auf das Fahrzeug übertragen. Dieses System war am 29. Juli 2009 von einer Panne betroffen, was grosse Auswirkungen auf das gesamte SBB-Streckennetz hatte. Währendem auf der Strecke Mattstetten-Rothrist noch konventionelle Signale vorhanden sind und auf dieser Strecke deshalb noch mit einer Geschwindigkeit von 160km/h gefahren werden konnte, sind im Lötschbergbasistunnel gar keine Signale mehr vorhanden, was zur Umleitung der Züge über die Bergstrecke zur Folge hatte.

Angreifer drangen angeblich in Kontrollsystem des US-Stromnetzes ein

Angreifern ist es offenbar gelungen, Software in Kontrollsystemen zu installieren, die dazu in der Lage ist, wichtige Systeme wie Stromversorgungs- und Wasseraufbereitungsanlagen der USA zu stören. Dabei soll eine Sicherheitslücke ausgenutzt worden sein. Laut einem Bericht des «Wall Street Journals[20]» unter Berufung auf US-Sicherheitsbehörden, sollen Angreifer in das US-Stromnetz eingedrungen sein und im System Programme hinterlassen haben, die für eine Störung der Elektrizitätsversorgung im ganzen Land benutzt werden könnten. Dem Bericht zufolge vermuten die amerikanischen Behörden, dass die Angreifer darauf abzielen, das US-Stromnetz steuern zu können. Sie hätten bislang noch nicht versucht, die Infrastruktur zu beschädigen, was sich jedoch in einem Krisen- oder Kriegsfall schnell ändern könnte.

Geplantes *Smart Grid* anfällig für Angriffe

Intelligente Netzte (so genannte *Smart Grids*) werden in Zukunft konventionelle Netze ablösen. So will die kalifornische Firma «Pacific Gas and Electric» bis 2011 intelligente Gas- und Stromzähler an ihre Kunden verteilen. Dabei werden beispielsweise intelligente Stromzähler bei den Endverbrauchern installiert, die gesammelte Daten über Strom oder Gasverbrauch des Kunden direkt an den Netzknoten des Versorgers melden. Da nun ein dichteres Netz an Daten vorhanden ist, kann auch die Verteilung und Anpassung besser reguliert werden. Auch partielle Netzausfälle können so schneller detektiert werden. Diese Geräte scheinen aber nun laut einer unter Verschluss gehaltenen Studie mehrere Sicherheitsschwächen zu haben. So sollen sie zum Beispiel für *Buffer Overflows* und *Rootkits* anfällig sein. Die eingesetzten Protokolle würden zudem keine Sicherheitsmechanismen aufweisen. Falls diese Schwachstellen von einem potentiellen Angreifer ausgenützt werden können, kann dies bis zum Stromausfall führen. So könnte ein Angreifer beispielsweise eine hohe Last signalisieren. Falls der Stromerzeuger auf diese vermeintliche Last regiert, kann dies zu einer Überspannung im Netz führen. Dabei wird als Übertragungsweg das *Frequency Hopping Spread Verfahren (FHSS)* zwischen 902 und 928 MHz verwendet, aber auch *WLAN* und *GPRS* Techniken kommen zum Einsatz. Im Moment werden intelligente Stromzähler nur in Pilotprojekten eingesetzt. Dies dürfte sich aber in naher Zukunft ändern. Die USA und auch Europa werden ab 2011 vermehrt auf Smart Grids setzen.

[20] http://online.wsj.com/article/SB123914805204099085.html (Stand: 31.08.2009)

Britische Experten warnen vor dem Einsatz chinesischer Telekommunikationskomponenten

Gemäss Aussagen von Britischen Experten[21] könnten Komponenten des chinesischen Telekomkonzerns Huawei benutzt werden, um Störungen bei wichtigen Infrastrukturen in Grossbritannien wie Telekommunikation, Strom- oder Wasserversorgung zu verursachen. Von Huawei stammen zentrale Bestandteile des neuen Kommunikationsnetzwerks von British Telecom. Huawei ist einer der grössten Telekommunikationsausrüster weltweit mit mehr als 87'000 Mitarbeitenden. Es handelt sich um ein privates Unternehmen, welches nicht an der Börse kotiert ist. Der Schwerpunkt der Produkte ist die Entwicklung und Herstellung von Geräten der Kommunikationstechnologie, namentlich im Bereich Mobilfunk, xDSL, Optische Netzwerke und Endgeräte. Die von den Britischen Experten geäusserten Zweifel konnten dabei weder belegt noch ansatzweise bestätigt werden.

Während früher die Steuerung von Infrastrukturen low-tech und insofern überschaubar und kontrollierbar war, kann man heute die Funktionen der eingesetzten hi-tech-Geräten nicht mehr so einfach überprüfen. Insofern müsste je länger je mehr bei der Auswahl von Geräten und der Auftragsvergabe für Projekte betreffend (kritischen) Infrastrukturen nicht nur auf den Anschaffungspreis, sondern auch auf die gebotene (langfristige) Sicherheit geachtet werden. Es ist dabei auch genau abzuwägen, ob SCADA-Systeme nur logisch oder auch physisch getrennt von weiteren Unternehmensnetzwerken betrieben werden sollen. Zudem empfiehlt es sich, redundante Systeme einzusetzen, um den Betrieb der Infrastruktur auch im Störungs- oder Schadensfall möglichst aufrecht erhalten zu können. Der Ausfall von Telekommunikation (insbesondere der Internetverbindung), Strom oder Transportmitteln kann bei Unternehmen wie Privatpersonen enorm hohe Kosten verursachen.

4.4 Vermehrte Fokussierung auf militärische Einheiten zur so genannten Informationskriegsführung in verschiedensten Staaten

Das Thema des so genannten Informationskrieges oder Information Warfare steht weit oben auf der Liste der mit Landesverteidigung und Kriegsführung betrauten Stellen in den einzelnen Staaten rund um den Erdball - und dies nicht erst seit den massiven *Denial-of-Service*-Angriffen auf estländische Regierungs- und Unternehmensnetzwerke im Jahr 2007. In Deutschland beispielsweise hat sich in diesem Zusammenhang eine Truppe bei der Bundeswehr formiert, die sich mit so genannten *Network Centric Operations (NCO)* befasst.

Im Einklang mit der allgemeinen technischen Konvergenz und Vernetzung (siehe Kapitel 5.1), hängen auch militärische Leit-, Kommunikations- und Kontrollsysteme vermehrt an integrierten Netzwerken und sind damit auch über Mittel der Informations- und Kommunikationstechnologie angreifbar. Dies bedeutet, dass für den Fall kriegerischer Auseinandersetzungen, nicht mehr nur der Einsatz von konventionellen, militärischen Mitteln, sondern auch ein direkter Angriff auf die Netzwerke des Gegners in Erwägung gezogen wird. Umgekehrt muss sich jede Armee mit fortlaufender Vernetzung ihrer Systeme auch mit dem unbedingten Schutz dieser Systeme befassen.
Es ist bekannt, dass vor allem die grossen, militärisch mächtigen Staaten, wie beispielsweise die USA und China, in den letzten Jahren grosse Bestrebungen in diese Richtung

[21] http://www.telegraph.co.uk/news/worldnews/asia/china/5072204/Britain-could-be-shut-down-by-hackers-from-China-intelligence-experts-warn.html (Stand: 31.08.2009)

unternommen haben. Dabei dürfte sich der Aufbau von entsprechenden Kapazitäten nicht nur auf defensive, netzwerkschützende Mittel beschränken.
Auch in der Schweiz ist seit 2001 das Konzept der «Information Operations» einer genaueren Prüfung unterzogen worden. Eine Konzeptstudie zu diesem Thema wurde verfasst und erste Lehren daraus führten zur Errichtung eines *CERT* für die militärischen Einrichtungen, dem so genannten MilCERT.

Allerdings stellen sich bei solchen Initiativen grundsätzlich einige staatspolitische und rechtsstaatliche Fragen. Grundsätzlich ist es klar, dass militärische Einheiten eines Staates über die Möglichkeiten verfügen müssen, ihre Systeme gegen IKT-gestützte Angriffe der Gegenseite zu schützen. Dies kann unter Umständen auch bedeuten, dass offensive Mittel zum Einsatz kommen, um die Systeme der Gegenseite lahmzulegen oder zu stören, bevor ein Angriff auf die eigenen Netzwerke überhaupt ausgeführt werden kann. Diese Mittel können entsprechend auch bei kriegerischen Handlungen als zusätzliches Kriegsmittel eingesetzt werden. Gerade aber in einer Zeit, in der klassische, kriegerische Auseinandersetzungen zwischen Staaten die Ausnahme bleiben dürften, und Konflikte vor allem unterhalb der Kriegsschwelle ausgetragen werden, ist der offensive Einsatz militärischer IKT-Mittel sehr verlockend, entspricht jedoch einem Gang aufs völkerrechtliche Glatteis.

Im Fall der Angriffe auf georgische Regierungssysteme wurde auffallend oft der Begriff «Cyberwar» verwendet. Allerdings handelte es sich in erster Linie um Angriffe rein krimineller Natur auf Computersysteme und Netzwerke eines Staates. Entsprechend waren die Angreifer im Zuge der kriegerischen Auseinandersetzung ziviler Natur und müssten konsequenterweise rechtstaatlich als illegale Handlung qualifiziert und über die Strafverfolgung im Staat des Geschädigten geahndet werden. Auch die Aktion einer Aktivistengruppe in Israel während dem Gaza-Krieg[22] ist unter diesem Aspekt zu verstehen. In diesen beiden Fällen ist allerdings eine teilweise Subsumierung unter das Kriegsrecht vertretbar, da es sich um Aktionen handelte, welche im Rahmen einer kriegerischen Handlung zwischen zwei Staaten oder staatsähnlichen Parteien ausgeführt wurden.

Eine plötzliche Aufweichung dieser Grenzen und Klassifizierung solcher kollateralen Aktionen als kriegerische Handlungen, mit einer entsprechenden Erwiderung durch militärische IKT-Aktionen, würde gleichzeitig eine Ausweitung der Legitimation militärischer Massnahmen gegen nicht militärische und nur indirekt am militärischen Konflikt partizipierende Teilnehmer bedeuten.

Beim Aufbau und Einsatz von offensiven militärischen IKT-Kapazitäten, seien sie nun ziviler oder militärischer Natur, ist genau festzulegen, wofür, in welchen Fällen, und vor allem gegen wen, unter welchen Umständen diese eingesetzt werden dürfen. Denn nicht jeder Angriff auf militärische oder staatliche Netzwerke ist per se ein kriegerischer Akt. Selbst dann nicht, wenn sich der Staat unter Umständen tatsächlich in einem kriegsähnlichen Konflikt befindet. Auch gestaltet sich bei solchen Angriffen naturgemäss die Attribution äusserst schwierig. Ein klarer Urheber kann oftmals nicht ausgemacht werden und Retorsionsmassnahmen können unabsehbare Kollateralschäden im Zielland mit sich bringen. Die Beispiele in Estland und Georgien zeigen, dass solche Angriffe sehr wohl auch bloss krimineller Natur sein können und entsprechend mit den Mitteln der Strafverfolgung verfolgt und geahndet werden sollten. Eine Vernebelung dieser klaren Trennlinie birgt die Gefahr, mit vorhandenen Mitteln unnötig in die Kernbereiche der zivilen Organe, die primär mit dem Schutz der inneren Sicherheit betraut sind, einzugreifen. Gleichzeitig bedeutet dies,

[22] http://www.heise.de/newsticker/Gaza-Konflikt-Der-Krieg-im-Internet--/meldung/121389 (Stand: 31.08.2009)

dass die Regeln der ordentlichen Strafverfolgung und insbesondere der Grundrechtsschutz von Beschuldigten ohne Not ausgehebelt werden.

4.5 Mehr politisch motivierte DDoS Angriffe

Laut dem Sicherheitsunternehmen Arbor Networks[23] kommen politisch motivierte Internet Angriffe immer häufiger vor. Die Frequenz der Angriffe und die Zahl der Ziele wachsen ständig. Ein möglicher Grund könnte sein, dass auch technisch nicht versierte Personen DDoS-Tools wie «Black Energy» oder « NetBotAttacker» kaufen und verwenden können. Solche Tools können über ein einfach zu bedienendes Interface verwendet werden. Dies zeigt auch der Versuch der BBC (siehe Kapitel 4.7). Währenddem bis anhin die DDoS-Angriffe im Bereich von Porno-Webseiten überwiegten, ist spätestens seit dem Angriff auf Estland klar, dass diese Technik auch als politische Waffe eingesetzt werden kann. Neben Angriffen in Georgien[24] sorgten beispielsweise im Januar 2009 russische Hacker dafür, dass Kirgisistan[25] vom Internet getrennt wurde. Die Attacke richtete sich gegen die beiden grössten Internet-Provider. Über die Motivation der Angreifer kann in diesem Fall nur spekuliert werden; sie dürfte aber auch politische Hintergründe gehabt haben.

Es gilt hier festzustellen, dass im Bereich von DDoS-Angriffen eine stetige Qualitätssteigerung zu beobachten ist. Die Zahl der benötigten angreifenden Computer wird immer kleiner. Mit so genannten DNS-Amplification Attacken kann beispielsweise erreicht werden, dass auch mit einem kleinen Botnetzwerk eine grosse Wirkung erzielt werden kann. So konnte in einem Fall[26] ein Datentransfer von 5 Gigabyte/Sekunde mit nur 2'000 Rechnern generiert werden.

4.6 Netzwerkausfall bei T-Mobile

Am Dienstag, 21. April 2009, war ab zirka 16 Uhr über das Mobilfunknetz von T-Mobile in Deutschland keine Kommunikation mehr möglich. Es handelte sich um den bisher grössten Ausfall eines Mobilfunknetzes in Deutschland[27]. Sämtliche Sprach- und SMS-Dienste fielen aus. Der Grund für diesen Ausfall war ein Software-Fehler im *Home Location Register (HLR)*, das für die Herstellung der Verbindung zwischen Mobilfunkstation und der zugehörigen Mobilfunknummer verantwortlich ist. Ein Ausfall im HLR führt dazu, dass keine Verbindungen mehr hergestellt werden können und das Netz nicht mehr erreichbar ist. Nachdem diese Störung behoben wurde, stand das Netz ab 19 Uhr teilweise wieder zur Verfügung.

[23] http://www.arbornetworks.com (Stand: 31.08.2009)
[24] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (Stand: 31.08.2009)
[25] http://www.pcwelt.de/start/sicherheit/firewall/news/192009/russische_cyber_miliz_attackiert_kirgisistan/ (Stand: 31.08.2009)
[26] http://www.pcwelt.de/start/sicherheit/firewall/news/192305/zwei_porno_sites_lassen_streit_eskalieren/ (Stand: 31.08.2009)
[27] http://www.welt.de/webwelt/article3603796/T-Mobile-schenkt-Gratis-SMS-als-Entschuldigung.html (Stand: 31.08.2009)

Am 25. Juni 2009 war auch das Telefonnetz von E-Plus während rund zwei Stunden von einer Deutschlandweiten Störung betroffen. In diesem Fall soll die Ursache ein Fehler im zentralen Vermittlungsserver gewesen sein[28].

Bei beiden Fällen scheint eine zentrale Komponente für den Ausfall verantwortlich gewesen zu sein. Diese Systeme sind in der Regel redundant ausgelegt, was einen solchen Ausfall verhindern sollte. Dies schützt sehr gut vor Hardwarepannen, also davor, dass ein Server ausfällt. Mindestens im Falle von T-Online scheint es sich jedoch um eine Softwarepanne gehandelt zu haben. Da auf redundanten Systemen in etwa die gleiche Software und Konfiguration läuft, erstaunt es nicht dass bei einem Umschalten auf das Backup-System die gleichen Softwareprobleme wie auf dem Hauptsystem auftauchen und dieses System ebenfalls zum Absturz gebracht wird.

Hervorzuheben ist die Tatsache, dass sich im Fall von T-Mobile Schwierigkeiten mit dem Aufbieten des Pikett-Dienstes ergeben haben. Da die zuständigen Techniker in der Regel über das hauseigene Mobilfunknetz aufgeboten werden, waren diese nur schwer zu erreichen. Durch die Verbreitung von Mobiltelefonen wird die Erreichbarkeit von Pikett- und auch Notfalldiensten immer häufiger auf das Mobiltelefonnetz ausgelagert. Die Konsequenzen, die der Ausfall dieses Netzes auf ein Notfalldispositiv haben kann, müssen stets berücksichtigt werden.

4.7 Grossbritannien: BBC erwirbt ein Botnetz zu Demonstrationszwecken

Die britische Rundfunkanstalt BBC hat im Zuge der Vorbereitung zu einer Sendung zum Thema Internetkriminalität die Kontrollsoftware für ein *Botnetz* erworben. Laut Angaben der BBC bestand das nach der BBC-Sendung «Click» benannte Netzwerk zum Zeitpunkt der Übernahme aus rund 22'000 *Zombie-Computern*. An die Botnetz-Software war die BBC durch den Besuch entsprechender Chatrooms gekommen. In solchen Chatrooms nehmen Kriminelle miteinander Kontakt auf und sie versuchen dort auch, ihre Dienste anzubieten. Ein Botnetz ist eine Ansammlung von Computern, die mit Schadsoftware infiziert sind und sich durch einen Angreifer fernsteuern lassen. Für die 22’000 Bots sollen dabei rund 700 Dollar verlangt worden sein. Dies sei vergleichsweise günstig, da es sich um ein unspezifisches und über die ganze Welt verteiltes Botnetz gehandelt habe. Je besser die Qualität des Botnetzes ist, desto teurer wird dieses auch verkauft. BBC spricht von Preisen bis zu zwischen 300 und 400 Dollar pro 1’000 Bots. Zu Demonstrationszwecken wurden zwei Test-E-Mail-Adressen binnen Stunden mit tausenden Spam-Nachrichten überflutet. Ebenfalls wurde laut der BBC nach Absprache mit dem Betreiber eine Website mit einem Distributed-Denial-of-Service-Angriff (DDoS) lahmgelegt. Dabei stellte sich heraus, dass bereits die Netzwerkanfragen von 60 PCs ausgereicht hätten, um die Webseite lahmzulegen. Inzwischen sind die betroffenen Computer-Nutzer laut BBC über die Vorgänge informiert worden. Dazu wurde der Desktop-Hintergrund infizierter Systeme mit einer entsprechenden Warnmeldung versehen.

Diese Vorgehensweise wirft die Frage auf, ob beispielsweise ein Sicherheitsunternehmen ein Botnetz übernehmen und es so manipulieren darf, dass sich dieses anschliessend deinstalliert oder wie in diesem Fall eine Warnmeldung bei infizierten Computern einblendet. Ob dies ein Weg sein kann, um Botnetze zu bekämpfen, wird sicherlich in Zukunft vermehrt diskutiert. Ein Erwerb von Botnetzen dürfte allerdings kontraproduktiv sein, da es den Markt

[28] http://www.zdnet.de/news/wirtschaft_telekommunikation_e_plus_netz_gestern_90_minuten_lang_ausgefallen_story-39001023-41005882-1.htm (Stand: 31.08.2009)

für Botnetze weiter antreibt und es für die Cyberkriminellen noch lukrativer würde, Botnetze aufzubauen. Der BBC-Bericht zeigt aber auch sehr anschaulich, dass sich ein Botnetz durch einfache Programme steuern lässt, welche auch Personen bedienen können, die keine Computerspezialisten sind. Der Trend in diesem Bereich geht jedoch noch weiter. Im letzten Jahr wurde durch Cyberkriminelle das Modell Crimeware-as-a-Service[29] entwickelt. Die Cyberkriminellen, die sich der technischen Schwierigkeiten bewusst sind, können bei diesem Modell einen entsprechenden Dienst «mieten». Über diese Plattformen erhalten sie den Service direkt und brauchen sich nicht mit technischen Problemen zu befassen. Es ist davon auszugehen, dass dieses neue Modell im Laufe des Jahres 2009 einen deutlichen Entwicklungsschub erleben wird.

4.8 USA: Zahl der Datenpannen 2008 massiv angestiegen

Gemäss dem in San Diego ansässigen Identity Theft Resource Center[30] kam es in den USA im Jahr 2008 zu Verlusten von insgesamt 35 Millionen Datensätzen. Im Vergleich zum Vorjahr stelle dies eine Zunahme von 47% der durch Unternehmen und Behörden gemeldeten Datenverluste dar. Die meisten Datenabflüsse fanden in der Privatwirtschaft statt. Hier ergreifen laut Studie der Finanzsektor und die Kreditkartenunternehmen am meisten Gegenmassnahmen. Das Identity Theft Resource Center listet fünf Kategorien auf, welche sich für die Datenverluste verantwortlich zeichnen: Verlust von digitalen Speichern (Laptops, USB-Sticks etc.), interner und externer Datendiebstahl, unbeabsichtigte Veröffentlichung und Verbreitung persönlicher Informationen sowie Verlust von Daten durch externe Dienstleister.

Es kann davon ausgegangen werden, dass einerseits immer mehr Daten gestohlen werden und verloren gehen, anderseits aber auch der Druck gestiegen ist, Datenpannen zu melden. In der Schweiz gibt es keine offiziellen Angaben über die Anzahl solcher Pannen. In der nationalen Datenschutzgesetzgebung gibt es denn auch keine explizite Norm, die den Inhaber einer Datensammlung verpflichtet, Datenpannen zu melden. Aber auch in der Schweiz sind Vorfälle bekannt, wie beispielsweise die Veröffentlichung vertraulicher Daten zum Schengen-Abkommen auf der Webseite des Eidgenössischen Justiz- und Polizeidepartements (EJPD) im Mai des letzten Jahres[31].

Mit Blick auf die vielfältigen Möglichkeiten von Datenverlusten wird ersichtlich, dass ein integrales Sicherheitskonzept den Fokus auf den Schutz der Informationen selbst legen muss. Verteilkanäle, Zugriffsrechte und Speicherorte müssen dem tatsächlichen Wert einer Information angepasst werden. Nicht jeder Kanal oder Speicherort ist gleich sicher und nicht alle Dokumente sind gleich sensibel. Dies zieht ein verstärktes Risikomanagement beim Umgang mit Daten und Informationen nach sich. Die Sensibilisierung der Mitarbeitenden ist dabei von grosser Bedeutung. Technische Schutzmassnahmen gehören zwar zum Grundschutz der Datensicherung, können aber im Falle eines zu sorglosen Umgangs mit Informationen wirkungslos sein. Das schwächste und anfälligste Glied in der Sicherheitskette ist und bleibt in den meisten Fällen der Mensch.

[29] HJB 2008/II Punkt 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (Stand: 31.08.2009)

[30] http://www.idtheftcenter.org/ (Stand: 31.08.2009)

[31] http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (Stand: 31.08.2009)

4.9 USA will Kampf gegen Cyberbedrohungen verstärken und Schutz erhöhen

Anfang Jahr veröffentlichte die neue US-Regierung unter Barack Obama ihre Agenda betreffend der Sicherheit der Vereinigten Staaten. Die elektronischen Netzwerke des Landes wurden darin als «strategisches Gut» deklariert und dem Schutz der nationalen IT-Infrastruktur ein hoher Stellenwert beigemessen. Zur Koordination der verschiedenen Stellen, welche sich mit dieser Thematik befassen, sollte ein direkt dem Präsidenten unterstellter «National Cyber Advisor» – auch bekannt als «Cyber Czar» – ernannt werden. Weiter wurde ein « Safe Computing Research and Development Effort» angekündigt, welcher zur Entwicklung einer neuen Generation besonders sicherer Hard- und Software für Behördennetzwerke führen soll.

Ende Mai wurde dann die «Cyberspace Policy Review» publiziert: Es handelt sich dabei um eine Bestandesaufnahme der aktuellen Lage im Cyberspace mit Empfehlungen für das weitere Vorgehen der Vereinigten Staaten in diesem Bereich. Die Autoren kamen zum Schluss, dass das Internet auf längere Sicht mit den traditionellen Telekommunikationstechnologien verschmilzt und auch andere Infrastrukturbetreiber dieses Netzwerk je länger je mehr als primären Kanal für die Interkonnektivität von Systemen verwenden (siehe auch SCADA Kapitel 4.3 und 5.2).

Der Betrieb des Internet wird, wie vielfach auch Infrastrukturen der physischen Grundversorgung, mehrheitlich von privaten Akteuren gewährleistet. So wurde auch in der Cyberspace Policy Review erkannt, dass für die Sicherheit in diesem Bereich die Zusammenarbeit mit diesen privaten Akteuren unabdingbar ist. Der Staat wie auch die privaten Betreiber von wichtigen Infrastrukturen haben ein grundsätzliches Interesse an der verlässlichen Funktionsweise der verwendeten Technologien und einer sicheren Datenübertragung innerhalb der Informationsinfrastrukturen. Deshalb wird auch für die USA ein « public-private partnership for cybersecurity» empfohlen, bei welchem die Teilnehmer durch Informationsaustausch und koordinierte Aktivitäten gemeinsam einen besseren Schutz, sowie mehr Sicherheit und Robustheit der digitalen Umwelt anstreben sollen. Weiter wurde erkannt, dass die Probleme im Bereich Internet nicht von den USA allein gelöst werden können, sondern im internationalen Kontext angegangen werden müssen. Insofern gilt es, die Voraussetzungen für eine sichere und starke digitale Nation im eigenen Staat durch Überarbeitung der relevanten Gesetzesgrundlagen und Richtlinien zu verbessern und einen Rahmen für koordinierte Massnahmen der involvierten Akteure aller Ebenen (lokal, national, international) bei Vorfällen im Cyberspace zu schaffen.

4.10 EU Kommission will kritische Infrastrukturen besser schützen

Auch die EU hat erkannt, dass die IKT in zunehmendem Masse mit dem Alltagsleben ihrer Bürger verflochten wird und einen unverzichtbaren Teil der Wirtschaft und Gesellschaft darstellen, da sie entweder Güter und Dienste von grundlegender Bedeutung bereitstellen oder die Grundlage für andere kritische Infrastrukturen bilden.

Auf Grund der immer stärkeren Abhängigkeit von den kritischen Informationsinfrastrukturen, ihrer grenzübergreifende Vernetzung und Verknüpfung mit anderen Infrastrukturen sowie ihrer Anfälligkeit und Bedrohungen ist es dringend notwendig, die Sicherheit und Robustheit dieser Infrastrukturen systematisch zu verbessern. Dadurch sollen sie sich an vorderster Front gegen Ausfälle und Angriffe zu verteidigen, denn durch Störungen der kritischen

Informationsinfrastrukturen können wichtige gesellschaftliche Funktionen ernsthaft beeinträchtigt werden.

Die jüngsten Attacken auf Informationsinfrastrukturen in Estland, Litauen und Georgien haben gezeigt, dass wichtige elektronische Kommunikationsdienste und -netze ständig bedroht sind.

Deshalb plädiert die EU-Kommission in ihrer Mitteilung vom 30. März 2009 über den Schutz von kritischen Informationsinfrastrukturen[32] für Massnahmen, welche die Sicherheit, Robustheit und Stabilität des Internet sowie allgemein der kritischen Informationsinfrastrukturen erhöhen. Um dies zu erreichen, will die Kommission öffentlich-private Partnerschaften fördern. Zudem plant die Kommission gemeinsame Kapazitäten und Dienste für eine europaweite Zusammenarbeit, ein Forum für Informationsaustausch zwischen den Mitgliedstaaten und ein europäisches Informations- und Warnsystem zu etablieren. Sie fordert die Mitgliedstaaten dazu auf, nationale Notfallpläne aufzustellen und regelmässige Notfallübungen für die Erprobung der Reaktionsfähigkeit auf Netzsicherheitsverletzungen grossen Ausmasses durchzuführen. Natürlich soll auch die Zusammenarbeit der nationalen CERT und CSIRT weiter gestärkt werden.

Die EU widmet sich folglich vermehrt dem Schutz vor Cyber-Angriffen und Störungen grossen Ausmasses durch die Stärkung der Abwehrbereitschaft, Sicherheit und Stabilität.

4.11 Facebook änderte seine AGB - für kurze Zeit

Anfang Februar wurden die Allgemeinen Geschäftsbedingungen (AGB) von Facebook überarbeitet. Facebook verfügte bereits vorher über ein unwiderrufliches Nutzungsrecht an allen veröffentlichten Daten. Die Änderung der AGB wollte dieses Nutzungsrecht auch auf gelöschte Daten ausweiten. Nach massiven Protesten hat sich Facebook allerdings entschlossen, wieder zu den vorherigen Geschäftsbedingungen zurückzukehren.[33]

[32] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:DE:PDF (Stand: 31.08.2009)
[33] http://www.heise.de/newsticker/Facebook-nach-dem-AGB-Debakel--/meldung/133094 (Stand: 31.08.2009)

5 Tendenzen / Ausblick

5.1 Cloud Computing, Auslagerung, Zentralisierung und das Information Ownership

Am 17. Mai 2009 hat das Schweizer Wahlvolk mit knappen 50,1 Prozent der Einführung *biometrischer Pässe* zugestimmt. Neben datenschützerischen Bedenken schien dabei vor allem auch ein im Bereich der Informationssicherung fussendes Argument für den knappen Ausgang entscheidend gewesen zu sein. Es ging dabei um die Art und Weise, wie die biometrischen Daten gespeichert werden sollen. Dies wird zentral, stellvertretend für alle Kantone auf Stufe Bund, beim Bundesamt für Polizei fedpol geschehen. Während des Abstimmungskampfes wurde diese Lösung mehrmals als unnötiges Klumpenrisiko bezeichnet. Fände eine Speicherung der Daten in den jeweiligen Herkunftskantonen statt, würde ein einzelner, erfolgreicher Angriff nicht alle Datensätze inkriminieren, sondern nur Teile davon. Um an alle biometrischen Aufzeichnungen zu gelangen, wären also im besten Fall 26 erfolgreiche Angriffe auf die kantonalen Datenzentren nötig und nicht nur einer auf Stufe Bund.

Gerade im Bereich der Informationssicherung sind solche Risikoüberlegungen an der Tagesordnung. Während die IKT-Sicherheit noch immer einer der Hauptpfeiler eines funktionierenden Informationssicherungskonzeptes ist, rückt der Schutz der Information selber mehr und mehr in den Vordergrund. Dabei handelt es sich um einen klassischen Risiko-Assessment und –Management Prozess. Beispielsweise fusst die Sperrung von Facebook in Unternehmen nicht nur auf Überlegungen der Arbeitseffizienz, sondern hat durchaus auch Gründe im sicherheitstechnischen Bereich. Allerdings besteht eines der grössten Risiken von *Social-Network-Seiten* darin, dass Personen mit ihrem Arbeitgeber verknüpft werden können, was unter Umständen in heiklen Bereichen unerwünscht ist. In diesen Fällen helfen nur klare Vorschriften zum richtigen Umgang mit Informationen, sei es im privaten oder im Arbeitsumfeld, unabhängig von der eingesetzten Technologie. Es gilt klar festzulegen, ob und wie Daten verbreitet werden können oder geschützt werden sollen.

Dieser Entwicklung hin zu einem strikten Information Ownership und einer kontinuierlichen Einstufung der Werte einzelner Informationen, Daten und Dokumente, stehen die verlockenden und kosteneffizienten Möglichkeiten zentral gewarteter und unterhaltener Datenbanken, Anwendungen und Plattformen entgegen. Namentlich Entwicklungen wie das Cloud-Computing, de facto Monopole im *Social-Networking* Bereich wie Facebook oder aber auch auf Zentralisierung, Echtzeitreporting für die Geschäftsleitung[34] und Effizienz ausgelegte SCADA-Systeme. So verheisst das *Cloud-Computing* beispielsweise auf der einen Seite Anwendungen, Dokumentenerstellung und –bewirtschaftung aus einem Guss. Angeboten von einem vertrauenswürdigen Drittanbieter, der auch für die Sicherheit des Gesamtsystems zuständig zeichnet. Unterschiedliche Patch-Levels, Applikationen etc. innerhalb des gleichen Unternehmens gehören somit der Vergangenheit an. Allerdings führt dies auch zu einer Konzentration des Risikos und unter Umständen zu einem Single-Point-Of-Failure. Die Prioritätensetzung im Informationsmanagement, Effizienz und Kosten oder aber Selbstverwaltung von Systemen (Sicherheit und Unterhalt), ist schliesslich jedem Unternehmen selbst überlassen.

[34] http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html (Stand: 31.08.2009)

Es ist abzusehen, dass in Zukunft das Spannungsfeld zwischen Kostendruck, Effizienz und der Verfügbarkeit von Information auf der einen Seite, sowie Klumpenrisiken, Business Outsourcing kritischer Informationen und Daten und zunehmender Verletzlichkeiten auf Grund einheitlicher, vernetzter Plattformen auf der anderen Seite weiter zunehmen wird. Die Lösung dieses Ziel- und Interessenkonfliktes muss dabei von Fall zu Fall das Resultat einer möglichst vollständig informierten Risikoabwägung sein und sich in erster Linie auf Gehalt des Wertes der zur schützenden, dem Betrieb gehörenden Information beziehen.

Dabei ist das der zentralen Speicherung biometrischer Daten auf Bundesebene entgegengebrachte Misstrauen ein bereits vielversprechendes Anzeichen. Allerdings ist dieses Misstrauen nun auch auf private Lösungen gleicher Art anzuwenden. Hingewiesen sei nur auf die zahlreichen Kundenprofile, die viele Unternehmen anlegen und unterhalten.

5.2 SCADA

Die Umstellung im Bereich SCADA-Systeme wird weiter fortschreiten und der ökonomische Druck dazu führen, dass nicht nur einzelne Komponenten, sondern vermehrt ganze Unterstationen ferngesteuert und unbemannt betrieben werden. Weiter vereinfacht die durchgängig gleiche Netzwerktechnologie den Wunsch des Managements, das Geschäfts- mit dem Kontrollnetzwerk zu verbinden. Ein Beispiel dafür sind intelligente Stromzähler, wie sie im neuen geplanten US-Stromnetz eingesetzt werden sollen. Diese Entwicklung wird in Zukunft weitere Herausforderungen an die IKT-Sicherheit stellen. So gilt es zu verhindern, dass sich Vorfälle, wie beispielsweise das Einschleppen von Schadsoftware ins Firmennetzwerk auf das Kontrollnetzwerk ausdehnen. Es wird damit unerlässlich, Grundsätze der herkömmlichen IKT-Sicherheit oder entsprechende Standards und Richtlinien auch auf Kontrollsysteme anzuwenden und von den Herstellern der verwendeten Geräte ausreichende Sicherheitsmechanismen zu fordern. Zu einem umfassenden Massnahmenpaket gehört auch der Erfahrungsaustausch unter den Betreibern von Kontrollsystemen (z.B. über Verwundbarkeiten) sowie zwischen diesen und den Behörden, welche unter anderem Informationen über aktuelle Bedrohungslagen beisteuern können. Die Melde- und Analysestelle Informationssicherung MELANI steht in engem Kontakt mit den Schweizer Stromversorgern und beteiligt sich am internationalen Informationsaustausch.

5.3 Allgemeine Entwicklung Cybercrime

Immer noch werden MELANI und KOBIK[35] täglich verschiedenste Vorfälle betreffend Vorschussbetrug, angeblichen Lotteriegewinnen und Abo-Fallen gemeldet. Scheinbar ist diese Art von Internetkriminalität immer noch erfolgreich. Dies zeigen auch Berichte aus den Ländern, aus denen solche Betrügereien verübt werden. Einigen Tätern ist es dort gelungen, innert kürzester Zeit bedeutende Summen zu ertrügen. Die Gewinne, die angeblich mit sogenannten Abo-Fallen tagtäglich gemacht werden, lassen ebenfalls aufhorchen. Neben all den technischen Entwicklungen im Bereich der Verbreitung und Benutzung von Internet Schadsoftware, gibt es auf der anderen Seite auch die Möglichkeit, ohne grosses technisches Know How, dafür aber mit der nötigen Hartnäckigkeit, Ausdauer und Kreativität, grosse Summen zu erschwindeln. Aus dem grossen Angebot an Internetnutzern findet ein

[35] KOBIK: Koordinationsstelle zur Bekämpfung der Internetkriminalität (http://www.kobik.ch)

Angreifer – falls er genügend Geduld mitbringt – fast immer ein passendes Opfer. Weitere Informationen zu Betrugsarten und den entsprechenden Warnungen finden Sie hier[36] [37].

Beispiel Vorschussbetrug, Lotteriebetrug

Bei dieser Betrugsart werden massenweise E-Mails an potentielle Opfer versendet. Die in den Briefen gemachten Angebote und Versprechungen sind frei erfunden und sollen lediglich eine glaubhafte Kulisse bilden, vor welcher dann der Betrug abgewickelt werden kann. Auch E-Mails von angeblichen Lottogewinnen sind weiterhin konstant im Umlauf. Hierbei handelt es sich ebenfalls um ein Unterart des Vorschussbetrugs.

Diese Masche funktioniert, wie Berichte aus Ghana zeigen. Dort gibt es das Phänomen «Sakawa»[38] [39]. Es handelt es sich dabei meistens um junge Männer aus ärmeren Schichten, die aufs grosse Geld aus sind. Das kriminelle Tun, das meistens von Internet Cafés aus betrieben wird, umfasst mittlerweile praktisch alles, was auch aus anderen Ländern der Region, vorab Nigeria, bekannt ist. Das rasche Umsichgreifen von Sakawa erklärt sich damit, dass es vielen Tätern in sehr kurzer Zeit gelungen ist, bedeutende Summen zu ertrügen und dass sie ihren Reichtum für jedermann sichtbar zur Schau stellen – was selbstverständlich viele ermuntert, es ihnen gleich zu tun. Im Kontext der Cyberkriminalität entstanden, hat Sakawa mittlerweile auch eine Ausdehnung auf gemeine, lokal begangene Verbrechen gefunden (auch Tötungsdelikte[40]), wobei das Ziel der Taten der Gelderwerb ist.

Beispiel Gratisangebote

Es häufen sich auch Meldungen bei MELANI, in welchen die Melder erzählen, dass sie nach Anmeldung auf einer Webseite eine Abonnementsrechnung erhalten und anschliessend mit Mahnungen eingedeckt werden. Diese Angebote zielen darauf ab, den Internetbenutzer zu einer schnellen Vertragsabschliessung bzw. Leistungsbeziehung zu verleiten, wobei der Kostenfaktor sowie weitere allfällige Vertragsbedingungen schlecht ersichtlich dargestellt werden. Ist so ein «Vertrag» erst einmal abgeschlossen, folgen Mahnungen und Betreibungsandrohungen, um den Kunden einzuschüchtern. Manchmal tragen die Schreiben auch Anwälte oder Inkassogesellschaften als Absender, um die Opfer zu verunsichern und zur «freiwilligen» Zahlung der fragwürdigen Forderung zu bewegen. Dabei handelt es sich meist um deutschsprachige Seiten. Die Anbieter werden laufend kreativer und auch frecher. Es wurden vielfach auch Rechnungen und Mahnungen an Personen versendet, die sich nie auf einer solchen Seite eingetragen haben.

Bisher wurde vor allem versucht, Internet-Nutzer via Suchmaschine auf solche Seiten zu locken. Verschiedene entsprechende Angebote kursieren dabei bei der Eingabe bestimmter Schlüsselwörter bei Google ganz zuoberst. Anscheinend wird jetzt ebenfalls versucht, Nutzer via E-Mail zu erreichen[41]. Auch werden die Techniken, um die Kosten so unerkannt wie möglich darzustellen, stets verbessert. Nachdem die Kosten sehr klein oder in den AGB versteckt worden sind, wird neuerdings mit animierten Bildern gearbeitet. Der Preis wird dabei erst nach einigen Sekunden eingeblendet, so dass das Opfer kaum die Gelegenheit

[36] http://www.den-trick-kenne-ich.ch/4/de/ (Stand: 31.08.2009)
[37] http://www.fedpol.admin.ch/fedpol/de/home/aktuell/warnungen.html (Stand: 31.08.2009)
[38] http://www.ghanaweb.com/GhanaHomePage/features/artikel.php?ID=162565 (Stand: 31.08.2009)
[39] http://www.modernghana.com/news/192603/1/female-sakawa-hits-accra.html (Stand: 31.08.2009)
[40] http://www.Ghanavoices.wordpress.com/2009/08/13/girls-killed-for-sakawa/ (Stand: 31.08.2009)
[41] http://www.melani.admin.ch/dienstleistungen/archiv/01089/index.html?lang=de (Stand: 31.08.2009)

hat, diesen zu erkennen. Auch hier scheint das Geschäft zu florieren. Es ist bekannt, dass täglich zwischen 15'000 und 20'000 Euro auf die Konten der Anbieter[42] einbezahlt werden.

Das Staatssekretariat für Wirtschaft (SECO) empfiehlt, diese Art von Rechnung nicht zu bezahlen und dem Anbieter nach Entdeckung des Irrtums mit eingeschriebenem Brief sofort zu erklären, die fragliche Webseite sei täuschend und der Vertrag werde deshalb angefochten. Das SECO schreibt weiter, dass ein einziges Schreiben genüge; die nachfolgende Korrespondenz des Anbieters könne ignoriert werden.

Für weitere Informationen dazu empfehlen wir Ihnen folgende Broschüre zu konsultieren: http://www.news-service.admin.ch/NSBSubscriber/message/attachments/7979.pdf .

5.4 Drive-by Infektionen

Drive-by Infektionen werden sich in Zukunft vermehrt verbessern, damit es schwieriger wird, diese zu entdecken. Heute wird die Drive-By Infektion in den meisten Fällen statisch auf die Webseite geladen. Hierbei besitzt der Angreifer beispielsweise eine Liste mit FTP-Logindaten. Anschliessend wird automatisch mit diesen Daten in das Konto eingeloggt, eine Webseite (meist die *Index-Seite* oder in eine vorhandene Javascript-Datei .js) heruntergeladen, der schadhafte Code eingeschleust und die Seite anschliessend wieder hinaufgeladen. Zugriff kann sich der Angreifer natürlich auch durch eine *Sicherheitslücke* verschaffen. Das hinaufgeladene Script ist aber für jeden Besucher und auch für den Webadministrator sichtbar und somit auch detektierbar.

Bereits im letzten Jahr gab es Techniken, die diese Erkennung, vor allem durch die Webseitenbetreiber, erschweren. Im Juni 2008 wurde eine Vielzahl Schweizer Webseiten gehackt und darauf ein bösartiges JavaScript platziert. Das perfide bei diesem Angriff war, dass bei einem normalen Aufruf der Seite der Schadcode nicht ausgeführt wurde. Wurde die Seite jedoch via Suchmaschine, beispielsweise Google oder Yahoo aufgerufen, dann wurde der Schadcode aktiviert. Der Grund dieser Verschleierungstaktik liegt darin, dass der Webseitenbesitzer seine Seite häufig aufruft, dies aber in der Regel direkt oder via Favoritenliste macht. Somit wird dazu beigetragen, die Infektion so lange als möglich unerkannt zu halten.

Währendem obenstehendes Beispiel noch durch ein statisches Javascript bewerkstelligt wurde und durch eine Analyse des Quellcodes erkannt werden konnte, zeigen neue Trends bereits eine Weiterentwicklung. Hierbei befindet sich der Code nicht mehr direkt auf der Webseite, sondern dieser wird vom Webserver eingespielt. Dabei wird bei jedem Besuch entschieden, ob und wenn ja, auf welcher Seite der schadhafte Code eingeblendet werden soll. Für den Webmaster ist es so praktisch unmöglich, die Infektion zu reproduzieren. In einem aktuellen Fall, bei dem auch ein Schweizer *Hosting Provider* betroffen war, schien der Angriff auch über einen kompromittierten FTP-Account zu laufen. Anschliessend wurde ein *PHP-Script* auf den Server geladen. Nun wurde aber nicht die Webseite, sondern der Webserver in der Art und Weise verändert, dass er von Zeit zu Zeit einen Besucher auf eine bestimmte Schadsoftwareseite umleitet. Ein *Cookie*, welches die Malware installiert, hilft dabei dem Angreifer, die Computer zu identifizieren. Dabei verstecken sich die Umleitungen nicht nur hinter den Index-Seiten, sondern auch hinter Bildern und Favicons.

Anstatt in IFrames wurden die Umleitungen im Befehl META-Refresh untergebracht. Diese Weiterleitungen sind bei Browsern noch weniger abgeschaltet als der IFrame-Befehl. In

[42] http://www.pressebox.de/pressemeldungen/ct/boxid-261364.html (Stand: 31.08.2009)

Kombination mit einer Einmal-Einblendung ist dieser praktisch gleich schwer erkennbar wie ein IFrame Exploit.

Um Ihren Computer gegen Drive-By Infektionen zu wappnen, lesen Sie das Kapitel „Browsereinstellungen zum Schutz gegen gängige Drive-By Infektionen“ im Anhang 7.2.

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 Control	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.
Biometrischer Pass	Pass mit elektronisch lesbaren biometrischen Daten. Auf einem RFID Chip werden die persönlichen Daten wie Name, Geschlecht, Geburtsdatum etc. gespeichert.
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 kompromittierter Rechner bestehen.
Bot/ Malicious Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Browser-Plug-Ins	Software, welche Webbrowsern zusätzliche Funktionalität gibt, beispielsweise um Multimedia Inhalte anzuzeigen.
Buffer Overflows	Pufferüberläufe (engl. buffer overflow) gehören zu den häufigsten Sicherheitslücken in aktueller Software, die sich u. a. über das Internet ausnutzen lassen können. Im Wesentlichen werden bei einem Pufferüberlauf durch Fehler im Programm zu große Datenmengen in einen dafür zu kleinen reservierten Speicherbereich, den Puffer, geschrieben, wodurch dem Ziel-Speicherbereich nachfolgende Informationen im Speicher überschrieben werden.
Computer Emergency Response Team	Computer Emergency Response Team (CERT). Als CERT (auch CSIRT für Computer Security Incident Response Team)

(CERT)	bezeichnet man ein Team, das sich mit der Koordination und Ergreifung von Massnahmen im Zusammenhang mit sicherheitsrelevanten Vorfällen in der IT befasst.
Cloud-Computing	Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Informationstechnik (IT). Die IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk.
Code	Programmanweisungen, die dem Computer die auszuführenden Befehle vorgeben.
Content Management Systeme (CMS)	Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Cookie	Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.
Denial-of-Service Attacke (DoS)	Denial-of-Service Attacke (DoS). Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Domain Name System (DNS)	Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Drive-By Infektion	Infektion eines Computers mit Malware allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
European Train Control System (ETCS)	Das European Train Control System (kurz ETCS) ist eine Komponente eines einheitlichen europäischen Eisenbahnverkehrsleitsystems. ETCS soll die Vielzahl der in den europäischen Ländern eingesetzten Zugsicherungssysteme ablösen. Es soll mittelfristig im Hochgeschwindigkeitsverkehr Verwendung finden und langfristig im gesamten europäischen Schienenverkehr umgesetzt werden.
Fast Flux Netzwerk“	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.
Flash Plug-In	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.
Frequency Hopping Spread Verfahren (FHSS)	Frequency Hopping Spread Spectrum (FHSS) ist ein Frequenzspreizverfahren für die drahtlose Datenübertragung. Es wird unterteilt in Fast- und Slow Hopping. Die Trägerfrequenz wechselt und die Sequenz des Frequenzwechsels wird durch Pseudozufallszahlen bestimmt.
File Transfer Protocol (FTP)	File Transfer Protocol (FTP) ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Web-seiten auf einen Webserver zu laden.
General Packet Radio Service (GPRS)	General Packet Radio Service (deutsch: „Allgemeiner paketorientierter Funkdienst“) ist ein paketorientierter Dienst zur Datenübertragung, welcher in GSM-Netzen (Mobilfunknetzen) verwendet wird.
Global System for Mobile Communications - Rail(way) (GSM-R)	Global System for Mobile Communications - Rail(way) (GSM-R oder GSM-Rail) ist ein Mobilfunksystem, das auf dem weltweit dominierenden Funkstandard GSM aufbaut, jedoch für die Verwendung bei den Eisenbahnen angepasst wurde.
Home Location Register (HLR)	Das Home Location Register (HLR) (deutsch: Verzeichnis des Heimatortes) ist eine (verteilte) Datenbank und zentraler Bestandteil eines Mobilfunknetzes. Es gilt als Heimatregister einer Mobilfunknummer, wobei jede innerhalb eines Netzes registrierte Mobilstation und deren zugehörige Mobilfunknummer in der Datenbank gespeichert ist.
IFrame	Ein IFrame (auch Inlineframe) ist ein HTML-Element, das der Strukturierung von Webseiten dient. Es wird benutzt, um externe Webinhalte in der eigenen Homepage einzubinden.
Index-Seite	Datei auf einem Webserver/ einer Website, welche meist als Startseite verwendet wird.
Internet-Protokoll (IP)	Das Internet Protocol (IP) ist ein in Computernetzen weit verbreitetes Netzwerkprotokoll und stellt die Grundlage des Internets dar. Es ist die Implementierung der Vermittlungsschicht des TCP/IP-Modells bzw. der Vermittlungsschicht (engl. Network Layer) des OSI-Modells.
IP-Adressen	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
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.
META-Refreshes	Um beim Aufruf einer Seite zu einer anderen URL weiterzuleiten (engl. forwarding), kann der Refresh-Tag genutzt werden. Über den Content-Parameter kann weiterhin eine Zeit gesetzt werden, bis die Weiterleitung erfolgt. Beispiel: <meta http-equiv="refresh" content="5; URL=http://www.melani.admin.ch" /> Hier wird nach 5 Sekunden auf die Webseite http://www.melani.admin.ch umgeleitet.
MP3 Player	Software oder Hardware welche komprimierte Musikdaten-Dateien (MP3) abspielen kann.
Network Centric Warfare (NCW)/ Network Centric Operations (NCO)	Network Centric Warfare (NCW), zu Deutsch: netz(werk)zentrierte Kriegführung, ist ein militärisches Konzept des Krieges im Informationszeitalter. Dabei werden moderne IT-Mittel in die Kriegsführung miteinbezogen. Network Centric Operations (NCO) bezeichnet die Durchführung von Operationen auf der Grundlage des Network Centric Warware.
P2P	Peer to Peer Eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt.
PHP-Script	PHP ist eine Skriptsprache, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird.
Referrers	Ein Referrer ist die Internetadresse der Webseite, von der der Benutzer durch Anklicken eines Links zu der aktuellen Seite gekommen ist (engl. to refer „verweisen“). Der Referrer ist ein Teil der an den Webserver geschickten HTTP-Anfrage.
Rogue-Software, Rogueware	Rogue-Software, auch Rogueware, ist eine sogenannte Malware, die vorgibt, eine bösartige Software (meist Spyware) gefunden zu haben und dies aber nur in seiner kostenpflichtigen Variante entfernen zu können.
Rootkits	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.
Scareware	Bei Scareware handelt es sich um Software, welche darauf ausgelegt ist, den Benutzer zu verunsichern oder zu verängstigen. Es handelt sich um eine automatisierte Form des Social Engineering. Fällt das Opfer auf den Trick herein und glaubt sich

	bedroht, so wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. In anderen Fällen soll das Opfer durch den Glauben an einen erfolgreichen Angriff zu Handlungen verleitet werden, welche den tatsächlichen Angriff erst ermöglichen.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Smart Grid	Als „Smart Grid“ wird ein intelligentes (Strom-)Netz bezeichnet, bei welchem Daten von verschiedenen Geräten (typischerweise den Zählern bei den Verbrauchern) aus dem Netz an die Betreiberin zurückgemeldet, und je nach Ausgestaltung auch Befehle an diese Geräte erteilt werden können.
Social-Network-Seiten	Webseiten auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen. Oft werden persönliche Daten wie Namen, Geburtstage, Bilder, Berufliche Interessen sowie Freizeitaktivitäten bekanntgegeben.
Supervisory Control And Data Acquisition (SCADA)	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Time to live (TTL)	Beim *Domain Name System* zeigt die Zahl Time to live (TTL) an, für welche Zeit (in Sekunden) ein Namenseintrag noch gültig ist. Nach Ablauf dieser Zeit muss die Namensauflösung wiederholt werden.
USB-Sticks	Kleine Datenspeichergeräte, die über die USB-Schnittstelle an einen Rechner angeschlossen werden.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
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.
Zombie-Computer	Synonym für Bot / Malicious Bot

7 Anhang

7.1 ICANN und BAKOM suchen nach Lösungen bei der Bekämpfung von Fast-Flux-Netzwerken

Im Halbjahresbericht 2007/II[43] befasste sich MELANI mit den technischen Aspekten rund um die Fast-Flux-Netzwerke. In den letzten zwei Jahren hat sich diese Problematik verschärft. Das zwang die ICANN[44], die Organisation, welche die Domain-Namen verwaltet, das Problem eingehend zu analysieren. Ein erster Bericht wurde im März 2008 vom ICANN Securtiy and Stability Advisory Committee (SSAC)[45] publiziert. Diese Problematik stellt die ICANN vor besondere Herausforderungen, da den Fast-Flux-Netzwerken die Nutzung des DNS via IP “Fast Flux” (A record mit kurzen TTL) und die Änderung der Nameserver (Double Fast Flux) zugrunde liegt.

In ihrem ersten Bericht schlug die SSAC bereits eine erste Reihe von Lösungen vor, mit denen eine Eindämmung dieses Phänomens angestrebt werden könnte. Erwähnenswert sind unter anderem die Deaktivierung der Botnetze, die die Fast-Flux-Infrastruktur beherbergen, die Deaktivierung der involvierten Domain-Namen und die Einschränkung des Wechsels der Nameserver.

Die Generic Names Supporting Organization (GNSO) der ICANN[46] veröffentlichte gestützt auf diesen Bericht im Januar 2009 einen ersten, vom Working Group on Fast Flux hosting (FFWG[47]) verfassten Bericht, dessen definitive Version am 6. August 2009[48] erschien.

Wir werden in Teil 1 den eben erschienenen Bericht analysieren und in Teil 2 die Vorstösse anderer Organisationen vorstellen, die sich (vor allem im Bereich des Phishings) mit der Eindämmung der illegalen Fast-Flux-Netzwerke befassen. In Teil 3 wird erläutert, was sich in der Schweiz im Hinblick auf die Anpassung der diesbezüglichen Gesetzgebung tut.

Teil 1

Als Erstes stellt sich der GNSO das Problem der Definition der zu illegalen Zwecken genutzten Fast-Flux-Netzwerke (Fast Flux attack networks) und deren Unterscheidung von den volatilen Netzwerken (volatile networking), die legal genutzt werden. Nach dem Zwischenbericht vom Januar 2009 gab die ICANN der Nutzerschaft die Möglichkeit, zu den bisherigen Studien Rückmeldungen zu geben. Daraus resultierten interessante Inputs, hauptsächlich seitens der wichtigsten Akteure auf diesem Gebiet, aber auch seitens Privatbürgern. Man ist sich bewusst geworden, dass verschiedene Internetbetreiber für ihre Tätigkeiten Techniken verwenden, welche den Fast-Flux-Netzwerken ähnlich sind. Dies sind beispielsweise:

---

43 http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=it&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1ah2oZn4Z2qZpnO2Yuq2Z6gpJCDdIB7gGym162epYbg2c_JjKbNoKSn6A— (Stand 01.09.2009)

44 http://www.icann.org (Stand 01.02.2009)

45 http://www.icann.org/en/committees/security/sac025.pdf (Stand 01.09.2009)

46 http://gnso.icann.org (Stand 01.09.2009)

47 http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-initial-report-26jan09.pdf (Stand 01.09.2009)

48 http://gnso.icann.org/issues/fast-flux-hosting/fast-flux-final-report-06aug09-en.pdf (Stand 01.09.2009)

- Organisationen, die Netzwerke mit hohem Angriffspotenzial verwalten (Netzwerke von Regierungen, militärischen Einrichtungen, aber auch von multinationalen Konzernen oder bedeutenden Internetakteuren): Sie müssen praktisch rund um die Uhr verfügbar sein und kurze *TTL* verwenden, um die erforderlichen Ressourcen umschichten zu können;

- Verteilte Netzwerke (wie zum Beispiel Akamai): In dem Fall können die volatilen Netzwerke die generierte Datenmenge auf mehrere Server verteilen oder die Wartezeiten verringern, indem sie über mehrere Server verfügen, die über eben so viele geografische Zonen verteilt sind;

- Mobilitätssupport: Auch in dem Fall ermöglichen kurze TTL den Aufbau von Ad-hoc-Netzwerken, um eine bestimmte Art von Mobilität zu unterstützen;

- Meinungsfreiheit / Interessengruppen: Überwindung von Zensur und Ermöglichen der Veröffentlichung von Material, die anders nicht möglich wäre (ausser den Fast-Flux-Netzwerken existieren noch andere Techniken, zum Beispiel das Netzwerk „Tor“, mit dessen Hilfe Inhalte an verschiedenen Orten beherbergt werden können, damit es beispielsweise schwieriger ist die Rechner ausfindig zu machen.)

Diese Überlegungen müssen im Vorfeld angestellt werden, um herauszufinden, welche Instrumente sich zur Eindämmung der zu kriminellen Zwecken genutzten Fast-Flux-Netzwerken am besten eignen. Kurze TTL zu verhindern würde beispielsweise sowohl den kriminellen wie den legalen Fast-Flux-Netzwerken schaden. Deshalb versuchte die GNSO die kriminellen Fast-Flux-Netzwerke über ihre Hauptmerkmale zu definieren:

- Netzknoten können auf infizierten Rechnern betrieben werden; das ist aber nicht zwingend;

- sie sind insofern volatil, als sie eine Gruppe von Bots benützen, um diese Wirkung zu erzielen;

- die Botnetze sind über mehrere voneinander unabhängige Systeme verstreut (autonomous systems);

- es kommt zu häufigen Wechseln des NS (name server);

- die IP der Rechner befinden sich vor allem im Abschnitt der Endkunden mit Breitband (ADSL, TV-Kabel);

- die Qualität der Whois-Einträge ist schlecht; es gibt nur wenige Informationen (Falschmeldungen) über den Registranten;

- der Proxy-Server nginx[49] ist oftmals auf Botnetzen installiert, was die Bildung eines Reverse Proxy ermöglicht, indem zwischen Opfer, Bot-Net und Mothership eine Verbindung installiert wird, durch den die Inhalte zirkulieren (zum Beispiel eine Website);

- der Domainname wird über ein bereits bestehendes und demnach unverdächtiges Konto registriert;

- die Domain-Namen, treten in verschiedenen Zahlenkombinationen auf (zum Beispiel as1.com, as2.com, as3.com usw. usf.);

---

[49] http://nginx.net (Stand 01.09.2009)

- der einzige Zweck des Fast-Flux-Netzwerks besteht darin, den Angriff zu verlängern (zum Beispiel eine Phishingattacke gegen ein Finanzinstitut).

Aufgrund dieser Überlegungen kristallisierten sich zwei verschiedene Meinungen heraus, wie illegale Fast-Flux-Netzwerke bestmöglichst eingedämmt werden können. Die erste empfiehlt als Mittel zur Bekämpfung den Informationsaustausch, die zweite würde handfestere Aktionen von Seiten der ICANN und ihrer Mitglieder (Registrare und Registry[50]) vorziehen. Was den Informationsaustausch angeht, wurden folgende Ideen lanciert:

- Weitere nicht heikle Informationen über Domain-Namen öffentlich zugänglich machen, die via DNS (und nicht via Whois) generiert werden. Diese Informationen könnten das Alter der Domain, die Anzahl von Wechseln des Nameservers in einer bestimmten Zeitspanne und Ähnliches umfassen;

- Veröffentlichung einer Zusammenfassung der Reklamationen, die gegen eine Domain erhoben wurden, gelistet nach Registrar, TLD oder Nameserver;

- die ISP ermutigen, Netflow/sFlow zu verwenden, um herauszufinden, ob auch Botnetze zu ihrer Kundschaft gehören ;

- private Initiativen fördern, die sich darum bemühen, den Informationsaustausch zu intensivieren (wie zum Beispiel die Anti-Phishing Working Group auf dem Gebiet der Phishing-Bekämpfung).

Es gibt aber auch Stimmen, die einschneidendere Massnahmen seitens der ICANN und ihrer Mitglieder fordern und folgende Lösungen vorschlagen:

- abgekürzte Verfahren, um in Zusammenarbeit mit offiziellen akkreditierten Organen einen Domain-Namen zu löschen;

- Benutzerregeln für die kurzen TTL und Beschränkung der Anzahl Veränderungen, die in einer bestimmten Zeit in den A oder NS record gemacht werden dürfen;

- Einteilung der Nameserver in „statische“ und „dynamische“. Bei statischen Nameservern muss die IP-Adresse des Nameservers bekannt gegeben werden. Bei dynamischen Nameservern wäre die Erhebung eines Gebührenzuschlags zu erwägen;

- Erhebung eines Gebührenzuschlags für die Änderungen der statischen Nameserver, der zu gleichen Teilen der ICANN und dem Registry zufällt. Die Einnahmen werden zur Verbesserung der Missbrauchsbekämpfung eingesetzt;

- Verbesserung der Registrierungsverfahren von Domain-Namen.

Wir werden im Folgenden sehen, dass einige dieser Verfahren in der Schweiz bereits angewendet werden oder sich in Vernehmlassung befinden. Andere dagegen stiessen bei den betroffenen Verbänden auf wenig Gegenliebe, insbesondere die Idee, für den Wechsel des Nameservers einen Gebührenzuschlag zu erheben. Sie wäre aus kommerzieller Sicht kontraproduktiv.

[50] “Registries” sind Organisationen, die sich mit der Zuteilung der Ressourcen für die Internet-Nummern befassen (IP-Nummern, autonome Systeme). Registrare dagegen befassen sich mit der Verwaltung der Domain-Namen-Reservation.

Am Schluss des Berichts empfiehlt die Arbeitsgruppe, mit Blick auf künftige Entwicklungen folgende Ideen zu prüfen:

- Herausfinden, welche der vorgeschlagenen Lösungen im Bereich der Gesetzgebung angewendet oder im kommerziellen Bereich umgesetzt werden können oder welche bloss zur Bestimmung von Best Practices dienen;
- Evaluieren, wie Registrar und Registry am besten in die Politik der Deaktivierung von Domain-Namen involviert werden können;
- Ein Fast Flux Data Reporting System (FFDRS) einrichten, das heisst eine Datenbank, die auf den Fast-Flux-Netzwerken Informationen sammelt;
- Die ICANN zur Initiantin von Best Practices machen, die zwecks Eindämmung des illegalen Handelns eine stärkere Reglementierung des Sektors anstrebt;
- Die Möglichkeit ausloten, weitere Partner in den Prozess der Entwicklung von Massnahmen zur Bekämpfung der illegalen Fast-Flux-Netzwerke einzubeziehen.

Teil 2

Im Schlussbericht der Arbeitsgruppe der GNSO wurde an mehreren Stellen auf die Vorstösse anderer Verbände hingewiesen, die auf eine Eindämmung illegaler Fast-Flux-Netzwerke abzielen (vor allem im Phishingbereich). Sie werden im Folgenden eingehend beleuchtet.

Eine der aktivsten Gruppen in diesem Bereich ist zweifellos die Anti-Phishing Working Group (APWG[51]). Es handelt sich um einen Zusammenschluss von Wirtschaftsakteuren, die sich der Bekämpfung von Identitätsdiebstahl und von betrügerischen Phishingversuchen via E-Mail widmen. In einem Bericht vom Oktober 2008[52] wendet sich die APWG an die Registry und macht ihnen Empfehlungen, um dem Phishing vorzubeugen oder zumindest dessen Auswirkungen zu mildern.

Gemäss APWG gibt es verschiedene Lösungen, die von der Sensibilisierung der User/innen über komplexe Identifikationssysteme und schnelle Methoden zur Deaktivierung von Phishing-Domains bis zu Techniken zur Aufdeckung von Betrugsversuchen reichen. Nachstehend die 5 wichtigsten Empfehlungen:

- Kurzverfahren zur Deaktivierung von Domain-Namen, das eine enge Zusammenarbeit zwischen Registry und offiziellen akkreditierten Organen vorsieht;
- Aktive Verwendung der gesammelten Daten, um Domain-Namen, die für Angriffe eingesetzt werden, aufzuspüren und zu deaktivieren;
- Übermittlung der Domain-Namen, die für die Angriffe genutzt werden, an die Strafverfolgung;
- Schutz der Kunden vor Phishingversuchen. Sobald sich Cyberkriminelle Zugangsdaten zur Domainverwaltung von Kunden erschlichen haben, können sie die DNS bestehender

[51] http://www.antiphishing.org (Stand 01.09.2009)

[52] Anti-Phishing Best Practices Recommendations for Registrars, http://www.antiphishing.org/reports/APWG_RegistrarBestPractices.pdf (Stand 01.09.2009)

Domains ändern oder neue registrieren, indem sie die unverdächtige Identität eines normalen Kunden verwenden[53];

- Verbot oder Einschränkung des Gebrauchs von Fast-Flux-Websites. Darunter sind Einschränkungen hinsichtlich des Wechsels der Nameserver-Namen oder eine Mindestzahl Minuten für die TTL zu verstehen.

Der APWG-Bericht enthält eine ganze Reihe weiterer Empfehlungen:

- Nachdem ein Domainname mit einer illegalen Tätigkeit in Verbindung gebracht werden konnte, müsste nebst seiner Schliessung untersucht werden, ob mit denselben Angaben (Name, IP, E-Mail, Adresse, Kreditkarte) weitere Domain-Namen registriert worden sind;

- Ein System zur Blockierung von verdächtigen Domain-Registrierungen (registrar lock) einrichten, danach möglichst viele Informationen sammeln, vom http Request Headers bis zu den persönlichen Daten des Registranten. Anschliessend versuchen, die gesammelten Angaben zu bestätigen: Prüfen, ob es Domain-Namen mit ähnlichen Eigenschaften gibt (zum Beispiel, ob sie sich mit Zahlenkombinationen abwechseln,siehe weiter oben); ob die Namen Teile von Domain-Namen oder bekannten Marken (eBay, PayPal, verschiedene Finanzinstitute) enthalten; die IP-Adressen untersuchen, die zur Registrierung von Namen verwendet wurden, und versuchen, diese zu bestätigen, indem man sie mit den bestehenden schwarzen Listen abgleicht (wie die Spamhaus XBL z.B.); E-Mail-Adressen auf ihre Echtheit hin überprüfen; den Zusatz “fully qualified domain name” (FQDN), d.h. die Angabe der IP-Adresse für obligatorisch erklären; verwendete Kreditkarten überprüfen.

- Danach könnte man ein System für die Zuteilung eines Punktesystems für die gesammelten Angaben entwickeln und auf diese Weise ein möglichst genaues Screening erzielen.

Die APWG hat vielfältige Vorschläge gemacht, die beträchtliche Anstrengungen und einen ausgeprägten Willen zur Zusammenarbeit voraussetzen. Doch die APWG ist nicht die einzige Gruppe, die solche Ziele verfolgt. Weitere erwähnenswerte Vorstösse sind zum Beispiel das Whois Data Problem Reporting Service (WDPRS)[54]. Es handelt sich um eine Web-Schnittstelle, über die die UserInnen den Registraren, die der ICANN angehören, eine Meldung über unvollständige oder eindeutig falsche Whois-Daten von Domain-Namen schicken können. Das kann nämlich ein erster Hinweis auf eine betrügerische Verwendung dieser Namen sein. Eine weitere Initiative ist Phishtank[55]. Über dieses Portal kann jedermann Phishing-E-Mails (und die entsprechenden Domainnamen, die eingefügt wurden) melden. Die auf diese Weise alimentierte Datenbank steht jedermann zur Verfügung, um eine Adresse zu testen und herauszufinden, ob es sich dabei um eine bereits bekannte Phishing-Website handelt. Folgende drei Organisationen betreiben weitere Aktivitäten in diesem Bereich: Die Messaging Anti-Abuse Working Group (MAAWG[56]), eine Arbeitsgruppe der wichtigsten weltweiten Akteure, die sich mit elektronischen Mitteilungsdiensten befassen; oder ShadowServer[57], die sich zur Hauptsache mit dem Monitoring von Botnetz-Aktivitäten

[53] http://www.icann.org/committees/security/sac028.pdf (Stand 01.09.2009)
[54] http://wdprs.internic.net (Stand 01.09.2009)
[55] http://www.phishtank.com (Stand 01.09.2009)
[56] http://www.maawg.or g (Stand 01.09.2009)
[57] http://www.shadowserver.org (Stand 01.09.2009)

beschäftigt, sowie StopBadware[58], die sich auf die Schaffung einer Datenbank der Schadsoftware im Netz konzentriert.

Teil 3

Auch die Schweiz ist nicht untätig geblieben. Einige Gesetzesneuerungen ermöglichten überhaupt erst den Beginn der Bekämpfung dieser Art von Kriminalität. Ein erster Schritt wurde mit der Änderung der allgemeinen Registrierungsbedingungen für Domain-Namen mit der Endung ".ch" unternommen. Bis Ende Februar 2009 war es nämlich möglich, einen Domain-Namen zu erwerben und ihn sofort zu benützen. Es wurde eine Rechnung ausgestellt und so konnte das erworbene Produkt mindestens 30 Tage benützt werden. Das machte es denjenigen mit schlechten Absichten einfach, Domain-Namen für die Dauer eines Monats zu registrieren, ohne dafür bezahlen zu müssen. Nach Ablauf eines Monats und nach erfolgter Mahnung konnte der Domainname gelöscht werden. Um diese Art von Missbrauch zu vermeiden, änderte SWITCH die Bestimmungen des Registrierungsvertrags[59]. In den Vertragsbestimmungen steht jetzt, dass "die Registrierung in das Zone File seitens SWITCH im Normalfall innert 24 Stunden nach der Verarbeitung des Zahlungseingangs erfolgt". Anders gesagt, muss der Domain-Name nun zuerst bezahlt werden, bevor man ihn verwenden kann. Diese erste Massnahme erwies sich als wirkungsvolle Abschreckung gegen die massive Registrierung von ".ch"-Domänen, die im Jahr 2008 für Phishingversuche verwendet wurden.

Doch das ist nicht alles. Das Bundesamt für Kommunikation (BAKOM) arbeitete einen Gesetzesentwurf aus, der noch den politischen Organen unterbreitet werden muss. Er sieht einen neuen Artikel in der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV) vor. Dieser Artikel räumt SWITCH die Möglichkeit ein, einen Domain-Namen auf die Endung ".ch" zu blockieren und zu löschen, wenn der Verdacht besteht, dass er benützt wird:

- um schädliche Codes zu verbreiten;
- um mit illegalen Methoden an sensible Daten zu gelangen.

Die Verdachtsmeldung muss an ein vom BAKOM akkreditiertes Organ übermittelt werden.

Der wichtigste und in allen Berichten umstrittenste Punkt (zum Beispiel im Dokument der APWG oder der GNSO, deren Besonderheiten weiter oben erläutert wurden) war die Tatsache, Kurzverfahren einzuführen, um dank der Zusammenarbeit von Registraren und akkreditierten Organen einen Domain-Namen vorübergehend stilllegen oder ganz löschen zu können. Mit diesem Gesetzesentwurf könnte die Schweiz in der Bekämpfung der Internetkriminalität jedoch einen grossen Schritt vorankommen.

7.2 Browsereinstellungen zum Schutz gegen gängige Drive-By Infektionen

Einleitung

Jede Webseite besteht aus unterschiedlichen Anweisungen, dem sogenannten HTML-Code. Diese Anweisungen geben dem Browser (z.B. Internet Explorer) vor, wie der Inhalt der

[58] http://www.stopbadware.org (Stand 01.09.2009)

[59] https://www.nic.ch/reg/ocView.action?res=EF6GW2JBPVTG67DLNIQXU234MN6SC2T4PAQGM6TDMI#a8 (Stand 01.09.2009)

Webseite darzustellen ist. Während einige Webseiten nur aus Textdokumenten bestehen und keine zusätzlichen Funktionen bieten (statische Seiten), warten andere Seiten mit dynamischen Inhalten auf. Beispiele dafür sind Laufschriften, Webformulare für Online-Bestellungen, animierte Bilder oder dynamisch eingeblendete Werbebanner. Solche dynamischen Funktionen können mit ActiveX Controls und JavaScript realisiert werden. Leider werden diese auch dazu missbraucht, um unerwünschte und schädliche Aktionen auf dem Rechner des Besuchers auszulösen.

Generell gilt:

Regelmässige Updates von Betriebssystem und Anwendungen
Einige Produkte stellen dazu eine automatische Update-Funktion zur Verfügung, die Sie unbedingt nutzen sollten. Überprüfen Sie regelmässig, ob diese aktiviert ist. Informationen zu aktuellen Software Updates sind in der Regel auf den Web-Seiten der jeweiligen Hersteller zu finden.

JavaScript einschränken
Schränken Sie die Ausführung von JavaScripts (Active Scripting) mittels Browsereinstellungen soweit als möglich ein (oder deaktivieren). Bei der Deaktivierung von JavaScript ist allerdings darauf hinzuweisen, dass viele Webseiten nicht mehr korrekt funktionieren werden. Sollte Sie das beim Surfen zu stark behindern, so lockern Sie die Einschränkungen (stufenweise) auf das für Sie tragbare Mass.

ActiveX Controls einschränken (nur Internet Explorer)
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»[60] Schritt für Schritt erläutert (wobei diese Anleitung zum Setzen der Sicherheitsstufe des Internet Explorers auch für andere Windows-Betriebssysteme gültig ist).
Wichtig: Da Active Scripting auf vielen Webseiten im Internet eingesetzt wird, können nach der Änderung dieser Einstellungen gewisse Webseiten nicht im vollen Umfang dargestellt werden. Aus diesem Grund empfiehlt es sich, häufig besuchte Webseiten (denen Sie vertrauen) in die Liste der «Vertrauenswürdigen Sites» aufzunehmen. Wie Sie dazu vorgehen müssen, ist ebenfalls im Dokument «Sicherheitseinstellungen für Windows XP», Seite 6, ersichtlich.

Hinweis: Das Benutzen der Sicherheitsstufe hoch beim Internet Explorer, deaktiviert automatisch die nachfolgenden Funktionen (Javascript, IFrame und META-Refresh)

[60] http://www.melani.admin.ch/dienstleistungen/00132/00149/index.html?lang=de (stand 01.09.2009)

Im Folgenden wird auf die einzelnen Bedrohungen im Bereich Drive-By Infektionen eingegangen und entsprechende Massnahmen vorgeschlagen.

Fall 1: Obsfuskiertes (verschleiertes) Javascript (Mit Javascript wird versucht den Computer auf eine bösartige Seite umzuleiten)

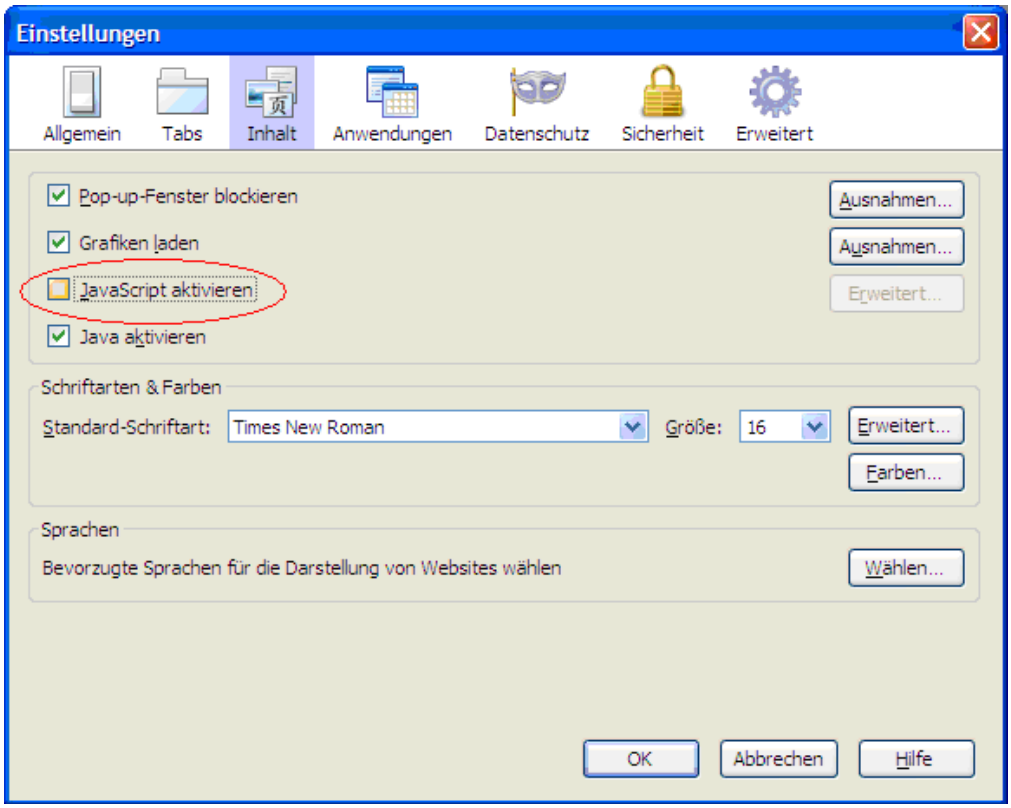
➔ Lösung: Javascript abschalten.

➔ Nachteil: Seiten, die Javascript verwenden, funktionieren nicht mehr.

Firefox

Möglichkeit 1: Verwendung des Programms NoScript[61]. Hierbei kann mit einem simplen Mausklick bei einzelnen Seiten, Javascript wieder dauerhaft oder für eine kurze Zeit aktiviert werden.

Möglichkeit 2: Unter Extras ➔ Einstellungen ➔ Inhalt: Kreuz bei « Javascript aktivieren » entfernen.

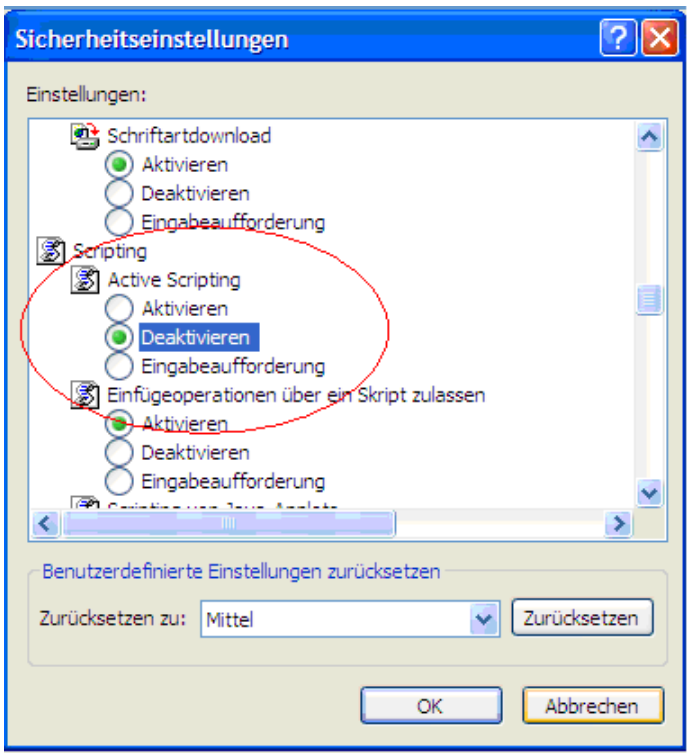


Internet Explorer

Unter Extras ➔ Interneteinstellungen ➔Sicherheit ➔ Stufe in der Zone Internet anpassen. Entweder kann das Scripting komplett deaktiviert werden oder man wird alternativ bei jeder Seite mit Javascript gefragt, ob man dieses aktivieren will (Eingabeaufforderung).

---

[61] https://addons.mozilla.org/de/firefox/addon/722 (Stand 01.09.2009)



Fall 2: IFrame-Exploit (Mit einem IFrame – Seite in der Seite – öffnet der Browser im Hintergrund eine bösartige Seite)

➔ Lösung: IFrame abschalten.

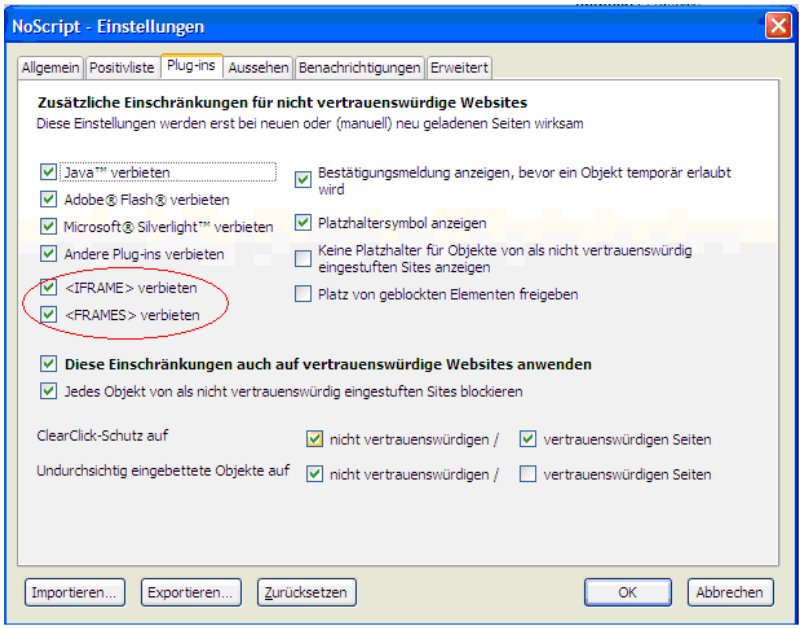
➔ Nachteil: Seiten, die IFrames benötigen funktionieren nur noch teilweise.

Firefox

Möglichkeit 1: Verwendung des Programmes NoScript

Nach Installation des Programms NoScript, im Browser auf die rechte Maustaste klicken, Auswahl NoScript wählen und in die Rubrik Einstellungen wechseln

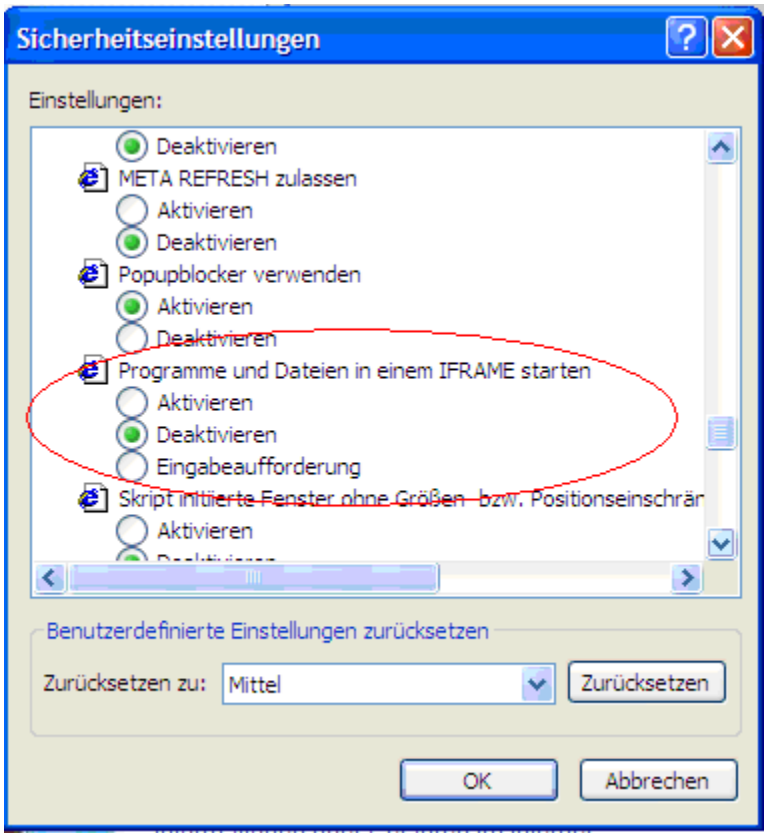
<IFRAMES> und <IFRAME> verbieten anwählen



Möglichkeit 2: Geben Sie in der Adresszeile des Browsers den Befehl: **About:config** und stellen die Funktion **Browser.frames.enabled** auf **false**.

Internet Explorer

Unter Extras ➔ Interneteinstellungen ➔Sicherheit ➔ Stufe in der Zone Internet anpassen. Entweder kann man IFrames komplett deaktivieren oder man wird alternativ bei jeder Seite mit einem IFrame gefragt, ob man dieses aktivieren will (Eingabeaufforderung).



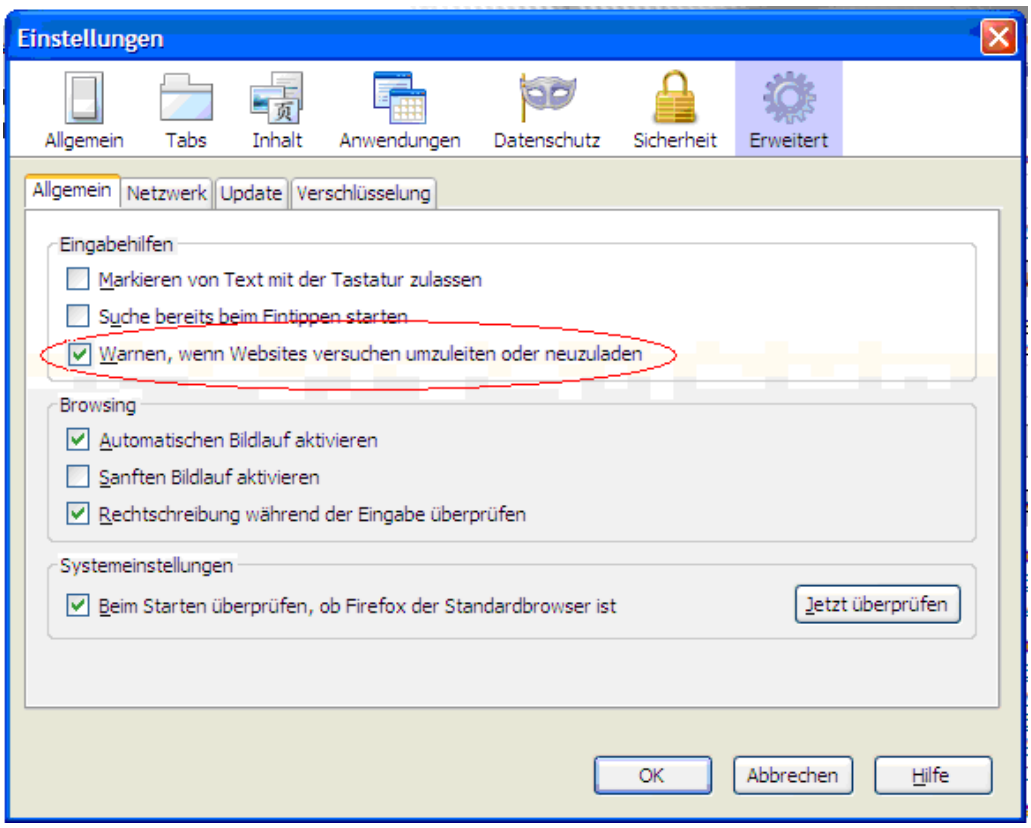
Fall 3: META-Refresh (Mit dem Befehl META-Refresh wird der Browser automatisch auf eine bösartige Seite umgeleitet)

➔ Lösung: META-Refresh einschränken.

➔ Nachteil: Seiten mit Weiterleitungen funktionieren nur noch teilweise.

Firefox

Unter Extras ➔ Einstellungen «Warnen, wenn Websites versuchen umzuleiten oder neuzuladen». Jedes Mal, wenn versucht wird den Browser umzuleiten, muss man dies manuell bestätigen.



Internet Explorer

Unter Extras ➔ Interneteinstellungen ➔Sicherheit ➔ Stufe in der Zone Internet anpassen können META Refreshes komplett deaktiviert werden.