Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

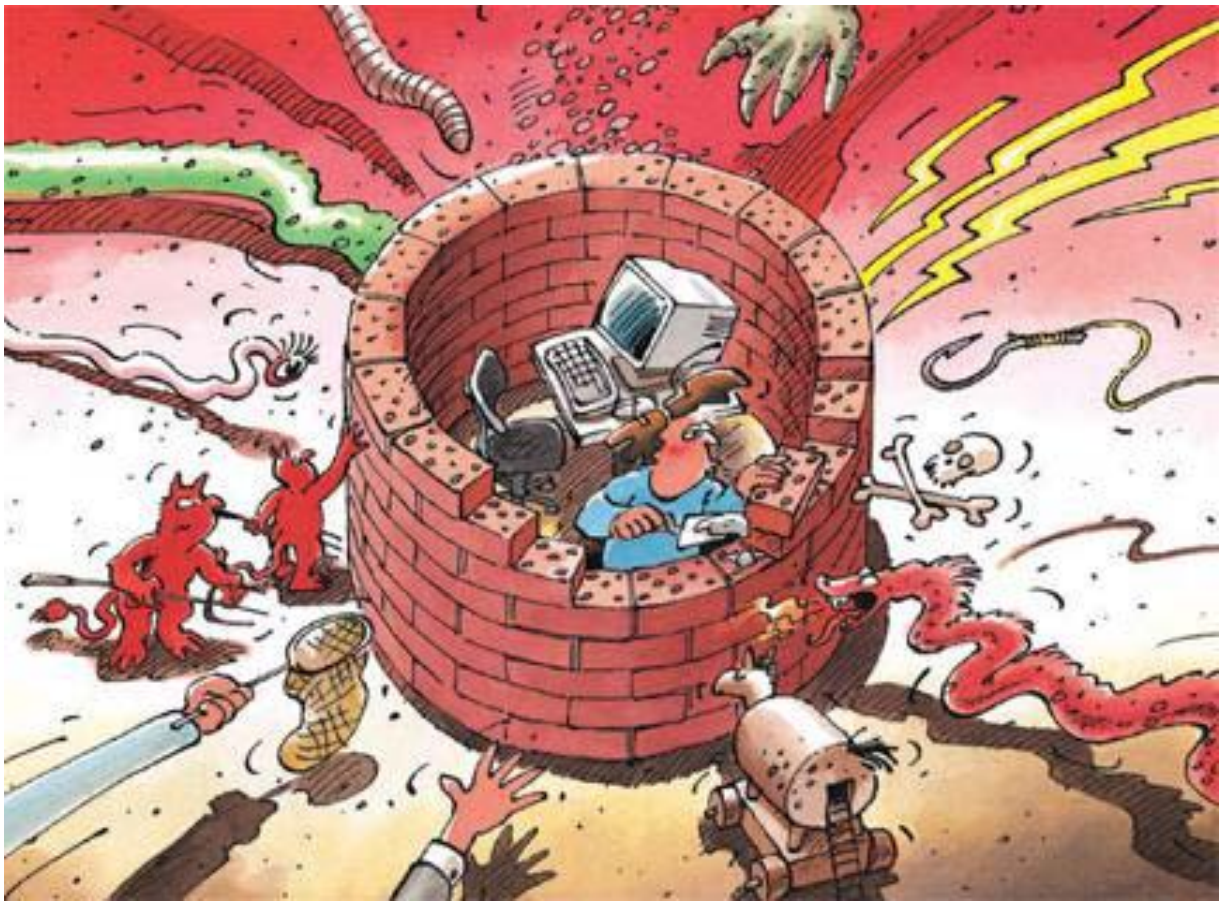
Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2010/II (Juli – Dezember)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2010/II

- **Stuxnet - Angriff auf Kontrollsysteme**
  Am Beispiel des Computerwurms Stuxnet ist im Berichtsjahr in den Medien die Problematik von Angriffen auf Kontrollsysteme (SCADA) breit behandelt worden, die in Fachkreisen schon seit geraumer Zeit diskutiert wird. Stuxnet ist jedoch der erste Fall, welcher weltweit grosse Beachtung fand. Bei entsprechend hoher Motivation und ausreichenden Ressourcen kann praktisch jedes System früher oder später infiltriert und sabotiert werden. Es ist davon auszugehen, dass sich ähnliche Angriffe in Zukunft wiederholt ereignen werden.
  ► Aktuelle Lage International: Kapitel 4.1
  ► Aktuelle Lage International: Kapitel 4.6
  ► Tendenzen / Ausblick: Kapitel 5.1
- **Angriffe auf die Verfügbarkeit (Distributed Denial of Service, DDoS) - Angriffe**
  Angriffe auf die Verfügbarkeit von Webseiten, so genannte Distributed Denial of Service (DDoS) Angriffe werden in der Cyberwelt für verschiedene Zwecke eingesetzt. Zu Beginn erfolgten Angriffe vor allem als einfache Vandalenakte. Inzwischen haben sich die Motivationen aber gewandelt. Man beobachtet beispielsweise DDoS als Rachewerkzeug, für die Schädigung der Konkurrenz, für Schutzgelderpressung oder politisch motivierte Angriffe.
  ► Aktuelle Lage Schweiz: Kapitel 3.1
  ► Aktuelle Lage Schweiz: Kapitel 3.2
  ► Tendenzen / Ausblick: Kapitel 5.2
  ► Anhang: Kapitel 7.1
- **Sicherheit von Smartphones**
  Lange ist man davon ausgegangen, dass die Virengefahr für Smartphones gering ist, da Smartphones für die Malware-Industrie kein lohnendes Ziel darstellen. Gründe dafür sind die Vielzahl der Betriebssysteme, die schwierige Verbreitung von Malware und die fehlenden „Computer-Crime-Geschäftsmodelle“. Die zunehmende Verbreitung von Smartphones und Mobiltelefonen mit PC-artiger Funktionssausstattung sowie die Speicherung sensibler Daten auf diesen Geräten, macht diese Geräte aber zunehmend auch für Kriminelle attraktiv.
  ► Tendenzen / Ausblick: Kapitel 5.3
- **Webseiteninfektionen anhaltend hoch**
  Webseiteninfektionen sind momentan die meistgenutzten Verbreitungsvektoren für Schadsoftware. Dabei kommt den zentralen Servern, welche verschiedenen Webseiten Inhalte zur Verfügung stellen, eine zentrale Rolle zu. Besonders bei Online Werbung, aber auch bei Statistikdiensten kann eine einzelne Kompromittierung weitreichende Konsequenzen zeitigen.
  ► Aktuelle Lage Schweiz: Kapitel 3.9
  ► Aktuelle Lage Schweiz: Kapitel 3.13
- **Phishing gegen Internetdienste nimmt zu**
  Gefährdet sind besonders diejenigen Dienste, welche nur mit Login und Passwort geschützt sind und wenn sich mit dem Zugang direkt oder indirekt Geld verdienen lässt. Betroffen sind neben dem Emissionshandel vor allem Kreditkarten, Online-Bezahlsysteme, Auktionsplattformen, E-Mail Provider und soziale Netzwerke.
  ► Aktuelle Lage Schweiz: Kapitel 3.5
  ► Aktuelle Lage International: Kapitel 4.3
  ► Aktuelle Lage International: Kapitel 4.4

2 Einleitung

Der zwölfte Halbjahresbericht (Juli – Dezember 2010) 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 zweiten Hälfte des Jahres 2010 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 Angriff auf die Verfügbarkeit der Webauftritte von SP, CVP, FDP und SVP

Die Websites der vier grossen Schweizer Parteien wurden innerhalb einer Woche mittels *Angriff auf die Verfügbarkeit* (DDoS) während jeweils mehreren Stunden beeinträchtigt respektive lahmgelegt. Bei der SP begannen die Angriffe am Montag 8. November 2010, die CVP registrierte eine Attacke am darauffolgenden Donnerstag. Am Freitagabend kam die FDP an die Reihe und am Sonntag die SVP. Laut SP riefen bis zu 200 Computer vor allem aus Deutschland, den Niederlanden und USA die Website zeitgleich auf. Innert vier Stunden kamen so acht Millionen Zugriffe zusammen. Die CVP sprach von über 120 Rechnern, die gleichzeitig Anfragen auf ihre Webseite starteten. Die Angriffe dürften mittels *Botnetz* erfolgt sein.

Über die Motivation dieser Angriffe ist nichts bekannt, insbesondere ob die Angriffe mit den Abstimmungen vom 28. November 2010 zusammenhingen. In dieser Abstimmung ging es unter anderem um die Ausschaffungsinitiative. Neben den bekannten Attacken dürfte es noch eine erhebliche Anzahl an Angriffen (gegen kleinere Firmen, respektive Webauftritte) geben, welche nicht an die Öffentlichkeit gelangen.

Auch wer kein grosses technisches Know-How hat, kann einen DDoS-Angriff im Untergrundmarkt relativ einfach in Auftrag geben. Dabei richtet sich der Preis nach der Kapazität der anzugreifenden Website. In der Regel können solche Attacken bereits für wenige hundert Dollar gebucht werden. Da es sich bei den angreifenden Computern um kompromittierte Systeme nichtsahnender Nutzer handelt, ist es sehr schwierig, auf technischem Wege den Ursprung des Angriffs zu eruieren. Je nach Angriffsart ist die Absender-IP-Adresse auch gefälscht.

3.2 Angriffe durch Wikileaks-Anhänger

Am 5. Dezember 2010 sperrte die Finanzdienstleisterin PostFinance das Spendenkonto des «Wikileaks»-Gründers Julian Assange wegen falschen Angaben zu seinem angeblichen Wohnsitz in Genf. In der Folge wurde die Website von PostFinance Ziel eines *Angriffs auf die Verfügbarkeit (DDoS)* durch mutmaßliche «Wikileaks»-Unterstützer. Der Angriff beeinträchtigte die Website für rund 22 Stunden und verlangsamte oder verunmöglichte damit für die 1.2 Millionen E-Banking-Kunden von PostFinance faktisch den Zugriff auf ihre Konten. Koordiniert wurden die Attacken offenbar durch eine informelle Gruppierung namens «Anon Operation», die seit Dezember 2010 elektronische Vergeltungsschläge gegen ihrer Meinung nach vermeintliche Wikileaks-Gegner durchführt. Die Gruppe rief dabei öffentlich dazu auf, sich ein Programm aus dem Internet herunterzuladen, welches dazu geeignet war, „sinnlose“ Anfragen in grossem Ausmass an eine beliebige Internetadresse zu senden. Je höher die Zahl der Internetnutzer, die dieses Programm einsetzen, desto grösser war die Wahrscheinlichkeit, dass die angewählte Internetseite ab einem bestimmten Zeitpunkt überlastet und deshalb nicht mehr erreichbar war. Neben PostFinance waren auch die Ebay-Tochtergesellschaft PayPal, sowie die Websites von Mastercard, Visa, Interpol und der Schwedischen Behörden Ziel ähnlicher Angriffe.

Im Zusammenhang mit diesem Angriff hat die Strafverfolgung in verschiedenen Ländern Verhaftungen vorgenommen. Das FBI hat in den USA 40 Häuser und Wohnungen durchsucht.[1] In Grossbritannien hat die Polizei fünf mutmassliche Computer Hacker festgenommen.[2] In den Niederlanden wurde eine 16 jährige Person verhaftet, welche an dieser Aktion teilgenommen hatte.[3] Aber auch die Behörden in Deutschland und Frankreich haben eigene Ermittlungen aufgenommen.[4]

Normalerweise werden für solche Angriffe Botnetze genutzt. In diesem Fall konnten «Wikileaks»-Sympathisanten ein Programm mit dem Namen «Low Orbit Ion Canon» (LOIC) herunterladen und danach die zu attackierende URL manuell eingeben oder ihren Computer freiwillig fernsteuern lassen. Dieser Aufruf erfolgte über soziale Netzwerke wie z.B. Facebook oder Twitter. Da es das Programm LOIC auch in einer im Browser ausführbaren Version gibt, konnten sich auch Personen mit wenig IT-Know-how an diesem Angriff beteiligen. Da es sich bei diesem Angriff vorwiegend um Angreifer ohne qualifizierte IT-Kenntnisse gehandelt hat, war es für die Polizei ein Leichtes, die hinter diesem Angriff stehenden Personen zu identifizieren.
DDoS Angriffe sind nichts Neues und werden häufig für Erpressungen oder Schädigung von Konkurrenzfirmen eingesetzt. Aber auch politisch motivierte Angriffe, wie es in dem oben beschriebenen Fall anzunehmen ist, werden vermehrt beobachtet. Neben den Demonstrationen auf der Strasse werden Proteste zunehmend auch in den virtuellen Raum getragen.

3.3 Erste Übung «Cyber Europe»

Die Europäische Union hat am 4. November 2010 eine erste europaweite Übung durchgeführt, um die Reaktionsfähigkeit der EU und EFTA-Länder bei einem möglichen Cyber-Angriff zu testen. Die eintägige Übung wurde von der Europäischen Agentur für Netzsicherheit (ENISA) organisiert. Es wurden die Bereiche Schutz kritischer Informationsinfrastrukturen, Strafverfolgung im Bereich Cyberkriminalität, GovCERTs und Regulatoren getestet. An der Übung angeschlossen waren insgesamt 22 EU- und EFTA-Staaten, darunter auch die Schweiz. Zusätzlich waren acht europäische Länder als Beobachter im Übungskontrollraum in Athen anwesend. Mehr als 150 Experten aus 70 öffentlichen Stellen in ganz Europa nahmen an der Übung teil. In der Schweiz waren dies die Melde- und Analysestelle Informationssicherung MELANI mit dem GovCERT.ch, die Bundeskriminalpolizei sowie das Bundesamt für Kommunikation. Sämtliche teilnehmenden Länder wurden mit mehr als 320 Vorfällen konfrontiert. Grundlage der Übung war ein Szenario, in dem die Internetverbindungen zwischen den beteiligten europäischen Ländern schrittweise ausfallen oder erheblich eingeschränkt werden. Bei der Übung mussten die Mitgliedstaaten zusammenarbeiten, um weitere Ausfälle zu verhindern und um die Verbindungen wieder herzustellen. Es wurde die internationale Kooperation, aber auch die nationale Zusammenarbeit zwischen den einzelnen Stellen, die für die Bekämpfung von Cyberangriffen verantwortlich sind, getestet. Dabei ging es vor allem um die Überprüfung der Kommunikationskanäle, Kommunikationspunkte und Abläufe innerhalb und zwischen den einzelnen Staaten. Weitere Ziele waren Erkenntnisse über das Vorfallmanagement innerhalb Europas, um Abläufe zur gegenseitigen Unterstützung bei Vorfällen oder massiven Cyber-Angriffen zu verbessern.

[1] http://www.tagesanzeiger.ch/digital/internet/FBIAktion-gegen-Anonymous/story/23000748 (Stand: 10. Januar 2011).

[2] http://cms.met.police.uk/news/arrests_and_charges/five_arrested_under_computer_misuse_act (Stand: 10. Januar 2011).

[3] http://www.n-tv.de/politik/Hacker-rufen-zum-Cyber-Krieg-article2110826.html (Stand: 10. Januar 2011).

[4] http://www.spiegel.de/netzwelt/netzpolitik/0,1518,742298,00.html (Stand: 10. Januar 2011).

Die Übung «Cyber Europe 2010» war ein erster wichtiger Schritt zur Stärkung der Cyber-Abwehrbereitschaft Europas und ist im Zusammenhang mit dem verstärkten Engagement der EU im Bereich *Schutz kritischer Informationsinfrastrukturen (CIIP)* zu sehen. Im Frühjahr 2009 wurde in Tallinn an der CIIP-Ministerkonferenz der EU-Mitgliedsstaaten erkannt, dass dringender Bedarf besteht, Abwehrmöglichkeiten, Sicherheit und Stabilität bei kritischen Informationsinfrastrukturen innerhalb der EU zu erhöhen.

Diese Übung war in ihrer Art die erste für Europa. Schon allein die Tatsache, dass 22 europäische Länder an der Übung teilgenommen haben, ist als Erfolg zu werten. Für eine detaillierte Analyse ist es allerdings noch zu früh. Trotzdem kann bereits jetzt gesagt werden, dass die Kommunikation vor allem zwischen den nationalen *CERTs* gut geklappt hat. Auf europäischer wie auch auf weltweiter Ebene gibt es bereits etablierte Kontaktlisten oder Organisationen, wie beispielsweise den Verbund europäischer Regierungs–CERTs (European Government CERTs - EGC), welche täglich genutzt werden. Private Betreiber von kritischen Informations-Infrastrukturen wurden in dieser ersten Übung noch nicht einbezogen. Für zukünftige Übungen ist deren Beteiligung jedoch geplant.

3.4 "Geschichten aus dem Internet" für mehr Sicherheit in der Informationsgesellschaft

Verschiedene Stellen aus Bund und Kantonen haben eine gemeinsame Broschüre mit dem Titel «Geschichten aus dem Internet - die man selber nicht erleben möchte» veröffentlicht. Anhand von Comics zeigt die Broschüre gefährliche Situationen im Web auf und wie man diese erkennt, darauf reagiert oder sie vermeiden kann. Sie handeln von der Weitergabe persönlicher Daten, von kriminellen Aktivitäten im Internet, ungenügendem Kinder- und Jugendschutz, hinters Licht geführten Konsumentinnen und Konsumenten, ungesicherten Computern und unverschlüsselten *WLAN-Netzen*. Zu jeder Geschichte werden Links zu Organisationen aufgeführt, die vertiefte Informationen anbieten. Ziel ist, die Sicherheit und das Vertrauen der Bevölkerung im Umgang mit den Informations- und Kommunikationstechnologien (IKT) zu stärken.
Die Comic-Geschichten richten sich in Deutsch, Französisch, Italienisch, Rätoromanisch und Englisch an die gesamte Bevölkerung. Sie stehen im Internet zum Download bereit oder können als gedruckte Broschüre bestellt werden.[5] Auf Wunsch können die Geschichten auch in geeigneten Datei-Formaten zur Publikation (unter Angabe der Quelle) bezogen werden.
Die Broschüre ist eine Umsetzungsmassnahme des Konzepts «Sicherheit und Vertrauen», das vom Bundesrat am 11. Juni 2010 zur Kenntnis genommen wurde.[6] Dieses Konzept zeigt Massnahmen auf, um die Bevölkerung und die KMU im sicherheitsbewussten und rechtskonformen Umgang mit den Informations- und Kommunikationstechnologien (IKT) zu unterstützen. Dadurch soll zudem das Vertrauen in die IKT gestärkt werden. Die Massnahmen werden unter der Leitung der Koordinationsstelle Informationsgesellschaft des BAKOM zusammen mit verschiedenen Fachorganisationen umgesetzt.

Internet, Computer und Handy gehören mittlerweile zum täglichen Leben der Menschen in der Schweiz. Die Vorteile der Internetnutzung sind aber stets auch mit Gefahren verbunden. Anders als bei einem Spaziergang durch die Strassen, sind die dunklen Ecken im Internet nicht immer auf den ersten Blick erkennbar. Die Broschüre hilft, die Gefahren im Internet zu

[5] http://www.geschichtenausdeminternet.ch (Stand: 10. Januar 2011).

[6] http://www.bakom.admin.ch/themen/infosociety/01691/01710/index.html?lang=de (Stand: 10. Januar 2011).

erkennen und wurde von der Bevölkerung gut aufgenommen. Sie wird im Schulunterricht, für die Elternbildung, die Sensibilisierung in Firmen, in Polizeistellen und für die Information von Konsumentinnen und Konsumenten erfolgreich eingesetzt. Die Broschüre war schon nach kurzer Zeit vergriffen und musste nachgedruckt werden.

3.5 Phishing von E-Mail-Konten

Seit Dezember 2010 werden vermehrt *Phishing* E-Mails gegen E-Mail Provider beobachtet , darunter die Swisscom. Im Gegensatz zu früheren Angriffen, bei denen das Opfer Login und Passwort direkt ins E-Mail schreiben und an eine angegebene E-Mail Adresse zurücksenden sollte, wird bei den aktuellen Angriffen ein Link gesendet auf den man klicken soll, um anschliessend auf eine Phishingseite umgeleitet zu werden. Diese gefälschte Webseite sieht dem Original täuschend ähnlich und fordert zur Eingabe von Login und Passwort sowie weiteren persönlichen Daten auf. Diese Vorgehensweise ist von früheren Angriffen gegen Finanzdienstleister bekannt. Diese aufwändigere Vorgehensweise zeigt zwei Dinge: Die potenziellen Opfer reagieren auf plumpe E-Mails nicht mehr (respektive zu wenig), und E-Mail-Logindaten sind im Untergrundmarkt weiterhin sehr gefragt, weil sie sich problemlos verkaufen lassen .

Dass Zugangsdaten zu Internetdiensten und vor allem Kreditkartendaten vermehrt im Visier der Cyberkriminellen stehen, deckt sich auch mit der Einschätzung von MELANI. Phishing-Versuche gegen E-Mail-Dienstleister wie Bluewin, Hotmail usw. nehmen zu. Vermehrt werden auch Logindaten von Websiteadministratoren gestohlen, welche dann zum Platzieren von *Drive-By Infektionen* auf Websites verwendet werden. Beispiele für Betrügereien, welche mit solchen Logindaten verübt werden können, sind in den Halbjahresberichten 2009/1[7] im Kapitel 3.3 und 2008/2[8] im Kapitel 3.6 beschrieben. Klassisches Phishing gegen Schweizer Finanzdienstleister wurde nur noch vereinzelt beobachtet. Grund dafür ist die Einführung verschiedenster Sicherheitselemente beim E-Banking.

Anzumerken ist, dass hinter E-Banking Angriffen (klassisches Phishing und E-Banking Schadsoftware) mit *zwei Faktoren Authentifizierung* und Phishing gegen Internetdienste, welche nur mit Login und Passwort geschützt sind, verschiedene Geschäftsmodelle und damit auch verschiedene kriminelle Gruppen stecken. Gruppen, die „einfaches“ Phishing betreiben, sind an den Login-Daten interessiert, nicht aber zwingend an dem Betrug, der mit diesen Daten anschliessend begangen wird. Dies verkleinert die eingesetzte kriminelle Energie, da man die Daten ja „nur“ verkauft, nicht aber am eigentlichen Betrug beteiligt ist. Bei E-Banking Angriffen ist eine Trennung zwischen Erlangung der Login-Daten und dem eigentlichen Betrug nicht mehr möglich, weil die Zweifaktoren Authentifizierung ein kleines Zeitfenster erzwingt, in dem der ganze Betrugsvorgang stattfinden muss. Neben der grösseren Komplexität stellt sich vor allem die Frage, wie man an das ergaunerte Geld gelangt. Das Geld muss hierzu gewaschen werden, was eine grosse Infrastruktur von Finanzagenten notwendig macht. Hierzu bedarf es einer guten Organisation und vor allem einer grösseren kriminellen Energie.

Viele Dienstleistungen im Internet können mittels einfacher Eingabe von Benutzername und Passwort aufgerufen werden. Vergisst der Kunde sein Passwort, kann er dieses über einen

[7] MELANI Halbjahresbericht 2009/1, Kapitel 3.3: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (Stand: 10. Januar 2011).

[8] MELANI Halbjahresbericht 2008/2, Kapitel 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (Stand: 10. Januar 2011).

Link «Passwort zurücksetzen» neu anfordern. Er erhält das neue Passwort per E-Mail zugestellt. Gelingt es einem Angreifer, das E-Mail-Konto zu hacken, kann er sich diesen Service zunutze machen, um auf verschiedenste Dienste des Opfers zuzugreifen und diese für seine Zwecke zu missbrauchen.

3.6 Mobiles Internet ausgefallen

Am 9. November 2010 beeinträchtigte eine Störung das mobile Internet der Swisscom. Praktisch alle Swisscom-Mobile Kunden waren über mehrere Stunden vom Internet abgeschnitten. Laut Swisscom trat gegen 7:30 Uhr bei Wartungsarbeiten eine Störung auf dem *GPRS-Netz* auf. Um die Störung zu beheben, musste der Dienst im Laufe des Vormittags neu gestartet werden. Der Neustart verursachte Probleme und führte zu diesem grossflächigen Ausfall.[9] Nicht betroffen waren das Telefonieren auf dem Mobilnetz, der Versand und Empfang von SMS sowie die Festnetz-Verbindungen. Als Entschädigung vergütete Swisscom ihren mobilen Internetkunden zehn Franken. Neben den Mobiltelefonen waren beispielsweise auch Zahlterminals für Kreditkarten und die tragbaren Computer der SBB-Zugführer von der Störung betroffen.

Das mobile Internet gehört immer mehr zum Alltag: Schnell die Abfahrtszeit des Busses abfragen, ein Ticket kaufen oder die neuesten Nachrichten herunterladen. Fällt das mobile Internet aus, muss man auf diese Dienstleistungen verzichten. Dies ist sicherlich zu verkraften.

Aber auch andere «wichtigere» Dienstleistungen wie beispielsweise mobile Kreditkarten-Terminals funktionieren immer häufiger auf Basis von mobilem Internet. Nochmals anders präsentiert sich die Situation bei mobil betriebenen Steuerungsanlagen in der Industrie und bei der Versorgungsinfrastruktur: Sollten diese auf Grund eines Verbindungsverlustes nicht mehr aus der Ferne kontrollierbar sein, könnte dies für Teile der Bevölkerung gravierende Folgen haben.

3.7 Radioausfall im Raum Bern

Am 16. Dezember 2010 um 7:15 Uhr ist ein Autofahrer auf spiegelglatter Fahrbahn mit seinem Wagen von der Strasse abgekommen und in einen Leitungsmast des Energieversorgers Bernische Kraftwerke (BKW) geprallt. Dies reichte aus, um einen Stromunterbruch in der Region auszulösen. Neben den Haushalten, die an diesem Morgen ohne Strom waren, war auch die Versorgung des nahegelegenen Sendeturms auf dem Bantiger unterbrochen. Dies beeinträchtigte die gesamte Radio- und Fernsehversorgung im Raum Bern. Um solche Vorfälle zu vermeiden, verfügt der Sendeturm über zwei unabhängige Stromversorgungen. Unglücklicherweise funktionierte der Schalter nicht, der in solchen Fällen von einem auf den anderen Stromkreis umschalten soll.

Das Radio wird für die flächendeckende Alarmierung im Falle einer Katastrophe oder eines Störfalles eingesetzt. So ist im Notfallkonzept Kernanlagen geregelt, dass die Gemeinden bei einem Reaktorunfall die Anweisungen via Radio von Kanton und Nationaler Alarmzentrale des Bundesamtes für Bevölkerungsschutz erhalten[10]. In der Bevölkerung ist allgemein

[9] http://www.swisscom.com/GHQ/content/Media/Medienmitteilungen/2010/20101109_MM_Stoerung_Mob_Internet_aufgehoben.htm (Stand: 10. Januar 2011).

[10] http://www.ensi.ch/fileadmin/deutsch/files/nfs_2006d.pdf , Seite 8 (Stand: 10. Januar 2011).

bekannt, dass bei einem Sirenenalarm das Radio eingeschaltet werden muss. Deshalb gilt es gerade hier, ein besonderes Augenmerk auf Ausfallsicherheit und Stabilität zu richten. Die UKW-Sender der SRG der Schweiz sind in Verfügbarkeitsklassen eingeteilt. Dementsprechend sind die grossen Sender einer hohen Verfügbarkeitsklasse zugeordnet. Dies gilt auch für den Sendeturm Bantiger. Als Schlüsselmerkmal ist dabei die maximal zulässige Ausfallzeit pro Ausfall festgelegt. Die Verfügbarkeit umfasst die ganze Versorgungskette, also nicht nur den Sender, sondern ebenfalls die Zuführung des Sendeprogramms, die Sendersteuerung usw. Hingegen gibt es keine Vorgaben bezüglich Notstromversorgung des regulären Radioprogramms. Dies im Unterschied zur Information der Bevölkerung durch den Bund in Krisenlagen (IBBK). Hier gelten höhere Schutzanforderungen. Dafür steht ein eigenes IBBK-Radio Sendernetz zur Verfügung.

Ein solcher Vorfall zeigt exemplarisch, wie wichtig die regelmässige Prüfung von Notfallkonzepten ist.

3.8 «Black hat-SEO»-Kampagne auch mit «.ch» Domänen

Suchmaschinenoptimierung oder «Search Engine Optimization» (SEO) sind Massnahmen, die dazu dienen, Webseiten im Suchmaschinenranking auf höhere Plätze zu bringen. Suchmaschinenoptimierung ist ein Teilgebiet des Suchmaschinenmarketing. Mit Techniken wie «*Cloaking*», «*Keyword Stuffing*» oder «*Hidden Text*» (beziehungsweise *Hypertext*) gelingt es, unbekannte Seiten an die Spitze der Suchmaschinenklassierung zu hieven und so eine bessere Sichtbarkeit und einen vermehrten Verkehr zu erreichen. Ethische Suchmaschinenoptimierung wird dabei «white hat»-Optimierung genannt. Sie verzichtet auf unerwünschte Praktiken und befolgt die Direktiven der einzelnen Suchmaschinen. Im Gegensatz dazu wird die Optimierung unter Einbeziehung unerwünschter Methoden «black hat»-Optimierung genannt.

Wenn ein Betrüger im Web eine Malware möglichst effizient verteilen will, infiziert er am besten eine rege besuchte Website (siehe Kapitel 5.5). Über eine einzige Website lassen sich so Zehntausende von Computern infizieren. Meistens sind die am stärksten besuchten Websites aber auch am besten geschützt (im Web finden sich zahlreiche Ausnahmen, welche die Regel bestätigen). Mit der SEO Technik reicht es, weniger bekannte (und schlechter geschützte) Websites mit geringem Verkehr zu kompromittieren und diese dann an die Spitze der Suchmaschinenklassifizierungen zu katapultieren.

Im August 2010 fand eine anhaltende «black hat SEO»-Kampagne mit dem Ziel statt, eine *Scareware* zu verbreiten. Sie bezog auch verschiedene Schweizer Domänen[11] mit ein. Nachdem auf einem Schweizer Webserver eine Sicherheitslücke festgestellt worden war, wurde unter jedem Domain-Namen auf diesem Webserver, eine Weiterleitung (self.location.href) platziert, die den Benutzer auf eine Webseite mit der *TLD* «co.cc» verwies, welche die Meldung „You're infected" einblendete und dem Benutzer ein Programm anbot, welches den Computer vermeintlich säubern könne (siehe Abbildung). Lädt man das Programm herunter und installiert dieses, fangen die Probleme aber erst an. Die Technik, dass viele in diesem Falle gehackte Seiten auf eine einzelne Zielseite verweisen, nennt man «*Linkfarm*». Diese Technik fällt ebenfalls unter den Begriff «black hat SEO».

[11] Dancho Danchev, Experte für Informatiksicherheit, analysierte die Kampagne ausführlich in seinem Blog: http://ddanchev.blogspot.com/2010/08/dissecting-scareware-serving-black-hat.html (Stand: 10. Januar 2011).

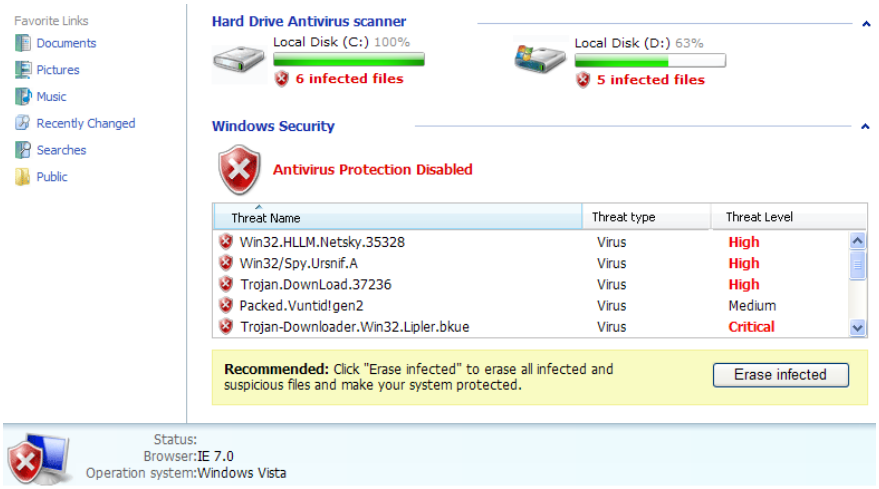


Abbildung 1: Beim Ansurfen von Kompromittierten ch.-Webseiten wird man auf eine Webseite umgeleitet, welche angibt, dass der Computer infiziert sei.

Auch Websites, die für Verbrecher nicht allzu attraktiv erscheinen, sollten unbedingt mit der notwendigen Sorgfalt geschützt werden. Wer ein *Content Management System* (CMS) wie beispielsweise «WordPress», «Joomla», «Drupal» usw. verwendet, sollte diese Applikationen regelmässig aktualisieren und so verhindern, dass Übeltäter freie Bahn haben. Zudem sollten auch die Hosting Provider bezüglich Webserver eine erhöhte Sicherheit anstreben.

3.9 Kampf gegen schädliche Websites

Ausgangslage

Vermehrt hacken Cyberkriminelle legitime Webseiten und platzieren dort schädlichen Code. Auf diese Weise können Phishing-Webseiten aufgeschaltet (siehe Kapitel 3.5) oder Webseiteninfektionen eingeschleust werden (siehe Kapitel 3.13). Im letzteren Fall kann es dann bereits ausreichen, eine entsprechend manipulierte Webseite aufzurufen, und schon hat man seinen Computer mit *Viren* oder *Trojanern* infiziert.

Sämtliche internetfähigen Rechner können mit Malware infiziert werden. Linux- und MacOS-Nutzer wiegen sich in falscher Sicherheit, wenn sie Viren und Trojaner nur als Windows-Problem sehen. Zudem sind auch Smartphones Ziel von Angriffen – Tendenz steigend (siehe Kapitel 5.3).

Massnahmen durch MELANI und SWITCH

Seit Ende November 2010 geht die Schweizer Domainname-Registrierungsstelle SWITCH intensiver gegen Schweizer Webseiten vor, welche schädliche Software verbreiten und Computer von Internetnutzern beim Surfen mit Malware infizieren.[12] SWITCH prüft nun Hinweise auf Malware verbreitende Webseiten und kontaktiert betroffene Halter und Betreiber (Provider) mit der Bitte, das Problem zu beheben. Wird innerhalb eines Arbeitstages nicht reagiert, blockiert SWITCH die Internetadresse für bis zu 5 Werktage, löscht während dieser Zeit die Zuweisung zu einem Nameserver und informiert MELANI.

[12] http://www.switch.ch/de/about/news/2010/malware-nov2010.html (Stand: 10. Januar 2011).

Wenn der Schadcode nicht entfernt wird, kann MELANI die Weiterführung dieser Massnahmen für 30 Tage beantragen.[13]

Wie bereits in Kapitel 3.5 des letzten MELANI-Halbjahresberichts[14] beschrieben, geht es bei diesen Massnahmen primär darum, Internetnutzer zu schützen und Betreiber von Internetpräsenzen auf die Kompromittierung ihrer Webseiten hinzuweisen. Die Blockierung von Domainnamen steht als letztes Mittel bereit, wenn eine Säuberung der Webseite durch den Betreiber nicht erfolgt und damit die Abwendung der Gefahr nicht anders zu bewerkstelligen ist. Die Erfahrung zeigt, dass die meisten Betreiber für die Informationen dankbar sind und innerhalb nützlicher Frist ihre Webseiten wieder in Stand stellen. In diesem Zusammenhang musste MELANI noch nie eine Sperrung beantragen und wird auch weiterhin diese Möglichkeit nur als ultima ratio und bei tatsächlicher akuter Gefährdung eines erheblichen Nutzerkreises anwenden.

Massnahmen anderer Organisationen

Da das Problem von kompromittierten Webseiten insgesamt zunimmt und nicht jede Registrierungsstelle so engagiert vorgeht wie SWITCH, beschäftigen sich immer mehr Internetakteure in diesem Bereich, ergreifen Massnahmen und stellen Produkte bereit, um Nutzer zu schützen. Insbesondere die Browser-Hersteller haben Mechanismen eingeführt, welche vor dem Besuch von möglicherweise schädlichen Webseiten warnen. So wird beim Aufruf einer entsprechenden Internetadresse jeweils eine Seite vorgeschaltet, welche den Nutzer über die Gefahr informiert, welche beim Laden der angeforderten Seite besteht. Google kennzeichnet potenziell schädliche Webseiten seit Kurzem bereits in den Suchergebnissen. Zudem bieten verschiedene Anti-Malware-Hersteller Produkte an, welche zum Einen Suchresultate als unbedenklich oder problematisch markieren, zum Anderen beim Aufrufversuch von schädlichen Webseiten warnen.

Alle diese Initiativen und Funktionen sind grundsätzlich begrüssenswert. Insbesondere die im Browser eingebauten und standardmässig aktivierten Schutzmassnahmen helfen sicherlich, Infektionen bei weniger versierten Internetnutzern zu verhindern. Die Erkennungsrate von schädlichen Webseiten ist jedoch sehr unterschiedlich und das alleinige Vertrauen auf einzelne Produkte kann die Nutzer in falscher Sicherheit wiegen. Wie bei allen Abwehrmassnahmen gegen schädliche Internetinhalte bietet keine Lösung einen 100%-igen Schutz, denn die Methoden der Angreifer ändern sich ständig, um die Entdeckung von eingeschleustem Schadcode zu erschweren. Neben den von verschiedenen Anbietern bereitgestellten, in Browser, Internetseiten oder *Toolbars* «eingebauten» Schutzmechanismen ist es nach wie vor unumgänglich, ein reguläres Anti-Malware-Programm (Anti-Viren-Scanner) zu installieren und regelmässig Betriebsystem und alle Applikationen zu aktualisieren, um das Infektionsrisiko zu minimieren.

Frankreichs Anti-Phishing-Initiative

Ähnlich verhält es sich mit Phishing-Filtern: Bei den kurzfristig auftretenden Phishing-Webseiten ist eine schnelle Reaktion von zentraler Bedeutung. Typischerweise sind die ersten Stunden nach dem Versand von E-Mails, welche einen Link zu einer Phishing-Webseite enthalten, der kritische Zeitraum. In den meisten Browsern gibt es eine Meldefunktion, über welche Phishing-Seiten gemeldet werden können. Es gibt zudem

[13] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (Stand: 10. Januar 2011).

[14] MELANI Halbjahresbericht 2010/1, Kapitel 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=de (Stand: 10. Januar 2011).

Toolbars (von Anti-Malware-Herstellern und spezialisierten Anbietern), die vor solchen Seiten warnen. Auch hier haben Nutzer die Möglichkeit, eine entdeckte Phishing-Seite zu melden. Die Meldungen werden dann analysiert und typischerweise wird kurz darauf durch das entsprechende Produkt vor der Webseite gewarnt. Anfang 2011 hat Microsoft in Zusammenarbeit mit PayPal und dem französischen CERT-LEXSI eine auf Bekämpfung von französischsprachigem Phishing fokussierte Initiative gestartet. Meldungen können von der Bevölkerung auf einer speziellen Webseite abgesetzt werden.[15]

Da die Reaktionszeit von Website-Betreibern und Hosting-Providern sehr unterschiedlich ausfällt, muss jede Möglichkeit zum Schutz von Internetnutzern ausgeschöpft werden. Je schneller Warnungen herausgegeben werden, desto weniger potenzielle Opfer gibt es. Die Vielzahl von Anbietern führt auch hier dazu, dass nicht alle Produkte vor allen gefährlichen Webseiten warnen, weil nicht alle Anbieter von einer spezifischen Webseite Kenntnis erhalten. Es kann deshalb nicht davon ausgegangen werden, dass man keine Phishing-Webseite angezeigt erhält, weil man ein Anti-Phishing-Produkt verwendet. Effizienter ist es, sämtliche E-Mails mit einer Aufforderung zur Passworteingabe zu ignorieren. Insofern gilt es nach wie vor generell kritisch zu sein, wenn man via E-Mail dazu aufgefordert wird, auf einer Webseite persönliche Daten wie Passwörter oder Kreditkarteninformationen einzugeben oder zu «verifizieren»“.

Der Eintrag der eigenen Webseite in Malware- oder Phishing-Filtern kann sehr unangenehm sein und unter Anderem potenzielle Kunden fernhalten. Nach der Wieder-Instandsetzung der Website stellt sich dann das Problem, dass die Einträge in diesen Filter- und Warnlisten wieder entfernt werden müssen. Dies gestaltet sich insofern schwierig, weil man zum Einen nicht weiss, in wie vielen und was für Listen die Adresse aufgeführt ist, und zum Anderen die Kontaktaufnahme mit den Anbietern häufig nur über das entsprechende Produkt effizient funktioniert. Dies führt dazu, dass nach einer Kompromittierung der Website eine aufwändige Nachbearbeitung des Vorfalles vorgenommen werden muss. Die Anbieter kontrollieren ihre Filter zwar regelmässig auf deren Aktualität – es kann aber unter Umständen eine längere Zeit dauern, bis ein Eintrag so wieder entfernt wird.

Um zu verhindern, dass die eigene Website kompromittiert wird, ist es unumgänglich, die Webapplikationen ständig auf dem neuesten Stand zu halten. Weiter empfiehlt es sich, die eigene Webpräsenz zu überwachen, um nach einer allfälligen missbräuchlichen Veränderung diese sofort wieder Rückgängig zu machen, bevor die entsprechende Internetadresse Eingang in Filter- und Warnlisten findet.

3.10 27C3: we come in peace – und hacken deine Website

Vom 27. bis 30. Dezember 2010 fand in Berlin der 27. «Chaos Communication Congress» unter dem Motto «we come in peace» statt.[16] An diesem vom Chaos Computer Club (CCC) organisierten Anlass, suchten die Teilnehmenden unter Anderem verschiedenste Websites auf Sicherheitslücken ab. Fündig wurden sie zum Beispiel bei der Website des Grasshopper Club Zürich. Das Logo des Vereins wurde kurzfristig durch dasjenige des FC Zürich ersetzt, Datenbanken der Webshops sowie Angaben von registrierten Nutzern extrahiert und dann online gestellt.

[15] http://www.phishing-initiative.com (Stand: 10. Januar 2011).

[16] http://events.ccc.de/congress/2010/wiki/Welcome (Stand: 10. Januar 2011).

So sah die GC-Webseite in der Nacht vom 28. auf den 29. Dezember aus:

Abbildung 2: Veränderte GC-Webseite.

Die Hacker haben nach ihrer Aktion ein Mail an alle GC-Newsletter-Abonnenten (deren Adressen in einer der Datenbanken gespeichert waren) versandt, in welchem sie auf die unzureichend geschützte Webseite hinwiesen.

We Come In Peace

Es ist Zeit dem Verein "uf de andere siite vo de Gleis" lebewohl zu sagen und das Spielfeld den echten Profis freizugeben.

Es ist tagisch, immer wenn ein Verein oder eine Seite aus dem Internet verschwindet, stirbt mit ihm ein Stueck Geschichte....
Um diesem auszuweichen, haben wir eine Sicherung der Datenbank der Shops und der Userdaten erstellt. - gern geschehn :)

Was vielleicht auch noch ganz informativ ist:

Dieses typo3 CMS ist so unfassbar scheisse. ich koennte pausenlos kotzen.
FCZ wird natuerlich wieder Meister und gcz wird abstreiten dass die Datenbank mit allen Benutzerdaten uA der Shops verloren gegangen sind.
Kann ja passieren, nicht jeder ist so fit mit Moderner technik. und so Datenbanken gehn nunmal einfach verloren, ist ja auch schon anderen grossen Firmen passiert. solange keine Kreditkarteninformationen in der Datenbank gesp... moment...

Abbildung 3: E-Mail der Hacker an alle GC-Newsletter-Abonnenten.

Da in der betroffenen Datenbank Passwörter im Klartext abgelegt waren, empfiehlt MELANI den eingetragenen Benutzern, ihre Passwörter umgehend zu wechseln.

MELANI empfiehlt, für Webdienste jeweils verschiedene Passwörter zu wählen, um zu verhindern, dass nach einer solchen Datenpanne die ganze Online-Identität von Hackern missbraucht werden kann. Insbesondere sollte für Anmeldungen, welche aus E-Mail-Adresse und Passwort bestehen NIE dasselbe Passwort wie für das E-Mail-Konto verwendet werden. Wenn Angreifer nicht wie hier «in Frieden kommen», ist das E-Mail-Konto das erste Ziel, bei welchem mit dem erlangten Passwort ein Login versucht wird; als zweites wird der Zugang zu verschiedenen sozialen Netzwerken ausprobiert.

Weitere Sicherheitslücken wurden auf Websites von politischen Parteien, rechtsradikalen Gruppierungen, Flughäfen, Medien, Regierungsstellen, u.v.a.m. gefunden.[17] Einen besonderen Scherz leisteten sich die Hacker mit dem Ersten Deutschen Fernsehen, auf dessen Website diese Falschmeldung aufgeschaltet wurde:

Abbildung 4: Kompromittierte Webseite des Ersten Deutschen Fernsehens mit der Falschmeldung.

3.11 Evaluationsstudie «Anti-Botnetz-Intiative Schweiz»

Botznetze lassen sich bereits für wenige US Dollar pro Tag mieten, wobei der Endpreis von der Leistungsfähigkeit und der Einsatzdauer des gewünschten Botnetzes abhängt. Es ist deshalb nicht erstaunlich, dass Botnetze heute den meisten kriminellen Aktivitäten im Internet zugrunde liegen.

Der erfolgreiche Kampf gegen Botnetze bedingt eine intensive Zusammenarbeit zwischen Internetprovidern, dem Staat und allenfalls Ermittlungsbehörden. Deshalb hat MELANI Ende 2010 die Hochschule für Technik in Zürich mit der Durchführung einer Evaluationsstudie beauftragt. Diese soll zeigen, in welcher Form eine solche Zusammenarbeit möglich ist und inwiefern im Ausland bestehende Initiativen (z.B. botfrei.de[18]) auf die Schweiz adaptiert werden könnten. Die Studie soll bis Ende Juni 2011 fertiggestellt sein.

3.12 In eigener Sache: Projektleiter «Cyberdefense»

Der Bundesrat hat am 10. Dezember 2010 eine Aussprache über die Bedrohung der Schweiz durch Angriffe aus dem Cyberspace und über mögliche Gegenmassnahmen

[17] http://events.ccc.de/congress/2010/wiki/Hacked (Stand: 10. Januar 2011).

[18] Das deutsche Anti-Botnet-Beratungszentrum ist ein Service von eco, dem Verband der deutschen Internetwirtschaft e.V., mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). https://www.botfrei.de/ (Stand: 10. Januar 2011).

geführt. Er hat entschieden, die Schutzmassnahmen gegen solche Angriffe auf die Schweiz zu verstärken. Er ernennt dazu Kurt Nydegger, ehemaliger Chef der Führungsunterstützungsbasis der Armee (FUB), zeitlich befristet zum Projektleiter für «Cyber Defense». Dieser wird eine Expertengruppe leiten, die bis Ende 2011 eine gesamtheitliche Strategie des Bundes gegen Cyber-Bedrohungen ausarbeiten soll.[19]

3.13 OpenX Server

Im letzten Jahr wurden diverse Webseiteninfektionen registriert, bei welchen die Ursache auf Sicherheitslücken in *AdServern* zurückgeführt werden konnten. So war die *OpenSource* AdServer Software OpenX während des ganzen Jahres von Sicherheitslücken betroffen, die es einem Angreifer ermöglicht haben, Administrationsrechte zu erlangen[20]. Da die Updates, welche solche Sicherheitslücken schliessen, nicht automatisch eingespielt werden, ist hier die Sorgfalt des Webadministrators gefragt. So warnten im Juni 2010 Sicherheitsexperten vermehrt vor veralteten OpenX-Versionen, da die Updates teilweise nur zögerlich eingespielt wurden.[21]

Auch in der Schweiz waren OpenX-*Sicherheitslücken* im Sommer 2010 Ursache für zahlreiche Infektionen in der Schweiz, darunter auch der Webauftritt einer grossen Schweizer Zeitung. Hierbei wurde die Werbung der Online Ausgabe mit einer Websiteinfektion versehen. Es ist klar, dass die Infektion einer solchen Webseite bedeutend folgenreicher ist als bei einer privaten Homepage (siehe auch Kapitel 5.5).

	200
hxxp://openx /www/delivery/ajs.php?zoneid=3&source=hxxp://www. .ch&cb= &loc=hxxp://www .ch&referer=hxxp://www .ch	200
about:blank	200
hxxp://www.dhfyjrud321.com/tds/in.cgi?default	**200**
hxxp://www.nbvhhdtn321.com/tds/in.cgi?8	**302**
hxxp://korkonvasiliy.com/hehehe/index.php?s=c4de1af395e576f5156ba255734c26c9	**302**
hxxp://korkonvasiliy.com/hehehe/404.php	**200**

Abbildung 5: Verbindungsprotokoll einer Webinfektion auf der Online Ausgabe einer Schweizer Zeitung.

Wie auf dem Verbindungsprotokoll zu sehen ist, wurde ein Besucher nach Aufruf der Webseite der Zeitung auf den Server «dhfyjrud321».com weitergeleitet, um danach verschiedene Sicherheitslücken in *Browser* und *Applikationen* auszunutzen. Zusätzlich wurde ein *Cookie* gesetzt, damit die Infektion nur beim ersten Besuch sichtbar ist. Dies erschwert die Analyse der Seite durch Sicherheitsexperten wie auch die Fehlererkennung und -behebung auf Seiten des Webadministrators.

Webseiteninfektionen sind momentan die meistgenutzten Verbreitungsvektoren für *Schadsoftware*. Dabei kommt den zentralen Servern, welche verschiedenen Webseiten Inhalte zur Verfügung stellen, eine zentrale Rolle zu. Besonders bei Online-Werbung, aber

[19] http://www.news.admin.ch/message/?lang=de&msg-id=36731 (Stand: 10. Januar 2011).

[20] http://www.heise.de/security/meldung/Ein-Jahr-alte-Luecke-gefaehrdet-OpenX-Ad-Server-1077941.html (Stand: 10. Januar 2011).

[21] http://news.softpedia.com/news/OpenX-Based-Malvertising-Attack-Discovered-145903.shtml (Stand: 10. Januar 2011).

auch bei Statistikdiensten kann eine einzelne Kompromittierung weitreichende Konsequenzen haben.
Bei Anbietern von Internetwerbung, aber auch anderer Inhalte, kommt dem Umgang mit der eingesetzten Software eine wichtige Bedeutung zu. Auch hier müssen alle Programme immer auf dem neuesten Stand gehalten werden. Am Ende gilt gerade bei solchen Diensten, dass eine Website nur so sicher sein kann, wie ihr schwächstes Glied. Und dies sind oftmals Angebote Dritter, welche in die Website eingespiesen werden und somit für die Websitebetreiber unkontrollierbar sind.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 «Stuxnet» – Angriff auf industrielle Kontrollsysteme

Mitte Juni 2010 wurde ein neuer *Computerwurm* entdeckt, welcher via *USB-Stick* ein vollständig gepatchtes Windows-7-System infizieren konnte. Dies gelang, weil unter Anderem zwei Treiber mit *Rootkit*-Funktionen im Wurm integriert sind, welche mit regulären, aber wohl gestohlenen *digitalen Signaturen* von zwei verschiedenen Firmen versehen waren, und sich deshalb ohne Warnung im System installieren liessen. Damals ahnte noch niemand, dass dies das meistdiskutierte Schadprogramm des Jahres werden sollte.[22] Analysen legten dar, dass die bereits vom «Conficker»-Wurm verwendete, sowie mehrere bislang ungepatchte Windows-Sicherheitslücken zur Verbreitung ausgenutzt wurden. Der Wurm namens «Stuxnet» kann über Druckerspooler und Netzwerkfreigaben weiterreisen und hat auch eine *Peer-to-Peer*-Komponente, welche gegenseitige Updates von infizierten Systemen innerhalb desselben Netzes ermöglicht. Auf diese Weise kann Stuxnet sich auch in nicht am Internet angeschlossenen Netzwerken aktualisieren, sobald eine neuere Version eingeschleppt wird.

Neben diesen aussergewöhnlich vielseitigen Infektionsvektoren für Windows enthält Stuxnet Code, um Anwendungen zu manipulieren, welche der Programmierung von industriellen Kontrollsystemen (so genannten *Speicherprogrammierbaren Steuerungen, SPS* – englisch *Programmable Logic Controllers, PLC*) dienen. Diese Anwendungen werden ebenfalls von «Stuxnet» infiziert und für dessen Weiterverbreitung sowie zur Infektion von SPS verwendet. Hier ist «Stuxnet» schon nahe an seinem Ziel, welches in der Beeinträchtigung der Funktionsweise bestimmter SPS besteht. Nur wenn ein System spezifische Kriterien erfüllt, entfaltet Stuxnet seine geplante Wirkung und manipuliert den laufenden Prozess. «Stuxnet» verschleiert seine Anwesenheit nicht nur auf Windows-Systemen, sondern auch in allen anderen befallenen Komponenten. So wird zum Beispiel die ursprüngliche Konfiguration der SPS gespeichert, damit bei Bearbeitung der Konfiguration nicht der veränderte Code, sondern die scheinbar intakte Konfiguration im Bearbeitungsprogramm angezeigt wird. Auch die von der SPS während des Betriebs an die Überwachungssysteme ausgegebenen Daten werden dahingehend verändert, dass die Manipulation an der betroffenen Industrieanlage nicht angezeigt wird.

[22] http://www.heise.de/thema/Stuxnet; http://www.spiegel.de/thema/stuxnet/; (Stand: 10. Januar 2011) .http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html; (Stand: 10. Januar 2011) http://www.symantec.com/business/theme.jsp?themeid=stuxnet; (Stand: 10. Januar 2011); http://www.langner.com/en/blog (Stand: 10. Januar 2011).

Die hoch komplizierte Funktionsweise dieser Malware gilt als bislang einzigartig. Eine weitere ungewöhnliche Eigenschaft von «Stuxnet» ist, dass nicht möglichst viele, sondern nur Systeme mit spezifischen Merkmalen infiziert werden – «Stuxnet» ist sehr wählerisch. Die Programmierung ist nicht darauf ausgelegt, gekaperte Computer für beliebige Internetkriminalität zu missbrauchen oder Schaden an IT-Systemen zu verursachen; vielmehr versucht «Stuxnet», ganz bestimmte Systeme ausfindig zu machen, über welche genau definierte SPS befallen und manipuliert werden können. Mit «Stuxnet» wurde ein sehr gezielter Angriff durchgeführt.

4.2 «Wikileaks»

Nicht erst seit dem zweiten Halbjahr 2010 beschäftigt die Whistleblower-Plattform «Wikileaks» die Gemüter. Seit 2007 offeriert «Wikileaks» Personen aus aller Welt die Möglichkeit, vertrauliche, zensierte oder andere nicht öffentliche Dokumente anonym zu übermitteln. Anschliessend unterzieht «Wikileaks» diese einer - nach eigenen Aussagen - den ethischen und journalistischen Grundsätzen verpflichteten Prüfung und stellt neben einer journalistischen Aufarbeitung oder einfachen Kommentierung auch die Rohdaten der Öffentlichkeit zur Verfügung. Die Idee hinter diesem Vorgehen ist relativ einfach: Durch die gleichzeitige Veröffentlichung von Artikel und Grundlagenmaterial soll ein Maximum an Transparenz geschaffen werden. Entsprechend nimmt«Wikileaks» auch keine interne Selektion vor, was die gelieferten Informationskomplexe betrifft, sondern veröffentlicht alles nach einer ersten Sichtung. Somit soll der Leser für sich selber entscheiden können, ob er den zur Verfügung gestellten Informationen glauben schenken will oder nicht. Die Leserschaft soll auch entsprechend nicht der Willkür eines nach klassischen Prinzipien funktionierenden Mediums ausgesetzt sein, welche eine Vorselektion der Geschichten vornimmt und selber entscheidet, sei es auf Grund journalistischer, ethischer oder kommerzieller Überlegungen, welche dieser Geschichten am Ende wie publiziert werden soll.

Die Vorgänge der letzten sechs Monate rund um die fortlaufende Publikation von rund 250'000 US-State-Departement-Depechen durch «Wikileaks» förderten dabei mehrere unabhängige Problemkreise zu Tage. Zum Einen entbrannte aufs Neue eine medien-ethische Diskussion, die sich vor allem auf die Frage konzentrierte, inwiefern es vertretbar ist, klassifizierte Dokumente nach einem de facto full-disclosure Prinzip einfach der Öffentlichkeit zugänglich zu machen. Dabei spielte auch die Frage nach den Absichten und Motiven des «Wikileaks» (Mit-)Gründers Julian Assange eine Rolle. Inwiefern die Personalisierung der Wikileaks Tätigkeiten auf Assange, die von «Wikileaks» vorgenommene Priorisierung der Informationen, entgegen ihrem eigentlichen credo, sowie die selektive Auswahl kollaborierender und mit Exklusivrechten ausgestatteten Medienhäuser durch Assange und der damit einhergehende inhärente Widerspruch zum eigentlichen «Wikileaks»-Gedanken zu werten sind, ist eine rein medienethische und –philosophische Diskussion, die nicht hier geführt werden soll.

Zwei weitere Vorgänge in diesem Zusammenhang haben aber einen klaren Bezug zum Thema der Informationssicherung. Zum einen die Frage, wie überhaupt 250'000 klassifizierte Botschaftsdepeschen in die Hände von «Wikileaks» gelangen konnten. Es ist noch immer unklar, ob eine einzelne Person oder mehrere Quellen «Wikileaks» mit diesen und weiteren Dokumenten beliefert haben. Allerdings scheint es erhärtet, dass im Rahmen einer besseren und effizienteren Vernetzung innerhalb der US-Regierungstellen Klumpenrisiken in Kauf genommen wurden. Dabei scheinen Dokumente unterschiedlichster Klassifizierung auf dem gleichen, gesicherten Netzwerk mit relativ weiten Zugriffsrechten für eine grosse Zahl von Benutzern abgelegt worden zu sein. Sollte sich dies bestätigen, wäre der Diebstahl dieser Dokumente ein klassisches Beispiel für eine verfehlte Informationssicherungsstrategie, wie

sie bereits mehrmals in den MELANI-Halbjahresberichten[23] diskutiert wurde. Dabei geht es in erster Linie darum, nicht nur die Sicherheit der Informationskanäle, Speichermedien und Netzwerke zu gewährleisten, sondern auch im Blick auf den bestimmten Wert einer Information weitergehende Sicherungsmassnahmen im Rahmen eines informierten Risikomanagementprozesses einzuleiten. Eine rein technische „One Size Fits All"-Strategie ohne spezifische Einschränkungen und Zugriffsrechte auch im physischen und personellen Bereich, angepasst an den tatsächlichen Wert einer bestimmten Information muss zwangsläufig zu einem Totalverlust eben dieser Informationen führen.

Ein zweiter Vorfall im Zusammenhang mit «Wikileaks» war die Mobilisierung durch «Anonymous Operation», um - in deren Terminus - mutmassliche «Wikileaks»-Gegner virtuell abzustrafen. Dieser Vorfall ist in Kapitel 3.2 beschrieben.

Die Vorfälle im Umfeld der Dokumentenveröffentlichung durch «Wikileaks» zeigen die ganze Palette der Probleme im Bereich der Informationssicherung auf. Die Weitergabe klassifizierter Dokumente an Dritte ist ein zunehmendes Problem in der Welt der Informations- und Kommunikationstechnologien. Oftmals wird noch zu wenig getan, um Informationen in die Tiefe («in depth») zu sichern, da man sich mit möglichst ausgefeilten technischen Perimetern begnügt. Leider schafft dieser Ansatz in erster Linie ein Klumpenrisiko und trägt weder der Insider-Problematik noch der Tatsache Rechnung, dass nicht jede Information den gleichen Wert besitzt und damit ein Rundum-Schutz in erster Linie die zu schützende Information in Betracht ziehen muss und nicht das Netzwerk, auf dem sie abgelegt ist.

Auch die in der Folge der «Wikileaks»-Debatte ausgeführten «Vergeltungsschläge»" zeigen einmal mehr, wie verwundbar Institutionen und Private gegenüber Angriffen sein können und Cyber-Angriffe die Gefahr von Kollateralschäden schon fast inhärent nach sich ziehen, wie dies auch bei früheren Aktionen, beispielsweise gegen Sex-Seiten-Betreiber in der Schweiz[24], der Fall war. Gerade die klar strafrechtlich relevanten Angriffe auf die PostFinance haben deutlich gemacht, dass hier bei den Beteiligten noch ein grosser Mangel an Sensibilisierung und Rechtsempfinden herrscht. Insofern ist das Durchgreifen der Strafverfolgung in einzelnen Ländern gegen die Mittäter zu begrüssen.

4.3 SSL und Zwei-Faktor-Authentifizierung – Sicherheit für die eigenen Kunden

Im Oktober 2010 veröffentlichte der Programmierer Eric Butler auf seiner eigenen Website eine recht interessante Erweiterung für den Browser «Firefox»: «Firesheep»[25]. Anlässlich der Konferenz «Toorcon» in San Diego analysierte[26] Butler die Gefahr, welche Provider des so genannten *Web 2.0* und in erster Linie Facebook verursachen. Beim Zugang zu einer Website wie Facebook erstellt der Server ein Cookie, das Namen und Passwort des Users enthält.

---

[23] MELANI Halbjahresbericht 2009/1, Kapitel 5.1: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (Stand: 10. Januar 2011) oder MELANI Halbjahresbericht 2009/2, Kapitel 5.1 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (Stand: 10. Januar 2011).

[24] MELANI Halbjahresbericht 2009/2, Kapitel 3.3 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (Stand: 10. Januar 2011) .

[25] http://codebutler.com/firesheep (Stand: 10. Januar 2011).

[26] http://codebutler.github.com/firesheep/tc12/#1 (Stand: 10. Januar 2011).

Wenn die Verbindung zwischen User und Empfänger nicht verschlüsselt ist und der User eine öffentliche WLAN-Verbindung nutzt. Wenn er sich beispielsweise mit dem eigenen Laptop in öffentlichen Gebäuden (z.B. Hotels, Restaurants, Flughäfen usw.) beziehungsweise an einer Konferenz befindet, an der eine Verbindung zur Verfügung gestellt wird, kann das erstellte Cookie gestohlen und verwendet werden, um sich als rechtmässigen User auszugeben. In der Fachsprache wird dies als «*Sidejacking*» bezeichnet. Zum Schutz gegen eine solche Art von Angriff ist eine verschlüsselte Verbindung zwischen User und Empfänger herzustellen. Google hat das Problem im Januar 2010 bei seinem E-Mail-Dienst («Gmail») behoben. Facebook als grösste Website des Jahres 2010 aber noch nicht.

Um zu beweisen, wie einfach ein «Sidejacking» funktioniert, hat Butler «Firesheep» veröffentlicht. Nach Einrichtung der Erweiterung genügt es, sich an einem offenen WLAN anzuschliessen, die Applikation zu starten und abzuwarten, bis sich ein User auf Facebook einloggt. Nun ist es möglich, das erzeugte Cookie zu stehlen und sich in Facebook mit dem Konto der anderen Person einzuloggen. Solches Vorgehen bei fremden Konten ist grundsätzlich strafbar, weshalb wir von der Verwendung von «Firesheep» abraten.

Das geschilderte Szenario stellt ein altbekanntes Problem dar. Bis anhin waren jedoch gewisse Kenntnisse erforderlich, um ein Cookie zu stehlen. Mit «Firesheep» wird das Ganze zu einem Kinderspiel. Die User müssen darauf achten, ausschliesslich Seiten mit *SSL* zu verwenden, wenn sie sich via offenes WLAN verbinden. Diese Vorkehrung haben die Unternehmen bereitzustellen und können nicht vom Nutzer selbständig eingeführt werden. Gleichzeitig weist MELANI darauf hin, dass immer mehr Angriffe gegen Internetdienstleister erfolgen, die zur Authentifizierung nur einen Faktor zur Verfügung stellen. Dies gilt beispielsweise für Onlineversteigerungen, Email-Konten und verschiedene Zahlungssysteme. Auch in solchen Fällen sind die Unternehmen darauf hinzuweisen, dass eine Zwei-Faktor-Authentifizierung das Risiko einer Kompromittierung verringert. Mit dieser Massnahme lassen sich für Unternehmen und Kunden beträchtliche Verluste vermeiden.

4.4 Vorfälle im Zusammenhang mit Emissionsrechtehandel

Bereits Anfangs 2010 fanden Phishing-Angriffe auf Emissionshandelsregister statt, indem Emissionsrechte unrechtmässig transferiert wurden.[27] Eine der dabei geschädigten Firmen verklagte daraufhin die Bundesrepublik Deutschland auf Schadenersatz mit der Begründung, dass die Sicherheitsstandards der zuständigen Behörde unzureichend seien.[28]
In einer Mitteilung kündigte die Deutsche Emissionshandelsstelle (DEHSt) am 16. November an, eine *Zwei-Faktor-Authentifizierung* mittels smsTAN für das Emissionsregister einzuführen.[29]

Am gleichen Tag wurden der rumänischen Tochtergesellschaft eines Schweizer Zementherstellers 1,6 Millionen Emissionszertifikate beim rumänischen nationalen Register entwendet, nachdem Kriminelle mit Hilfe eines Trojaners die Zugangsdaten der Firma ausgespäht hatten. Der verwendete Trojaner «Nimkey» wurde bislang vor Allem gegen

---

[27] Siehe MELANI Halbjahresbericht 2010/1, Kapitel 4.9 http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html (Stand: 10. Januar 2011).

[28] http://www.heise.de/security/meldung/Datenklau-bei-Emissionsrechten-kommt-vor-Gericht-1098072.html (Stand: 10. Januar 2011).

[29] http://www.dehst.de/cln_153/nn_1662430/SharedDocs/Mailings/DE/2010/10-11-16__smsTAN.html (Stand: 10. Januar 2011).

Kunden von amerikanischen Banken eingesetzt. Seine Eigenschaften (u.a. Diebstahl privater Schlüsselzertifikate, Aufzeichnen von Tastatureingaben, Kopieren von Daten aus der Zwischenablage) eignen sich aber auch, um Anmeldeinformationen anderer Dienste abzugreifen – insbesondere wenn es sich dabei nur um Login und Passwort handelt. Das Auftreten von «Nimkey» in diesem Zusammenhang führte dazu, dass verschiedene europäische Emissionshandelsregister Ende November den Handel zumindest kurzzeitig aussetzten.

Anfang Dezember erhielten dann viele Unternehmen eine E-Mail der «European Climate Registry», in welcher die Empfänger dazu aufgefordert wurden, auf einer Website ein Konto zu eröffnen respektive die Logindaten zu validieren. Die Europäische Kommission und die nationalen Register distanzierten sich von diesem Unternehmen: Es sei kein offizielles Register, sondern ein rein privatrechtliches Internetangebot, dessen Seriosität und Nutzen nicht beurteilt werden könne – die Website ist nach wie vor online.[30]

Die Europäische Kommission will die Sicherheitsstandards bei den Emissionshandelsstellen erhöhen. In einer späteren Phase soll der Handel über ein einziges europäisches Register abgewickelt werden.[31] Bis zur Zusammenführung müssen die nationalen Register selbst für genügend Schutz sorgen und sicherere Verfahren einführen. Verschiedentlich wurde dies bereits vollzogen.

Wie bereits in früheren Halbjahresberichten erwähnt,[32] ist eine Verlagerung der Angriffe von Cyberkriminellen weg vom Online-Banking hin zu weniger gut geschützten Diensten und (Handels-)Plattformen feststellbar. Gefährdet sind besonders diejenigen Dienste, welche nur mit Login und Passwort geschützt sind und wenn sich mit dem Zugang direkt oder indirekt Geld verdienen lässt. Betroffen sind neben dem Emissionshandel unter anderem Online-Bezahlsysteme, Auktionsplattformen, E-Mail Provider und soziale Netzwerke.

4.5 NATO übt die Cyberverteidigung und nimmt die Cyberbedrohung in ihr strategisches Konzept auf

Vom 16. bis 18. November 2010 führte die NATO eine Übung namens «Cyber Coalition 2010» durch.[33] Getestet wurden Abläufe und die Koordination zwischen den verschiedenen Akteuren, welche bei einem Cyberangriff auf die NATO und ihre Mitgliedstaaten zusammenarbeiten müssen. Dies war die dritte Übung dieser Art.

Am NATO-Gipfel in Lissabon, welcher vom 19. bis 20. November 2010 stattfand, verabschiedeten die Staats- und Regierungschefs der Mitgliedstaaten ein neues strategisches Konzept des Nordatlantik-Bündnisses, gemäss welchem Cyber-Angriffe als ernsthafte Bedrohung angesehen werden müssen. Konsequent will die NATO deshalb ihre eigenen Fähigkeiten wie auch diejenigen ihrer Mitgliedstaaten weiter entwickeln, um Angriffe auf Computernetze zu verhindern, zu entdecken, sich dagegen zu verteidigen und sich von solchen Angriffen zu erholen. Auch sollen die nationalen Fähigkeiten zur Bekämpfung der Computerkriminalität gestärkt und besser koordiniert werden. Zudem soll die Fähigkeit

[30] Von der European Climate Registry wurde bereits im Sommer 2009 ein entsprechendes Mail versandt. Die Domain „europeanclimateregistry.eu“ ist seit Dezember 2008 auf eine Person in Brüssel registriert.

[31] Richtlinie 2009/29/EC vom 23.04.2009, Punkt (38).

[32] Siehe beispielsweise: MELANI Halbjahresbericht 2008/2, Kapitel 3.6 http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=de (Stand: 10. Januar 2011).

[33] http://www.nato.int/cps/en/SID-70CABE49-11886860/natolive/news_69805.htm

weiterentwickelt werden, zur Energiesicherheit und insofern auch zum Schutz kritischer Energieinfrastrukturen beizutragen.

Die Frage, ob respektive wann Angriffe auf Computernetzwerke als bewaffnete Angriffe qualifiziert werden sollen und einen «Bündnisfall» gemäss Art. 5 des NATO-Vertrages auszulösen vermögen, wurde am Gipfel in Lissabon nicht geklärt. Bis Juni 2011 soll eine detaillierte NATO-Politik zum Schutz vor Cyberkriminalität («cyber defence policy» / «politique de cyberdéfence») entwickelt und ein Aktionsplan für ihre Umsetzung ausgearbeitet werden.

Interessanterweise wurde der in den offiziellen NATO-Sprachen Englisch und Französisch verwendete Begriff «cyber-defence» (engl.) / «cyberdéfence» (franz.) von der Deutschen ständigen Vertretung bei der NATO in der Gipfelerklärung und im strategischen Konzept mit «Schutz vor Computerkriminalität» übersetzt.[34] Dies könnte ein Hinweis darauf sein, dass sich die Bündnispartner (noch) nicht einig sind, ob auf einen Cyber-Angriff eine militärische oder vielleicht doch eher eine zivile Reaktion angemessen ist. Unbestritten ist lediglich die Tatsache, dass auch das Militär in der Lage sein sollte, seine Infrastrukturen zu schützen.

4.6 Trend zu USB-Würmern

USB-Datenträger werden immer häufiger als Verbreitungsweg von Schadsoftware genutzt. «Stuxnet»[35] und «Conficker»[36] sind nur die prominentesten Vertreter dieser Gattung. USB-Speichermedien werden immer billiger und immer häufiger eingesetzt. Zudem sind viele Computersysteme gegen USB-Schädlinge schlechter geschützt als beispielsweise gegen Schädlinge, welche über Netzwerke oder E-Mail verbreitet werden. Gemäss der spanischen Firma «Panda Security» sollen sich 25% der 2010 neu in den Umlauf gebrachten Würmer via USB verbreiten können[37]. Dies geht aus einer Studie hervor, welche in 10'470 Unternehmen aus Europa, Nord- und Lateinamerika durchgeführt wurde. Immer noch ist auf vielen Firmencomputern die Datei autorun.inf, welche das automatische Starten von Programmen ermöglicht, nicht deaktiviert. Durch diese Funktion lassen sich problemlos Schadprogramme installieren, und dies bereits beim Anschluss des USB-Geräts an den Computer.

Der Infektionsvektor USB wird dabei vor allem in Kombination mit anderen Infektionsvektoren benutzt. Das USB-Gerät dient dabei in erster Linie dem Überwinden der Firmen-Firewall. Ist die Schadsoftware erst einmal im Netzwerk der Firma, sind die Hürden für eine Ausbreitung viel kleiner.

Was für Auswirkungen ein privater USB-Stick haben kann, zeigte die eingeschleuste Schadsoftware, welche 2008 in das Netzwerk des Pentagons gelang. Ein Soldat steckte einen mit einer Malware verseuchten privaten USB-Stick in einen am US-Militärnetz hängenden Rechner im Mittleren Osten. Von dort verbreitete sich die Schadsoftware in und über zahlreiche interne Netzwerke, bis er schliesslich auch Zugang zu einem als Geheim

---

[34] http://www.nato.diplo.de/Vertretung/nato/de/04/NATO__Gipfel__Lisboa__1911_Seite.html (Stand: 10. Januar 2011).

[35] Siehe Kapitel 4.1 und 5.1 des vorliegenden Berichtes.

[36] Siehe http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de, Kapitel 4.2 (Stand: 10. Januar 2011).

[37] http://press.pandasecurity.com/news/25-of-new-worms-in-2010-are-designed-specifically-to-spread-through-usb-devices/ (Stand: 10. Januar 2011).

eingestuften Bereich des Netzwerkes bekommen haben soll.[38] Auch die Schadsoftware «Conficker» fand den Weg in verschiedene Firmennetzwerke, darunter Spitäler und Militärnetzwerke.

Gerade für Angriffe gegen Firmen sind USB-Speichermedien als Überträger von Schadsoftware besonders geeignet und deshalb gefährlich. Jede Firma hat mittlerweile gute Abwehrmethoden des Netzwerkes installiert und auch der E-Mail-Verkehr wird in den meisten Fällen zentral gegen Schädlinge überwacht. Schafft es aber ein Schädling via USB über einen Computer eines Mitarbeiters hinter die Firewall in das Firmennetzwerk zu gelangen, stehen dem Schädling Tür und Tor offen. Gerade für gezielte Angriffe und besonders abgeschottete Systeme ist dies ein geeigneter Angriffsvektor. Die Wahrscheinlichkeit, dass ein Mitarbeiter irgendeinmal einen USB-Stick oder andere USB-Geräte wie Fotokamera oder Smartphone sowohl an den privaten wie auch an den Firmencomputer anschliesst, ist dabei sehr gross. Auch eine vorgeschaltete Prüfung von USB-Sticks durch mehrere Anti-Viren-Programme garantiert dabei keinen vollständigen Schutz, da gerade bei gezielt und in kleinen Zahlen eingesetzter Schadsoftware Anti-Viren-Programme in der Regel versagen.

4.7 «Here you have» Computerwurm – «Iraq Resistance»

Am 9. September 2010 begann sich ein bislang unbekannter Computerwurm im Internet zu verbreiten und störte den E-Mail-Verkehr von mehreren amerikanischen Unternehmen. Der Wurm versendete E-Mails mit dem Betreff «Here you have» und E-Mail-Text «This is The Document I told you about, you can find it Here» oder «Just For you» und E-Mail-Text «This is The Free Download Sex Movies, you can find it Here». Dem «Here» war jeweils ein Link zum Schadcode hinterlegt. Der Link verwies vermeintlich auf ein Dokument oder eine Videodatei, tatsächlich lud man sich beim Anklicken jedoch die Schadsoftware auf den Computer und wurde aufgefordert, die Datei auszuführen. Der Wurm verbreitete sich in der Folge über Laufwerkfreigaben und versendete das Mail mit dem Link an Kontakte im Adressbuch. Ausser seiner Verbreitung und dem damit zusammenhängenden Mail-Aufkommen, welches gewisse Server überlastete, richtete der Wurm keine besonderen Schäden an.

Zur Urheberschaft bekannte sich eine Person mit dem *Nickname* «Iraq Resistance», welche vorgab, Teil der bislang unbekannten Gruppe «Tariq bin Ziyad Brigades for Electronic Attack (TbZBEA)» zu sein. Das Ziel des Urhebers bestand jedoch nicht darin, möglichst grossen Schaden anzurichten. Er sei kein Terrorist, teilte er in einer Bekennerbotschaft auf YouTube mit.[39] Die Aktion sei als Protest zu verstehen: zum Einen gegen die US-Invasion des Irak, zum Anderen gegen die für den 11. September 2010 angekündigte Koran-Verbrennung in den USA (welche schliesslich nicht durchgeführt wurde, jedoch aus anderen Gründen).

Die Methode, durch Abgreifen der Adressbücher auf infizierten Systemen und einen zum Klicken verlockenden E-Mail-Text, ist einfaches, aber sehr wirksames «*social engineering*». Den E-Mails wird höheres Vertrauen geschenkt, weil man den Absender kennt und der Text in den Nachrichten ist so allgemein gehalten, dass er für viele Empfänger plausibel klingt. In den Jahren 2000 («I LOVE YOU»-Virus) respektive 2001 («Anna Kurnikova»-Virus) wurden ähnliche Computerwürmer in Umlauf gesetzt, welche ihre Verbreitung mit vergleichbaren Methoden vorantrieben. Eine wichtige Regel beim Umgang mit E-Mails ist

[38] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain (Stand: 10. Januar 2011).

[39] http://www.youtube.com/watch?v=IkMifFGqt78 (Stand: 10. Januar 2011).

deshalb, dass man (auch von bekannten Absendern) unerwartet erhaltene Nachrichten mit Links oder Dateianhängen grundsätzlich vorsichtig behandelt und im Zweifelsfall beim Absender nachfragt, worum es sich genau handelt. Als Dateianhänge wurden in letzter Zeit vermehrt PDF-Dokumente als Infektionsvektor verwendet. Schon der alleinige Klick auf einen Link zu einer präparierten Website oder das Öffnen einer Datei kann dazu führen, dass der Computer infiziert wird.

Der vorliegende «Here you have» getaufte Wurm wurde für politisch und religiös motivierten Cyberprotest in Umlauf gesetzt. Wenn er neben seinen Verbreitungsmechanismen auch noch Anweisungen zu weitreichender Datenbeschädigung enthalten hätte, wäre die Geschichte für einige Unternehmen bedeutend weniger glimpflich ausgegangen.

4.8 Grosses Botnetzwerk durch niederländische Polizei vom Internet getrennt

Die niederländische Polizei hat am Montag 25. Oktober 2010 die Kommandoserver des Botnetzes «Bredolab» vom Netz getrennt. «Bredolab» soll weltweit mehr als 30 Millionen Computer infiziert haben. Die niederländische Polizei hat insgesamt 143 Server, die das Botnetz gesteuert haben, vom Internet getrennt. Parallel dazu wurde auf dem Flughafen von Yerevan ein 27-jähriger Mann verhaftet. Dieser steht im Verdacht, der führende Kopf der Betreiber des Botnetzes zu sein. In den vorangehenden Wochen hatten die Ermittler die Infrastruktur tiefgehend analysiert.

Für den Betreiber des Botnetzes stand dabei vor allem die Verbreitung einer Schadsoftware im Vordergrund. Die verwendete zu diesem Zweck Webseiteninfektionen. Nachdem ein Computer durch die Schadsoftware infiziert worden war, suchte diese nach Login und Passwort von Webseitenadministratoren. Die gefundenen Daten wurden wiederum verwendet, um weitere Websites zu infizieren. Dies geschah vollautomatisch. Die jetzt abgeschalteten Server wurden vom niederländischen Betreiber «Leaseweb» verwaltet. Üblicherweise würden die Server nach der Entdeckung sofort vom Netz genommen, in diesem Falle habe «Leaseweb» die Server jedoch auf Anweisung der Polizei weiter betrieben, damit das Netzwerk analysiert werden konnte.

Der oder die Täter hatten sich hier darauf spezialisiert, ein möglichst grosses Botnetzwerk zu generieren, um Teile davon entweder zu vermieten oder zu verkaufen. Da es sich bei «Bredolab», um einen sogenannten Downloader handelt, kann auf einen Computer, wenn infiziert, nachträglich jede beliebige Schadsoftware nachgeladen werden.

MELANI hat bereits am 9. April 2010 mittels Newsletter auf diese Schadsoftware und auf die erhöhte Gefahr von Webseiteninfektionen hingewiesen[40]. Der Grund der Warnung war, dass das neu entwickelte Checktool der Melde- und Analysestelle Informationssicherung MELANI, welches Schweizer Webseiten auf allfällige Webseiteninfektionen überprüft, eine Vielzahl von mit «Bredolab» infizierten Webseiten entdeckt hatte. Betreiber oder Provider wurden anschliessend kontaktiert, damit sie die Infektionen entfernen.

Eine neuartige Vorgehensweise hat die niederländische Polizei gewählt, um die Benutzer der verseuchten Computer zu warnen. Hierzu werden die entsprechenden Kontroll- und Kommandoserver verwendet, um auf dem jeweiligen infizierten Computer eine *Pop-up*

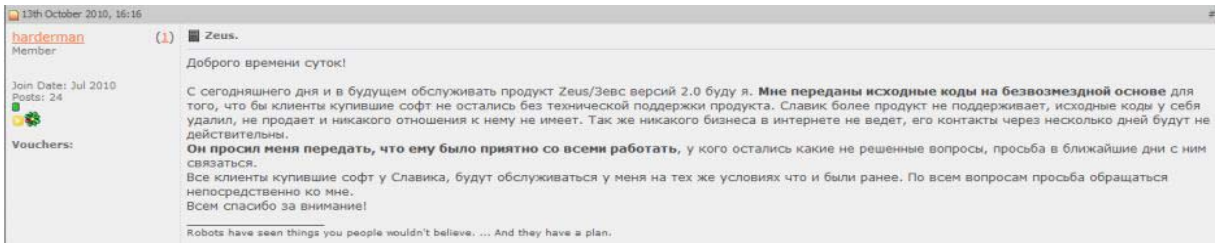
[40] http://www.melani.admin.ch/dienstleistungen/archiv/01107/index.html?lang=de (Stand: 10. Januar 2011).

Warnmeldung auf dem Bildschirm anzuzeigen, dass der Computer mit einer Schadsoftware infiziert ist.

4.9 ZeuS und SpyEye – Fusion zwischen zwei der grössten E-Banking Trojaner?

Der Trojaner «ZeuS» ist wahrscheinlich die meistverbreitete E-Banking Schadsoftware, die derzeit im Umlauf ist. Zu diesem Thema gibt es zahlreiche Berichte, Artikel und Aktivitäten[41].

Ab Anfang 2010 machte eine andere E-Banking Schadsoftware namens «SpyEye» von sich reden. Diese hat eine Funktion mit dem Namen «ZeuS Killer Code» integriert. Damit sollte herausgefunden werden, ob ein zu infizierender Computer bereits «ZeuS» beherbergte. Traf dies zu, wurde der Rivale eliminiert. Somit kam es zu einem eigentlichen Krieg zwischen den beiden Trojanern. Der unter den Pseudonymen «Gribodemon» und «Harderman»[42] bekannte Autor von «SpyEye» wurde in der Untergrundszene zudem vor Kurzem berühmt, als er im Juli ankündigte, der Autor von «ZeuS» habe ihm den Code der Malware sowie die Verwaltung der Kundschaft abgetreten:


13th October 2010, 16:16

harderman (1)
Member

Join Date: Jul 2010
Posts: 24

Vouchers:

Zeus.

Доброго времени суток!

С сегодняшнего дня и в будущем обслуживать продукт Zeus/Зевс версий 2.0 буду я. **Мне переданы исходные коды на безвозмездной основе** для того, что бы клиенты купившие софт не остались без технической поддержки продукта. Славик более продукт не поддерживает, исходные коды у себя удалил, не продает и никакого отношения к нему не имеет. Так же никакого бизнеса в интернете не ведет, его контакты через несколько дней будут не действительны.
Он просил меня передать, что ему было приятно со всеми работать, у кого остались какие не решенные вопросы, просьба в ближайшие дни с ним связаться.
Все клиенты купившие софт у Славика, будут обслуживаться у меня на тех же условиях что и были ранее. По всем вопросам просьба обращаться непосредственно ко мне.
Всем спасибо за внимание!

Robots have seen things you people wouldn't believe. ... And they have a plan.

Abbildung 6: Forumeintrag von «Harderman» in dem er im Juli ankündigt, dass der Autor von «ZeuS» ihm den Code der Malware sowie die Verwaltung der Kundschaft abgetreten hat.

In verschiedenen nachfolgenden Mitteilungen gab «Harderman» öffentlich zu verstehen, die Version 2 von «ZeuS» würde nicht mehr weiter entwickelt werden. Die Gemeinschaft könne jedoch mit einer neuen Malware rechnen, die aus der Fusion zwischen «SpyEye» und «ZeuS» entstehen werde.

4.10 Organisation für Geldwäscherei «J1 Network» zerschlagen

Die Organisation «J1 Network» wurde bekannt, weil sie schmutziges Geld aus Onlineverbrechen wusch. Ihr Name ist darauf zurückzuführen, dass sie Mitglieder hauptsächlich aus ausländischen Studierenden rekrutierte, welche über ein «J1»-Visum für eine Niederlassung in den Vereinigten Staaten verfügten. Verschiedene kriminelle Gruppen, die im Cyberspace tätig waren, hatten ihre Dienste genutzt. Dies galt insbesondere für Banden, die E-Banking Schadsoftware einsetzten, um online Geld von Bankkonten

[41] Die Website von Brian Krebs, einem auf Kriminalität im Cyberspace spezialisierten Journalisten, enthielt beispielsweise 15 Artikel, in denen ZeuS während des besagten Semesters im Zentrum des Geschehens stand: http://krebsonsecurity.com (Stand: 10. Januar 2011). Die Website https://zeustracker.abuse.ch/ (Stand: 10. Januar 2011) enthält über 500 «ZeuS» C&C sowie eine durchschnittliche Identifizierung des schädlichen Codes bei den grössten Antiviren von 36.85%.

[42] Der Blog «MalwareIntelligence» enthält ein Interview mit dieser Person: http://www.malwareint.com/docs/spyeye-analysis-ii-en.pdf (Stand: 10. Januar 2011).

abzuziehen. Das FBI teilte mit, 37 Personen verhaftet zu haben, die der Organisation angehörten[43].

Abbildung 7: Vom FBI gesuchte Personen den J1 Netzwerks.

Die Angeklagten, die sich grösstenteils mit Studentenvisa auf amerikanischem Boden aufhielten, eröffneten bei verschiedenen Finanzinstituten Konten. Dabei verwendeten sie falsche Ausweise. Nach Erhalt des Geldes, das von Onlinekonten gestohlen wurde, behielten sie einen gewissen Prozentsatz für sich. Den Rest schickten sie nach Russland.

Nun wurde die Organisation vom FBI zerschlagen. Das FBI schätzt die Gesamtsumme der gewaschenen Gelder auf rund drei Millionen Dollar.

4.11 Kreditkartenmoneymule

Ende Dezember 2010 machte untenstehendes E-Mail die Runde. Den Empfängern wurde in schlechtem Deutsch schmackhaft gemacht, als so genannter «Kreditkarten*moneymule*» zu agieren. Ihnen würden gestohlene oder gefälschte Kreditkarten per Post zugesendet, mit welchen dann Geld abgehoben und dieses abzüglich einer Provision an den Täter respektive an einen weiteren Finanzagenten gesendet werden sollte. Im E-Mail gab es auch gerade Antworten auf die häufig gestellten Fragen und es wurde schon im Einleitungssatz auf mögliche strafrechtliche Konsequenzen aufmerksam gemacht:

[43] Die Mitteilung des FBI in New York kann unter http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo093010.htm nachgelesen werden (Stand: 10. Januar 2011).

Subject: Unternehmensfuhhrung sucht Teammitglieder

Eine Arbeit fur jemanden der sich im Klaren ist, dass falls was schief gehen sollte er im bestenfalls mit einer Bewahrungsstrafe auskommt , im schlimmsten ....

Ich bin in diesen Business seit 2002, mit mir hat eine Menge Leute gearbeitet , aber nur 2 wurden verhaftet und auch die nur wegen Ihrer Gierigkeit und Dummheit. Jeder einzelne der geschnappt wird, ist nicht nur ein finanzieller Verlust, sondern auch eine grosse Gefahr fur die gesamte Mannschaft. Deswegen sind folgende Regel zu befolgen:

1. Die Vorschriften werden strengstens eingehalten. Das Geld wird nur in den von mir bestimmten Bankautomaten zu der von mir angesagten Zeit abgehoben. Es wird nur die abgesprochene Summe abgehoben. Die Vorschriften fur das Erhalten der Kreditkarten und fur die Gelduebergabe werden strengstens befolgt. 2. Das Geld ist ehrlich abzugeben (keine Tauschungsversuche) 3. Nur anonyme Simkarten benutzen, dieses Telefon fur Anrufe der Freunde und Verwandte nicht verwenden 4. Sich nie mit *Arbeitskollegen* dieses Businesses treffen, wenn sich einer mit dir treffen moechte, arbeitet er zu 99% fur die Bullen 5. Wenn du keine Disziplin hast, die Regeln nicht einhalten kannst, bzw. mich fur paranoid haltst - dann sollen wir keine Zusammenarbeit auch versuchen.

Arbeitsbeginn
Du hollst die Kreditkarte ab. Wo das sein wird gebe ich am Telefon durch (meist bei dir in der Stadt oder in einer Grossstadt in deiner Umgebung. Zusammen mit der Karte erhalst du eine genaue Anweisung wo, wann und wie viel Geld abzuheben ist. Die Anweisung ist 100% genau auszufuhren, davon hangt unser Verdienst und auch deine Sicherheit ab. Fur die erste Karte musst du eine Pfandsumme von 300 Euro hinterlassen. Dies ist fur die Sicherheit, dass falls du alles abhebst und verschwindest, ich meine Kosten fur die Kreditkartenbeschaffung und die Transportkosten zu dir, decke. Du erhalst diese Pfandsumme bei der ersten Abhebung zurück, also bei den ersten Bankautomaten. Fur das erste mal erhallst du eine Kreditkarte und die dazugehorige Pin mit einen Abhebelimit von 1500 Euro. Hebst so viel ab, wie es in der Anweisung angegeben wird. Aus den abgehobenen Geld erhallst du 600 Euro , - 300 als Pfandruckgabe und 300 als dein Verdienst. Das restliche Geld ubergibst du an mich, wie das geschehen soll schreibe ich dir per sms. Weiter erhallst du 2-4 Karten pro Woche (Pfand brauche ich nicht mehr). Zum Anfang werden die Karten mit einen kleineren Guthaben sein 1000 bis 2000 Euro, davon erhallst du 300 bis 600 Euro als deine Provision. Spater, wenn unsere Zusammenarbeit gut verlauft und du alle Regel befolgst, arbeitest du mit Karten mit maximalen Guthaben, wo du pro Karte bis zu 1500 Euro verdienen kannst.

Um die Arbeit starten zu konnen, brauchst du eine anonyme Simkarte die du in jeden zweiten Internetkafe oder Callcenter erhalten kannst. So bald du diese hasst, teilst du mir die Nummer an meine Email: mit. Weiter schreibe ich dir eine Sms was du weiter zu tun hasst.

Gleich die Antworten auf meisstgestellte Fragen:
1. Was fur Garantien habe ich, dass Sie mit meinen 300 Euro nicht verschwinden?

An.: Gar keine, aber anders wird es nicht gehen. Wenn du Angst um 300 Euro hasst (vielleicht ist es eine grosse Summe fur dich) dann hoere ich von dir zu 100% nichts mehr, so bald du um die 5000 Euro abgehoben hasst.

2. Ich habe keine 300 Euro, kann ich als Garantie meinen Pas, meinen Studentenausweis, mein Wort, meine Freundin , meinen Arsch, etc. hinterlassen?

An: NEIN, ich stelle jeden Tag einen neuen Mitarbeiter an, meine Ausgaben pro Kartenzubereitung und den Transport zu dir sind ca. 300 Euro und falls du mit der Karte verschwindest habe ich 300 Euro Verlust- das muss nicht sein.

P.S So lange du nicht probierst an Geld zu kommen, weisst du nicht wo fur du geboren bist. Dein Leben lang auf Hartz 4 zu sitzen bzw. fur 1000 Euro im Monat deinen Arsch aufzureissen oder einige Male deinen Mut zusammen zu nehmen und vom Leben alles zu bekommen versuchen. Die, welche Mut und Nerven genug haben, diese Arbeit an zu nehmen, werden in ca. einen halben Jahr zu wohlhabenden Menschen und kriegen mit, dass das Geld nicht alles ist. Bevor du also meinen Angebot annimst uberlege ernsthaft ob du es wirklich brauchst und durchziehen kannst!!!

Moneymules oder sogenannte Finanzagenten sind bei Kriminellen rar und deshalb sehr gefragt. Normalerweise werden diese verwendet, um Geld aus betrügerischen Bankzahlungen zu waschen. Dazu werden mehr oder weniger plausible Geschichten erfunden, damit das Opfer keinen Verdacht schöpft, dass es sich bei diesen Transaktionen um einen Betrug respektive um Geldwäscherei handeln könnte. Im vorliegenden Fall verhält es sich anders, da der Täter offen zu einer Straftat aufruft und auch noch Tipps gibt, wie man verhindern kann, dass man erwischt wird. In der Tat ist beim Kreditkartenmoneymule die Gefahr kleiner, erwischt zu werden. Währendem bei E-Banking Betrug der Finanzagent als Empfänger fungiert und schon bei der ersten betrügerischen Zahlung auffällt und aus dem Verkehr gezogen wird, ist hier die Rückverfolgbarkeit schwieriger. Deshalb ist das E-Mail auch bewusst nicht darauf angelegt, unwissende Leute zu rekrutieren, sondern richtet sich an Personen mit einem kriminellen Potential. Nicht ausgeschlossen werden kann jedoch,

dass es sich hier um eine Spielart des Vorschussbetrugs handelt und der interessierte Bewerber nach dem Versand der 300 Euro Einstiegsgebühr nie mehr etwas von seinem «Arbeitgeber» hört. Der Täter muss in diesem Falle kaum mit einer Anzeige rechnen, da das Opfer ja selber versucht hat, kriminell zu werden.

5 Tendenzen / Ausblick

5.1 «Stuxnet» - der Beginn der SCADA Trojaner

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 hat in den letzten Jahren in diesem Bereich grosse Veränderungen gebracht. Thermometer, Druckmesser, Pumpen, Schalter und weitere sogenannte Feldelemente verfügen heute häufig über eine eigene IP-Adresse und nutzen *TCP/IP* 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: Malware sowie Angreifer («Hacker») halten Einzug. Entsprechend werden in dieser Hinsicht vor allem die internationalen Kontakte und eine vertiefte Zusammenarbeit zwischen Staat und Betreibern kritischer Informationsinfrastrukturen in diesem Bereich angestrebt, um zeitnah Informationen über neu auftretende Gefahren und Abwehrmassnahmen auszutauschen. MELANI steht in engem Kontakt mit den Schweizer Stromversorgern und beteiligt sich am internationalen Informationsaustausch wie beispielsweise im Rahmen des «European SCADA and Control Systems Information Exchange» EuroSCSIE.

Trotz zahlreicher Spekulationen, wer hinter der Schadsoftware «Stuxnet» steckt, ist die Täterschaft immer noch unbekannt – und sie wird es wahrscheinlich auch bleiben. Solche Angriffe leben gerade von dem Vorteil, dass die Rückverfolgbarkeit extrem schwierig bis unmöglich ist. Mit geringem Risiko kann man eine grosse Wirkung erzielen. Da die finanzielle Absicht bei diesem Angriff von untergeordnetem Interesse und die Motivation eher politischer Natur sein dürften, liegt die Vermutung eines staatlichen Eingriffs nahe. Die Möglichkeiten elektronischer Spionage und Sabotage sind in Nachrichtendienstkreisen seit längerem bekannt und werden auch aktiv genutzt. «Stuxnet» ist nur der erste Fall, welcher weltweit grosse Beachtung fand. Anders als Terroristen suchen Staaten ihre Ziele sorgfältig aus und greifen nur diejenigen Anlagen an, deren Störung als unumgänglich eingestuft wird, um nationale Interessen zu schützen. Bei entsprechend hoher Motivation und ausreichenden Ressourcen kann praktisch jedes System früher oder später infiltriert und sabotiert werden. Es ist davon auszugehen, dass sich ähnliche Angriffe in Zukunft wiederholt ereignen werden.

5.2 DDoS – Hintergründe und Motivationen

Angriffe auf die Verfügbarkeit von Webseiten, so genannte Distributed Denial of Service (DDoS) Angriffe werden in der Cyberwelt für verschiedene Zwecke eingesetzt. Zu Beginn erfolgten Angriffe vor allem als einfache Vandalenakte. Inzwischen haben sich die Motivationen aber gewandelt. Man beobachtet beispielsweise DDoS als Rachewerkzeug, für die Schädigung der Konkurrenz, für Schutzgelderpressung oder politisch motivierte Angriffe. Während kleinere DDoS Angriffe meist im Verborgenen bleiben und nicht an die Öffentlichkeit gelangen, gibt es immer wieder grössere DDoS-Angriffe, welche darauf

abzielen, eine grosse (Medien-)Aufmerksamkeit zu erreichen. Webseiten respektive Webserver gehören dabei zu den bevorzugten Zielen. Es können aber auch Mailserver, DNS-Server, Router und Firewalls oder andere Arten von Internetdiensten betroffen sein. Nachfolgend werden verschiedene Motivationen der Täter beschrieben.

Politische Angriffe

Politisch motivierte Anfgriffe, stellen kein neues Phänomen dar. Die Hacker bedienen sich vielfältiger illegaler oder zumindest zweifelhafter Mittel, um Aufmerksamkeit für ihre Anliegen zu gewinnen. Häufige Anwendung finden DDoS-Angriffe oder das Verunstalten von Webseiten.

Prominentestes Beispiel einer politisch motivierten DDoS-Attacke war der Angriff gegen Estland, welcher im Jahr 2007 statt gefunden hat. Nach einem Streit um die Verlegung eines sowjetischen Kriegerdenkmals in der Hauptstadt Tallinn waren estnische Webseiten wochenlang nicht erreichbar. Aber auch als kriegsunterstützende Massnahmen werden DDoS Angriffe eingesetzt. Bei den Kampfhandlungen im Konflikt um die abtrünnigen Republiken Südossetien und Abchasien im Jahre 2008 waren ebenfalls viele offizielle georgische Internetseiten nicht mehr erreichbar oder wurden verunstaltet. Betroffen von den Attacken waren insbesondere georgische Regierungsseiten. Ein Jahr später, zum Jahrestag der russischen Offensive, wurden DDoS-Angriffe gegen «Twitter», «Facebook» und «LiveJournal» beobachtet, die einem georgischen *Blogger*[44] mit Namen «Cyxymu»[45] galten, der sich in seinen Blogeinträgen jeweils kritisch zur russischen Kaukasus-Politik äusserte.[46] Eine DDoS-Attacke, welche ebenfalls politisch motiviert gewesen sein dürfte, richtete sich im April 2008 gegen das durch die USA unterstütze «Radio Free Europe» in Weissrussland. Die Attacke startete am Jahrestag der atomaren Katastrophe von Tschernobyl. An diesem Tag sendete das Radio die Live-Übertragung einer Protestaktion in Minsk, welche an die Not der Opfer erinnerte und sich gegen einen Erlass der Regierung zum Bau eines neuen Atomkraftwerkes aussprach. Angeblich wurde die Website des Senders während des Höhepunkts der Attacke mit bis zu 50'000 Befehlen pro Sekunde überflutet.

Auch in der Schweiz haben bereits politisch motivierte DDoS Angriffe stattgefunden. Die mutmasslich erste politisch motivierte DDoS-Attacke in der Schweiz fand 2007 statt. Damals war die Verfügbarkeit der Internetseite der Parlamentsdienste (parlament.ch) für mehrere Tage beeinträchtigt. In kurzen Abständen wurden Suchanfragen gestellt, die lange Resultatlisten erzwangen, was die Antwortzeit des Servers beeinträchtigte. Das genaue Motiv, welches hinter dieser Attacke stand, wurde nie geklärt, das Ziel lässt aber dennoch einen politischen oder zumindest nicht finanziellen Hintergrund vermuten.[47] Drei Jahre später, im November 2010, wurden die Webseiten von vier Bundesratsparteien angegriffen. Auch hier wurde eine politische Motivation vermutet, insbesondere weil der Angriff in die Zeit vor der Abstimmung über die Auschaffungsinitiative gefallen ist (siehe Kapitel 3.1). Klar hingegen ist die Motivation beim DDoS-Angriff gegen die PostFinance im Dezember 2010 nach der Kontoschliessung des «Wikileaks»-Gründers Julian Assange. Speziell bei diesem Angriff war, dass sich «Wikileaks»-Sympathisanten ein Programm namens Low Orbit Ion Canon herunterladen und einsetzen konnten, welches dann die Anfrageflut gegen die PostFinance ausgelöst hat (siehe Kapitel 3.2). Eine solche Vorgehensweise wurde schon

---

44 http://news.cnet.com/8301-27080_3-10305200-245.html (Stand: 14. Februar 2011).

45 http://cyberinsecure.com/distributed-denial-of-service-attack-takes-down-twitter/ (Stand: 14. Februar 2011).

46 http://wwwguardian.co.uk/world/2009/aug/07/georgian-blogger-accuses-russia (Stand: 14. Februar 2011).

47 Siehe MELANI-Halbjahresbericht 2007/2, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01048/index.html?lang=de (Stand: 14. Februar 2011).

beim DDoS Angriff gegen Estland beobachtet. Damals wurde ein Skript, das IP-Adressen und DNS-Server von rund 18 estnischen Websites mit Pings überflutete, in russischsprachigen Foren herumgereicht.

Erpressung und Schädigung der Konkurrenz

Für Firmen, welche einen grossen Teil ihrer Geschäfte über das Internet abwickeln, bedeutet ein Ausfall der Web-Infrastruktur einen grossen finanziellen Schaden. Dieser Schaden kann bei einem mehrtägigen Ausfall bis zur existenziellen Bedrohung reichen. Hier setzen die Kriminellen an und benutzen ihre Botnetzwerke, um bei Firmen, welche im Internet aktiv sind, Gelder zu erpressen. Das Vorgehen erinnert dann auch stark an Schutzgelderpressung. Das nachfolgende Beispiel illustriert, wie ein solches Erpresserschreiben aussehen kann.

Sehr geehrter Shop-Admin,

am , um 12:00 Uhr werden wir Ihren Shop für 30 Minuten unerreichbar für Sie und Ihre Kunden machen.

Dies hat folgenden Grund:

Wir werden Ihren Online Shop mit einfachen DDoS attackieren, so dass weder Sie, noch Ihre Kunden Zugriff auf Ihre Webseite, geschweige denn auf den Server haben.

Dies wird nur ein kleiner Testlauf sein damit Sie sehen wie ernst es uns ist!

Wir bieten Ihnen hiermit die Option an, weder die Testattacke noch den folgenden DDoS zu bekommen, indem Sie bis morgen 300 Euro in Form eines Ukash Vouchers (an jeder Tankstelle zu erhalten) uns via eMail, an die angegebene E-Mail Adresse (@) senden.

Informationen über Ukash finden Sie auch auf http://www.ukash.com oder an Ihrer Tankstelle.

Sollte bis morgen 11:45 Uhr kein Ukash Code eingegangen sein, so werden wir um Punkt 12:00 Uhr den DDoS starten, anfangs nur für 30 Minuten. Falls Sie nicht zahlen wird Ihr Service für längere Zeit offline bleiben,was ihren Umsatz wohl stark sinken lassen wird.

Abbildung 8: Erpresserschreiben an einen Webshop Besitzer

Der Betreiber des Webshops hat dann die Möglichkeit, zu zahlen oder sich auf den Angriff einzulassen und diesen mit Hilfe seines Providers abzuwehren. Je nach der Grösse des dahinterliegenden Botnetzwerks ist dies aber sehr schwierig und kann nicht zuletzt mit einer Kündigung seitens Provider enden. In der Schweiz wurden bis anhin vor allem DDoS Angriffe gegen Seiten des Sexgewerbes beobachtet. Schon im Herbst 2007 wurden verschiedene solche Seiten unter Anderem über ein Botnet angegriffen. Obwohl die Eigentümer mehrmals den Provider gewechselt haben, war das Portal über mehrere Monate nicht erreichbar. Auch waren schon die grossen Provider Swisscom und Cablecom durch DDoS-Angriffe betroffen. Die Angriffe galten hier aber nicht dem Provider selbst, sondern deren Kunden[48].

Das Gefährliche an solchen Angriffen ist, dass sie Auswirkungen auf die restliche Netzinfrastruktur haben können und schlimmstenfalls das ganze Netz beeinträchtigen. In der realen Welt wäre dies vergleichbar mit dem Anschlag auf eine bestimmte Person in einem Gebäude. Um an die Person heranzukommen, wird gerade das ganze Gebäude dem

[48] MELANI Halbjahresbericht 2009/1, Kapitel 3.4 http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (Stand: 14. Februar 2011) und MELANI Halbjahresbericht 2009/2, Kapitel 3.3 http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (Stand: 14. Februar 2011).

Erdboden gleichgemacht. Weitere Personen, die sich zum falschen Zeitpunkt im Gebäude befinden und ebenfalls zu Schaden kommen, werden als Kollateralschäden durch die Angreifer bewusst in Kauf genommen.

Rachewerkzeug

Unter Cyberkriminellen ist Denial of Service schon lange ein Werkzeug, um sich lästige Konkurrenten vom Hals zu halten, respektive potentielle «Kunden» zu überzeugen, auf die eigenen Netze respektive Dienste zu wechseln. Konkurrenten oder unliebsame Kommentare werden dabei konsequent abgestraft. Nebst der Konkurrenz stehen vor allem IT-Sicherheitsfirmen im Visier der Kriminellen. So hatte beispielsweise der «Storm Worm» einen Mechanismus eingebaut, um Seiten von Online Viren-Scannern mittels DDoS Angriff anzugreifen und lahmzulegen und somit das eigene Botnetzwerk vor Entdeckung zu schützen. Ein anderes Beispiel betraf die Sicherheitsfirma IBM/ISS, deren Experten die Struktur eines Botnetzwerkes untersucht haben. Kurzum wurde die Internetanbindung des Unternehmens für mehrere Tage mittels DDoS gestört.[49]

Da die Angriffe nicht immer nur auf ein spezifisches Ziel (meist eine Website) gerichtet sind, sondern auf die unterliegende Infrastruktur der (Hosting-)Provider, werden auch andere Internetauftritte und Netzwerke in Mitleidenschaft gezogen. Im besten Falle entstehen dadurch nur finanzielle Einbussen für die Unbeteiligten, im schlechtesten Falle können weitaus kritischere Prozesse, die vom angegriffenen Netzwerk abhängen, gestört oder unterbrochen werden.

5.3 Mobile (in)security

Als erster Smartphone-Virus machte der Wurm «Cabir», welcher sich über die Bluetooth Schnittstelle verbreitete, im Jahr 2004 auf sich aufmerksam. Abgesehen davon, dass er für leere Akkus verantwortlich war, da er ständig nach erreichbaren *Bluetooth*-Geräten suchte, richtete er allerdings keinen grossen Schaden an.

Lange ist man davon ausgegangen, dass die Virengefahr für *Smartphones* gering ist, da Smartphones für die Malware-Industrie kein lohnendes Ziel darstellen. Gründe dafür sind die Vielzahl der Betriebssysteme, die schwierige Verbreitung von Malware und die fehlenden „Computer-Crime-Geschäftsmodelle“. Die zunehmende Verbreitung von Smartphones und Mobiltelefonen mit PC-artiger Funktionssausstattung, sowie die Speicherung sensibler Daten auf diesen Geräten, macht diese aber zunehmend auch für Kriminelle attraktiv.

Mit der Etablierung und Konzentrierung von Mobiltelefonbetriebssystemen, wie sie im Moment stattfindet[50], steigt zudem die Gefahr von Vorfällen mit Schadsoftware, wie man sie auch vom Computer her kennt. Der Weckruf war sicherlich eine kritische PDF-Lücke auf dem iPhone im August 2010, welche für grosses Medieninteresse gesorgt hat. Wenn eine präparierte PDF-Datei mit dem Browser «Safari Mobile» geöffnet wurde, liess sich auf den Apple-Geräten «iPhone», «iPad» und «iPod Touch» ein *Jailbreak* vornehmen. Dass eine solche Lücke auch für Kriminelle interessant ist, liegt auf der Hand. Aber auch für das «Android»-Betriebssystem wurde im August der erste SMS-Trojaner gesichtet. Als Mediaplayer getarnt versendete er nach der Installation kostenpflichtige SMS. Zwar war die

[49] http://www.tecchannel.de/sicherheit/news/1737083/storm_worm_schlaegt_zurueck_it_security_forscher_angegriffen/ (Stand: 17. Februar 2011).

[50] http://www.zeit.de/digital/mobil/2011-02/nokia-microsoft-wp7 (Stand: 17. Februar 2011).

Installation umständlich und erforderte viel Benutzerinteraktion. Trotzdem liessen sich auch hier Benutzer dazu verleiten, die Installation durchzuführen. Auch eine Schadsoftware, die sich als «Angry Bird»[51] ausgibt, das Spiel «Tap Snake», das nicht nur ein Spiel ist[52], oder vor kurzem «Geinimi»[53] hatten es auf «Android»-Handys abgesehen.

ZeuS Mitmo: Man-in-the-mobile

Im Untergrund gibt es Bestrebungen für weitere Innovationen. So gibt es beim wohl meistverbreiteten E-Banking Trojaner «ZeuS Anzeichen», dass sich dieser auch die Mobile Welt zu Nutze macht. Die spanische Sicherheitsfirma «S21» veröffentlichte kürzlich einen Artikel über eine Variante, die angeblich verwendet wird, um die Systeme zur Zwei-Kanal-Authentifizierung anzugreifen, die als zweiten Kanal das Mobiltelefon verwenden[54]. Dabei werden dem Benutzer des Computers, der mit dieser speziellen Version von «ZeuS» infiziert ist, während der E-Banking-Session verschiedene Fragen zu seinem Mobiltelefon inklusive Telefonnummer gestellt. Danach wird dem Opfer erklärt, dass das Finanzinstitut aus Sicherheitsgründen ein neues Zertifikat an das Mobilfunktelefon sende (die Nummer ist ja jetzt dem Betrüger bekannt), welches dann zu installieren sei. Mit diesem angeblichen Zertifikat infiziert man nun auch noch das Mobiltelefon. Zum Zeitpunkt der E-Banking-Transaktion, wenn die Bank via SMS den Authentifizierungscode schickt, ist diese Mitteilung für den Kunden nicht sichtbar. Sie wird vielmehr dem Betrüger zugestellt, der dann das Login vornehmen kann.

Es ist voraussehbar, dass E-Banking Benutzer ihre Transaktionen in Zukunft vermehrt auch über ihr Mobiltelefon abwickeln werden. Das stellt Finanzinstitute vor neue Herausforderungen, nicht nur weil das Mobiltelefon noch nicht über die gleiche Absicherung verfügt wie ein „normaler“ Computer. Gerade bei der Zwei-Kanal Authentifizierung SMS-TAN ergeben sich so neue Möglichkeiten, den E-Banking Benutzer zu täuschen, abgesehen davon, dass somit das Smartphone nicht mehr als unabhängiger Authentifizierungskanal gebraucht werden kann. Diese Gefahren sind sicherlich noch nicht unmittelbar, trotzdem müssen solche Gedanken schon jetzt in die Planung der nächsten Generation E-Banking Authentifizierung eingehen.

Spionage-Applikationen für Mobiltelefone

Im zweiten Semester 2010 wurden zahlreiche Applikationen veröffentlicht, mit welchen Gespräche, Mitteilungen und weitere persönliche Daten (Agenda, GPS usw.) auf mobilen Geräten ausspioniert werden können. Nebst den bereits bekannten Programmen «FlexiSpy» und «SpyPhone» fanden sich darunter neue Namen wie «Phone Creeper» oder «Remote iPhone Spy». Die Entstehung zahlreicher Applikationen für Spionagezwecke wirft verschiedene Fragen auf: Sind diese oder ähnliche Funktionen auch bei anderen, vordergründig harmlosen Applikationen eingebaut? In welchem Rahmen dürfen Spionage-Apps überhaupt verwendet werden? Eine mögliche Antwort auf letztere Frage liefert die Verhaftung von 50 Personen in Rumänien, die Spionage-Applikationen für Mobiltelefone verwendet hatten[55]. Zu den gängigsten Motiven gehörte es, dem Ehepartner oder einem Konkurrenten nachzuspionieren.

---

[51] http://www.heise.de/security/meldung/Android-Luecken-ermoeglichen-heimliche-Installation-von-Apps-1134661.html (Stand: 10. Januar 2011).

[52] http://www.f-secure.com/weblog/archives/00002011.html (Stand: 14. Februar 2011).

[53] http://blog.mylookout.com/2010/12/geinimi_trojan/ (Stand: 14. Februar 2011).

[54] http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html (Stand: 14. Februar 2011).

[55] http://www.theregister.co.uk/2010/07/01/romanian_spyware_arrests/ (Stand: 14. Februar 2011).

Nicht nur Smartphone: GSM-Angriff und SMS of Death

Auch wenn für die Smartphones viel Werbung gemacht wird, beträgt ihr Anteil am weltweiten Mobiltelefonmarkt momentan nur 19%[56]. Die Forscher Collin Mulliner und Nico Golde stellten deshalb am «Chaos Communication Congress»[57] ein mögliches Szenario vor, um «normale» Mobiltelefone anzugreifen, die den Hauptanteil des weltweiten Marktes ausmachen. Der Angriff erfolgte mittels eines simplen SMS, das präpariert wurde, um den *binären* Angriffs-Code zu transportieren. Dieses Prinzip nutzen übrigens auch Mobilfunkprovider, um auf den Mobiltelefonen Konfigurationen vorzunehmen oder zusätzliche Dienste einzurichten. Der gezeigte Angriff hat zur Folge, dass das Mobiltelefon zum Absturz gebracht wird.

Die Attraktivität des Mobiltelefons als Angriffsziel für Malware-Attacken und Datendiebstahl wird von zwei Hauptfaktoren bestimmt: Erstens, je mehr das Mobiltelefon dieselben Funktionen wie ein PC erfüllt (Internetzugang, Speicherung sensibler Daten, Abwicklung von Finanztransaktionen etc.), desto mehr wird es zu einem lukrativen Angriffsziel für Kriminelle. Zweitens, analog zur Malware welche auf den PC abzielt, kann auch für Mobiltelefon-Malware davon ausgegangen werden, dass mit der Grösse des «Zielpublikums» auch die Attraktivität eines Angriffs wächst. Es ist also damit zu rechnen, dass moderne Mobiltelefone mit zunehmender Verbreitung ein immer attraktiveres Angriffsziel darstellen. Durch diese Entwicklungen dürften sich in Zukunft die Sicherheitsprobleme aus dem Internet in die mobile Welt übertragen. Smartphones werden sich in den kommenden Jahren immer mehr zu kleineren Personal Computern entwickeln. Schon jetzt ist die Unterscheidung zwischen Smartphone, Tablett-PC und Notebook fliessend. Ein Unterschied ergibt sich aber in der Absicherung der Systeme. Während auf Computern Sicherheitsprogramme zum Standard gehören, sind diese im Smartphone Bereich praktisch nicht existent. Ausserdem sind mehr als 85 Prozent der weltweit eingesetzten Mobiltelefone so genannte «Feature Phones», einfache Geräte mit nur geringem Funktionsumfang wie beispielsweise dem Abspielen von mp3-Dateien und vor allem keiner Update Möglichkeit[58]. Aber auch bei den restlichen Smart-Phones wird ein Update erfahrungsgemäss nicht sofort eingespielt, da dieses an den Computer angeschlossen werden muss und nicht wie beim PC gewohnt im Hintergrund über das Netzwerk funktioniert.

5.4 „Cloud Computing“ - Vorsichtsmassnamen

Nicht erst seit gestern kursiert der Begriff *«Cloud»* im Zusammenhang mit der Art und Weise wie Private, Unternehmen und Verwaltungen mit ihren Dokumenten, Applikationen und dergleichen umgehen sollen. Das Prinzip dahinter ist dabei relativ einfach und genau genommen eine Rückkehr zu den Anfängen der Computer und Netzwerke. Anstelle von ausgewachsenen Client-Systemen, auf denen alles verwaltet wird von Betriebssystem, über Applikationen bis hin zu Dokumenten, soll in der Cloud der Computer zu Hause oder am Arbeitsplatz in erster Linie als Terminal fungieren. Benötigte Textverarbeitungsprogramme, Daten und weitere Applikationen liegen zentral auf einem Rechner und werden über eine Netzwerkanbindung zur Verfügung gestellt. Der Vorteil einer solchen Lösung liegt dabei auf der Hand. Anstelle des Administrationsaufwandes für jeden einzelnen Computer und den darauf enthaltenen Programme und Daten, kann man sich in der Cloud auf die zentralen Systeme konzentrieren. Patch-Zyklen betreffen nur noch ein System und jeder daran

[56] http://www.gartner.com/it/page.jsp?id=1466313 (as of 14 February 2011).

[57] Chaos Communication Congress (Berlin, 27.-30. Dezember 2010).

[58] http://www.wired.com/threatlevel/2010/12/simplest-phones-open-to-%25E2%2580%259Csms-of-death%25E2%2580%259D/ (Stand: 10. Januar 2011).

angebundene Benutzer verfügt immer über die neusten und dem letzten Stand entsprechenden Applikationen. Auch Dokumente werden so einfacher und von überall zugänglich gemacht, da sie nicht mehr nur Lokal auf einem *Netzwerk-Share* oder einem Computer existieren.

Allerdings wirft dieser Ansatz schon lange diskutierte Fragen und Sicherheitsbedenken auf. Das Information-Ownership wird de facto aus der Hand gegeben und das ganze Vertrauen betreffend die Sicherung von Daten liegt in den Händen eines Dritten. Insofern ist der Trend hin zum Cloud-Computing auch ein Trend hin zurück zum blinden Vertrauen in die Techniker und IT-Sicherheitsexperten. Gerade diese Entwicklung aber war in den letzten Jahren in Umkehr begriffen, da die Sicherheit von Netzwerken und IT generell vermehrt von Unternehmen und Verwaltungen nicht mehr nur als Unterstützungsfunktion, sondern auch als strategische Werte erkannt wurden. Insofern stellt sich in absehbarer Zeit ein klassischer Zielkonflikt zwischen tieferen Transaktionskosten, effizienterer technischer Sicherheit und der Tendenz, sich mit angepassten technischen, personellen und physischen Sicherungsmassnahmen um Informationen innerhalb des Unternehmens zu kümmern.

Auch auf Seiten der Cloud-Anbieter stellen sich im Moment noch einige Probleme. So werden bei den meisten die Daten der Kunden und angebotenen Dienste nicht lokal und statisch immer am gleichen Ort belassen, sondern über mehrere Rechenzentren verteilt verschoben und nach Bedarf zusammengestellt. Insofern ist ein klare Aussage, wo genau sich welches Dokument wann genau befindet nicht machbar. Dies wirft auch rechtliche Fragen auf, denn je nach Land in dem sich zu einem bestimmten Zeitpunkt ein bestimmtes Dokument befindet, gelten verschiedene Gesetze.

5.5 Netzmonopole – ein Sicherheitsproblem?

Wenige grosse Akteure des Netzes sind in der Lage, die Entwicklung des Internets und der Netzinfrastrukturen zu beeinflussen[59]. 2010 wurden hier verschiedene Rekorde aufgestellt. Diesbezüglich stellt sich die Frage, wie sich solche Konzentrationen auf die Sicherheit auswirken.

Mit einem Anteil von fast 6,4% am gesamten Internetverkehr stellte Google einen neuen Verkehrsrekord auf[60]. Wenn Google ein ISP wäre, würde es sich gemäss Arbor Networks um den weltweit zweitgrössten handeln. Als grösster Provider gilt derjenige, der mehrheitlich für den Transitverkehr bei Google zuständig ist.

[59] Man denke beispielsweise nur an Googles Initiative, eine Glasfaserinfrastruktur einzurichten, die es dem Durchschnittsamerikaner ermöglicht, mit einer hundert Mal höheren Geschwindigkeit als bis anhin im Web zu surfen. - http://googleblog.blogspot.com/2010/02/think-big-with-gig-our-experimental.html (Stand: 10. Januar 2011). Oder man denke an die Ziele von Mark Zuckerberg, dem Vater von Facebook, der mit seiner Plattform zum Eintrittstor ins Web werden möchte (http://www.wired.co.uk/news/archive/2010-11/04/facebook-mobile-platform (Stand: 10. Januar 2011) http://www.spiegel.de/wirtschaft/unternehmen/0,1518,719920,00.html (Stand: 10. Januar 2011) http://www.ustream.tv/recorded/3848950 (Stand: 10. Januar 2011) http://www.newyorker.com/reporting/2010/09/20/100920fa_fact_vargas (Stand: 10. Januar 2011).

[60] http://asert.arbornetworks.com/2010/10/google-breaks-traffic-record/ (Stand: 10. Januar 2011).

Facebook wurde zur meistbesuchten Website in den Vereinigten Staaten[61] und überholte somit das Branchenschwergewicht Google.

Gemäss den Aussagen von «BitTorrent»[62], welche die File-Sharing-Programme «BitTorrent» und «µTorrent» vertreibt, verwenden hundert Millionen Benutzer eine der beiden vom Unternehmen hergestellten Software. Das Content-Management-System (CMS) «Drupal gab» seinerseits bekannt, dass bereits 1% aller Websites mit dieser Software verwaltet wird[63].

Laut «Twitter» wurden in Japan unmittelbar nach dem Beginn des Jahres 2011 über 7'000 Tweets pro Sekunde veröffentlicht. Auf beeindruckende Weise zeigte das Unternehmen in seiner Publikation auf einer Karte, wie in den verschiedenen Zeitzonen der Welt während Neujahr Tweets veröffentlicht wurden[64].

Malware-Infektionen

Eine Webseiteninfektion auf einer grossen Plattform ist wohl der Albtraum eines jeden IT-Sicherheitsexperten. In diese Richtung gehen die Vorfälle mit kompromittierten Ad-Servern, wie in Kapitel 3.13 beschrieben. Wenn es gelingt, Ad-Server von grossen Zeitungen zu knacken, ist eine grosse Reichweite garantiert. Der Computer Wurm «Koobface» hat es hingegen speziell auf Benutzer des Social Networks Facebook abgesehen und infiziert dort unzählige Besucher. Dabei wird «Koobface» über Drive-By Infektionen und Facebook-Meldungen verbreitet, welche den Empfänger auffordern eine Datei herunterzuladen und auszuführen. *P2P-Plattformen* werden als Infektionsvektor oft unterschätzt. Nebst dem eigentlichen Dokument können Filme, Musik oder Software, die von P2P-Netzen stammen, auch einen Trojaner oder Dropper enthalten. Eine weitere Gefahr ergibt sich im Zusammenhang mit den am häufigsten verwendeten CMS wie «Drupal» oder «WordPress». Durch eine Sicherheitslücke in einer solchen Software («WordPress» hat bereits solche verzeichnet) wären Hunderttausende von Websites vor Angriffen nicht mehr sicher. Denkbar wäre auch ein Angriff auf den *Domain Name Service (DNS)* von wichtigen Websites, um den Benutzern präparierte Kopien der angeforderten Webseiten unterzujubeln, um diese so zu infizieren[65].

Verwendung persönlicher Daten

Grosse Unternehmen wie Facebook sammeln eine riesige Anzahl Daten. Google StreetView fotografierte nicht nur Strassen für die eigene Karte, sondern sammelte auch Daten zu den unterwegs angetroffenen Wireless-Anschlüssen[66]. Websites wie «Groupon.com» tragen wichtige Daten über die eigenen User wie Geolokalisierung und Vorlieben zusammen. «Foursquare.com» weiss genau, wer sich wann wo befindet[67]. Dies ermöglicht einerseits das

---

[61] http://www.hitwise.com/us/press-center/press-releases/facebook-was-the-top-search-term-in-2010-for-sec/ (Stand: 10. Januar 2011).

[62] http://www.bittorrent.com/pressreleases/2011/01/03/bittorrent-inc-grows-to-over-100-million-active-monthly-users-massive-user- (Stand: 10. Januar 2011).

[63] http://buytaert.net/drupal-7.0-released (Stand: 10. Januar 2011).

[64] http://www.flickr.com/photos/twitteroffice/5330386295/ (Stand: 10. Januar 2011).

[65] Ein berühmter Fall war derjenige von Twitter Ende 2009 (http://www.wired.com/threatlevel/2009/12/twitter-hacked-redirected/ (Stand: 10. Januar 2011). Wenn sich dort statt einer Mitteilung des Defacements eine Kopie der Website von Twitter befunden hätte, hätte ein solcher Angriff zu schwerwiegenden Auswirkungen führen können.

[66] MELANI Halbjahresbericht 2010/1, Kapitel 4.5 http://www.melani.admin.ch/dokumentation/00123/00124/01119/index.html?lang=de (Stand: 10. Januar 2011).

[67] http://www.zdnet.com/blog/feeds/foursquares-privacy-loopholes/2607 (Stand: 10. Januar 2011).

Profil einer Person und ihrer Gewohnheiten anhand von Daten weniger Webseiten zu erstellen. Andererseits ist über die von solchen Unternehmen gesammelten Daten und ihre Verwendung nur wenig bekannt. Die Web-Benutzer sind immer häufiger bereit, ihre eigenen persönlichen Daten auf den grössten Websites zu verbreiten.

Die Entstehung der Giganten im Netz führt somit zu zahlreichen Fragen. Diese betreffen die Daten- und Benutzersicherheit, aber auch die Wandlung des Internet. Sie wird immer mehr von Gruppen bestimmt, die viel Geld verdienen und von denen nichts oder nur wenig bekannt ist.

6 Glossar

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

AdServer	AdServer werden zur Auslieferung und Erfolgsmessung von Internetwerbung eingesetzt. Sowohl der physische Server selbst, auf dem eine AdServer-Software läuft, als auch diese Software können als AdServer bezeichnet werden.
Angriff auf die Verfügbarkeit / (Distributed) Denial-of-Service Attacke. (DoS oder DDoS)	Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Applikationen	Ein Computerprogramm, das eine bestimmte Aufgabe erfüllt. Textverarbeitungsprogramme und Internet Browser sind Beispiele für Applikationen.
Binärdatei	Eine Binärdatei ist eine Datei, die im Unterschied zu einer reinen Textdatei auch nicht-alphabetische Zeichen enthält. Es kann somit jeder beliebige Bytewert vorkommen. Dateien im Binärformat werden eher zur Speicherung von Daten verwendet.
Blog	Ein Blog ist ein auf einer Website geführtes und damit meist öffentlich einsehbares Tagebuch oder Journal, in dem mindestens eine Person, der Web-Logger, kurz Blogger, Aufzeichnungen führt, Sachverhalte protokolliert oder Gedanken niederschreibt.
Bluetooth	Eine Technologie, die eine drahtlose Kommunikation zwischen zwei Endgeräten ermöglicht und vor allem bei Mobiltelefonen, Laptops, PDAs und Eingabegeräten (z.B. Computermaus) zur Anwendung gelangt.
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	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Firefox, Opera, Chrome und Safari.
Computer Emergency Response Team (CERT)	Als CERT (auch CSIRT für Computer Security Incident Response Team) bezeichnet man ein Team, das sich mit der Koordination und Ergreifung von Massnahmen im Zusammenhang mit sicherheitsrelevanten Vorfällen in der IT befasst.
Cloaking	Cloaking (engl. verhüllen) ist eine Technik zur Suchmaschinenoptimierung, bei der dem Webcrawler der Suchmaschinen unter der gleichen URL eine andere Seite präsentiert wird als dem Besucher. Sie dient zur Verbesserung der Rangordnung in Suchmaschinen und der Indexierung.
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.
Computerwurm	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.
Content Management System (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.
Digitale Signatur	Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.
DNS-Amplification-Attack	Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und als Amplifier (Verstärker) benutzt.

Domain Name System (DNS)	Mit Hilfe vom DNS lassen sich das Internet und deren Dienste benutzerfreundlich bedienen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Drei-Wege-Handshake	Der Drei-Wege-Handschlag (Three-Way-Handshake) ist ein Verfahren zum Aufbau verlustfreier Datenübertragungen zwischen zwei Instanzen. Obwohl überwiegend in der Netzwerktechnik verwendet, ist der Drei-Wege-Handschlag nicht darauf beschränkt.
Drive-By Infektionen	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.
General Packet Radio Service (GPRS)-Netz	General Packet Radio Service (deutsch: „Allgemeiner paketorientierter Funkdienst“) ist ein paketorientierter Dienst zur Datenübertragung, welcher in GSM-Netzen (Mobilfunknetzen) verwendet wird.
Hidden Text	Versteckter Text auf Webseiten, der zwar existiert aber für den Menschen nicht lesbar ist. Beispielsweise, wenn die Schriftfarbe transparent ist.
Hypertext	Ein Hypertext ist ein Text, der mit einer netzartigen Struktur von Objekten Informationen durch Hyperlinks zwischen Hypertext-Knoten verknüpft. Hypertext wird in Auszeichnungssprachen geschrieben, die neben Format-Anweisungen auch Befehle für Hyperlinks beinhalten, die bekannteste ist die Hypertext Markup Language (HTML) für Internetdokumente.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Jailbreak	Mit Jailbreaking (englisch: Gefängnisausbruch) wird das Überwinden der Nutzungseinschränkungen auf Apple Produkten mittels geeigneter Software bezeichnet.
Keyword Stuffing	Keyword Stuffing gilt als unethische Suchmaschinen-Optimierungs-Methode. Mit überflüssigen und häufig Wiederholten Schlüsselwörtern (Keywords) in den Meta-Tags oder im Inhalt der Webseite wird versucht, die Suchmaschine zu täuschen.
Linkfarm	Als Linkfarm wird eine Ansammlung von Webseiten oder ganzen Domains im Web bezeichnet, die primär dem Zweck dient, möglichst viele Hyperlinks auf eine andere Webpräsenz zu legen.
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer,

	Trojanische Pferde).
Moneymule / Finanzagent	«Geld-Maultier». Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht.
Netzwerk-Share	Ein Netzwerk-Share oder eine Netzwerkfreigabe ist ein Gerät oder Informationen auf einem Computer auf das oder die via Fernzugriff von einem anderen Computer über ein Netzwerk zugegriffen werden kann.
Nickname	Unter einem Nickname versteht man im heutigen deutschen Sprachgebrauch einen (meist kurzen) Namen, den ein Computernutzer als Pseudonym in Foren und Chats benutzt.
OpenSource	Open Source ist eine Palette von Lizenzen für Software, deren Quelltext öffentlich zugänglich ist und durch die Lizenz Weiterentwicklungen fördert.
Peer to Peer (P2P)	Peer to Peer ist 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.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Pop-up	Ein Pop-up ist ein visuelles Element eines Computerprogramms. Der Name kommt daher, dass diese Elemente „aufspringen“ (engl. „pop up“) und dabei andere Teile überdecken.
Programmable Logic Controller (PLC)	Englisch für Speicherprogrammierbaren Steuerungen (SPS).
Proof of Concept (PoC)	Proof of Concept. Ein kurzer, nicht zwangsläufig kompletter Beweis, dass eine Idee oder Methode funktioniert. Beispielsweise werden häufig Exploit-Codes als PoC veröffentlicht, um die Auswirkungen einer Schwachstelle zu unterstreichen.
Resolver	Resolver sind einfach aufgebaute Software-Module, die auf dem Rechner eines DNS-Teilnehmers installiert sind und die Informationen von Nameservern abrufen können. Sie bilden die Schnittstelle zwischen Anwendung und Nameserver.
Rootkit	Auswahl an Programmen und Technologien, welche den unbemerkten Zugang und die unbemerkte Kontrolle eines Computers ermöglichen.

SCADA	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Scareware	Bei Scareware handelt es sich um Software, welche darauf ausgelegt ist, Computerbenutzer zu verunsichern oder zu verängstigen.
Schutz kritischer Informationsinfrastrukturen (CIIP)	Wichtiger Bestandteil der nationalen Sicherheitspolitik und Verteidigungsplanung. Überbegriff für Konzepte und Strategien zum Schutz kritischer Infrastrukturen / kritischer Informationsinfrastrukturen.
Sicherheitslücken	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Sidejacking	Beim Session Sidejacking wird von einem Angreifer der Netzwerkverkehr zwischen zwei Parteien gelesen, um das Session-Cookie zu stehlen.
Smartphones	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.
Speicherprogrammierbare Steuerung (SPS)	Eine Speicherprogrammierbare Steuerung (SPS), englisch Programmable Logic Controller (PLC), ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird. Seit einigen Jahren löst sie die "festverdrahtete" verbindungsprogrammierte Steuerung in den meisten Bereichen ab.
SSL	Secure Sockets Layer. Ein Protokoll, um im Internet sicher zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen.
Toolbar	Symbolleiste in einem Computerprogramm auf der Schaltflächen, Symbole, Menüs oder andere Elemente platziert werden.
Top Level Domain (TLD)	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
Transmission Control Protocol / Internet Protocol	TCP/IP ist eine Familie von Netzwerkprotokollen und wird wegen ihrer grossen Bedeutung für das Internet auch als

(TCP/IP)	Internetprotokollfamilie bezeichnet.
Trojanisches Pferd	Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen.
Universal Serial Bus (USB)	Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
USB Memory Stick	Kleine Datenspeichergeräte, die über die USB-Schnittstelle an einen Rechner angeschlossen werden.
Viren	Ein selbstreplizierendes, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirtprogramm oder eine Wirtdatei hängt.
Web 2.0	Web 2.0 ist ein Schlagwort, das für eine Reihe interaktiver und kollaborativer Elemente des Internets, speziell des World Wide Webs, verwendet wird. Der Begriff postuliert in Anlehnung an die Versionsnummern von Softwareprodukten eine neue Generation des Webs und grenzt diese von früheren Nutzungsarten ab.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Zwei-Faktor-Authentifizierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z.B. Fingerabdruck, Retina-Scan, Stimmerkennung, usw.)

7 Anhang

7.1 DDoS – Analyse eines immer häufigeren Phänomens

Eine Denial-of-Service (DoS) Attacke hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Von einem Distributed Denial of Service (DDoS) Angriff, also einem „verteilten“ DoS ist dann die Rede, wenn ein Opfer von vielen verschiedenen Systemen koordiniert und gleichzeitig angegriffen wird. Bei den angreifenden Systemen handelt es sich meist um infizierte Computer, welche in einem Botnetz organisiert sind. In Kapitel 5.2 wurde auf die Motivation, welche hinter einem DDoS Angriff steckt, eingegangen. Dieses Kapitel

soll dagegen einen vertieften Einblick geben, welche Technik hinter einer solchen Attacke steckt und welche Mittel hauptsächlich eingesetzt werden, um die Schäden eines solchen Angriffs in Grenzen zu halten.

DoS-Angriffe – Methoden und Funktionsweise

Im Allgemeinen lassen sich zwei Arten von DoS-Angriffen unterscheiden. Die einen zielen darauf ab, ein System durch Überlastung der Rechner- und Speicherressourcen ausser Betrieb zu setzen (protocol-based und application-based). Die anderen versuchen, das Netz durch (Müll-)Abfragen so zu sättigen, dass der legitime Datenverkehr (flood-based) behindert wird. Gemäss Arbor Networks handelte es sich bei 45% der von ihnen festgestellten Angriffe im Jahr 2009 um flood-based und bei 49% um application-based Angriffe.[68]

Bei den application-based oder protocol-based Angriffen werden unter anderem folgende Techniken verwendet:

SYN-Flood-Angriff
Ein SYN-Flood-Angriff nutzt den Ablauf des Aufbaus einer TCP/IP-Verbindung, des sogenannten *Handshakes*. Ein Benutzer sendet zur Herstellung einer solchen Verbindung – beispielsweise, um von einem Server eine Website anzufordern – eine „SYN"-Anfrage an den Server. Dieser antwortet mit einer "SYN-ACK"-Mitteilung, der normalerweise eine Antwort des Benutzers mit "ACK" folgt. Zu diesem Zeitpunkt ist die Verbindung hergestellt[69]. Beide Parteien verwenden somit den so genannten "Three-Way Handshake" (oder "3-Step Handshake"). Wenn nun der Computer eines Benutzers den "Three-Way Handshake" nicht mit einem "ACK" abschliesst, erwartet der Server diese Antwort weiterhin und verwendet somit Speicherressourcen. Eine DoS-Attacke erfolgt, wenn ein Angreifer Tausende von SYNs schickt, ohne den Verbindungsaufbau mit einem ACK abzuschliessen. In der Folge muss der Server seinen Speicher verwenden, um alle Verbindungen aufrecht zu erhalten. Dies erfolgt solange, bis der Speicher gefüllt und nicht mehr in der Lage ist, neue Anfragen – somit auch rechtmässige – anzunehmen.

Prozessflutung
Dass auch mit geringen Netzwerkressourcen ein Webserver lahmgelegt werden kann, zeigt folgende Vorgehensweise, welche beispielsweise auf den Webservern Apache 1.x und Apache 2.x funktioniert. Bei jeder Anfrage einer Webseite wird auf dem Webserver ein Prozess gestartet, der wiederum geschlossen wird, wenn die Anfrage beendet, das heisst die Webseite fertig geladen ist. Wenn nun versucht wird möglichst viele Verbindungen zu öffnen und diese auch möglichst lange offen zu halten, ist irgendeinmal die maximale erlaubte Anzahl paralleler Prozesse erreicht, es werden keine neuen Anfragen mehr zugelassen und die Seite ist nicht mehr erreichbar.[70] Der Angriff ist besonders interessant, da er keine grosse Bandbreite erfordert. Zudem stehen im Netz Programme wie beispielsweise Slowloris zur Verfügung, die diesen Angriff durchführen und auch einfach zu handhaben sind (auch via Proxy oder Tor)[71].

---

[68] "Worldwide Infrastructure Security Report", Arbor Networks 2009, http://www.arbornetworks.com/dmdocuments/ISR2009_EN.pdf (Stand: 10. Januar 2011).

[69] Wir haben das System zur Herstellung einer Verbindung vereinfacht. Eine empfehlenswerte und interessante Lektüre stellt "Computer Network" von Andrw S. Tanenbaum dar.

[70] http://www.securityfocus.com/archive/1/456339/30/0/threaded (Stand: 10. Januar 2011).

[71] http://vimeo.com/7618090 (Stand: 10. Januar 2011).

„Ping of Death" und Smurf Attacke
Eine altbekannte Technik ist der „Ping of Death", bei dem ein deformiertes Ping-Paket[72] versandt wird. Bei einer sogenannten Smurf Attacke sendet ein Angreifer Pings (ICMP-Echo-Requests) an die Broadcast-Adresse eines Netzwerks. Der Absender wird gefälscht und die Adresse des Opfers eingetragen. Je nach der Konfiguration des Routers wird die Anfrage in das Netzwerk geleitet und eine Antwort aller angeschlossenen Computer an das Opfer erzwungen. Router, die dieses Verhalten zulassen werden auch Smurf Amplifier genannt. Je nach Anzahl Computern im betroffenen Netzwerk, kann eine einzige Anfrage um Grössenordnungen verstärkt werden.

Application Attack
Eine andere Angriffsart hat es auf die Funktionen auf Webservern abgesehen, welche grosse Ressourcen benötigen. Dies gilt beispielsweise für die Suchfunktion innerhalb eines Webauftritts oder den Betrieb eines Content Management System (CMS) (wie WordPress oder Drupal), welche die Seite zum Zeitpunkt der Anfrage kreieren (im Gegensatz zu den statischen Seiten, die auf dem Server zur Verfügung stehen). Ein Angriff auf solche Seiten ist natürlich um ein Vielfaches effizienter.

Bei flood-based Angriffen erfolgen die Zugriffe von verschiedenen Computern aus. (Es handelt sich dabei meist um infizierte Computer, die einem Botnetz angehören. Andere werden in vollem Bewusstsein eigens dafür eingesetzt, einen Angriff durchzuführen.) Dabei wird mit Anfragen die gesamte Upstream-Bandbreite des Servers ausgenutzt, damit dieser die Seite nicht mehr senden oder den angeforderten Dienst nicht mehr liefern kann. Wie effizient eine solche Art von Angriff ist, hängt von der entsprechenden Bandbreite des Servers ab. Allgemein gilt die Vorstellung, dass ein grosses Botnetz zu grösseren Angriffen in der Lage ist. Es gibt jedoch verschiedene Techniken, die einen solchen Angriff verstärken, damit auch für grosse Angriffe kleinere oder mittlere Botnetze eingesetzt werden können.

DNS-basierte Angriffe
Eine DNS-Anfrage kann nach drei verschiedenen Verfahren beantwortet werden:

- autoritativ: der Server holt die Datei aus der lokalen Zonendatei
- rekursiv: der Server holt die Daten von einem anderen Nameserver
- iterativ: der Server antwortet mit einem Verweis auf andere Nameserver

Bei rekursiven Anfragen schickt der *Resolver* also eine rekursive Anfrage an den ihm zugeordneten Nameserver. Hat ein Nameserver die gewünschte Information auch nicht im eigenen Datenbestand, so kontaktiert dieser weitere Server bis er eine positive Antwort oder von einem autoritativen System eine negative Antwort bekommt. Ein Nameserver sollte nun eigentlich nur Anfragen akzeptieren, die von lokalen oder befugten Kunden stammen. In Tat und Wahrheit nehmen aber viele DNS-Server Anfragen von irgendeiner Quelle entgegen. In solchen Fällen werden diese als Open Resolver[73] bezeichnet. Bei einem Angriff können nun Anfragen an solche Open Resolver gesendet werden, bei denen die Adresse des Opfers als Antwortadresse angegeben ist. In der Folge wird das Opfer mit DNS-Antworten überhäuft, die es nicht beantragt hat. Dies hat ebenfalls zur Folge, dass nur die IP-Adresse des Nameservers sichtbar ist, nicht aber diejenige des Angreifers. Diese Anonymisierung des Angriffs erschwert eine wirkungsvolle Abwehr. Eine Technik, diesen Angriff zu verstärken, ist die *DNS-amplification.* Nameserver regieren in bestimmten Fällen auf kurze Anfragepakete mit sehr langen Paketen. Eine 60 Bytes lange Anfrage kann eine mehr als 4000 Bytes lange

[72] http://insecure.org/sploits/ping-o-death.html (Stand: 10. Januar 2011).

[73] Eine mit Sicherheit interessante Lektüre stellt der Text von Randal Vaughn und Gadi Evron "DNS Aplification Attacks" dar, http://www.isotf.org/news/DNS-Amplification-Attacks.pdf (Stand: 10. Januar 2011).

Antwort provozieren. Der Verstärkungsfaktor liegt in diesem Fall also bei mehr als 65. Hinzu kommt ein höherer Rechenaufwand aufgrund der IP-Fragmentierung. Durch die DNS-Erweiterung EDNS ist diese Angriffsart erst praktikabel geworden, da vorher die maximale Länge eines DNS-Pakets auf 512 Bytes beschränkt war (was einem Verstärkungsfaktor von unter 10 entspricht). Eine inzwischen etwas veraltete Untersuchung (2005)[74] ergab, dass 75% der externen DNS unbefugte Anfragen und infolgedessen Poisoning-Angriffe[75] oder DoS ermöglichten.

Ein Ausweitungseffekt lässt sich auch dank der Benutzung von P2P-Netzen erzielen. In solchen Fällen wird der Server des Opfers als einzige Quelle für ein bekanntes File (Film, Album oder anderes) angegeben, so dass die Benutzer des P2P-Netzes das gewünschte File bei jener IP-Adresse beantragen. Mit dieser Thematik beschäftigten sich verschiedene Forscher[76].

Es wird auch beobachtet, dass Angriffe, die mittels Botnetz durchgeführt werden, zunehmend effizienter werden. Angreifer benutzen beispielsweise nicht alle Computer im Botnetz gleichzeitig. Ein grösserer und länger anhaltender Effekt ergibt sich, wenn auf zufällige Weise Maschinen mit einem mässigen Verkehr eingesetzt werden, die den verschiedenen Untergruppen des Botnetzes angehören (von verschiedenen Providern und verschiedenen geografischen Regionen ausgehend). Dies verzögert den Prozess zur Filtrierung der IP-Adressen seitens des Opfers.

DoS-Angriffe – Gegenmassnahmen

Vor kurzem veröffentlichte das CERT der niederländischen Regierung ein Dokument, welches eine Reihe nützlicher Massnahmen auflistet, um sich gegen DoS-Angriffe zu schützen[77]. Der erste Punkt betrifft keinen technischen, sondern den organisatorischen Aspekt der *Unternehmenskommunikation*:
Was ein Unternehmen kommuniziert und wie es dies tut, ist unbestritten ein entscheidender Faktor. Eine Kommunikationsstrategie kann als erste Massnahme gegen DoS-Angriffe fungieren oder aber auch der Auslöser einer DoS-Attacke sein. Dies zeigt das Beispiel PostFinance von Dezember 2010 deutlich: Die Kommunikation, das Konto von Julian Assange zu sperren, führte zu einer Reaktion seitens der Bewegung Anonymous und hatte einen DDoS-Angriff zur Folge. Die Risiken und Auswirkungen einer Kommunikation in der breiten Öffentlichkeit muss deshalb im Vorfeld abgeschätzt werden.

Technische Massnahmen können am Netzwerkeingang oder direkt beim Provider getroffen werden:
Den Verkehr genau analysieren.
Dies ist eine erste Massnahme, um zu verstehen, welcher Verkehr zu den Servern gelangt. Infolgedessen lässt sich auch eruieren, was herauszufiltern ist. Zu den am häufigsten

---

[74] http://dns.measurement-factory.com/surveys/sum1.html (Stand: 10. Januar 2011).

[75] Siehe Kapitel 7.3 des Berichts von MELANI 2008/2: http://www.melani.admin.ch/dokumentation/00123/00124/01085/index.html?lang=it (Stand: 10. Januar 2011).

[76] http://www.pank4j.com/research/p2pddos.pdf (Stand: 10. Januar 2011) und http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5254891%2F5273826%2F05273837.pdf%3Farnumber%3D5273837&authDecision=-203 (Stand: 10. Januar 2011).

[77] http://www.govcert.nl/english/service-provision/knowledge-and-publications/factsheets/protect-your-online-services-against-ddos-attacks.html (Stand: 10. Januar 2011).

verwendeten Applikationen, die Netflow-Daten analysieren, gehören unter anderen die Open-Source-Tools wie NFSen[78] und NFDump[79].

Paketfiltrierung und Anfragegrenzen:
Die schadhaften Pakete eruieren[80] und herausfiltern, damit der Server nur auf berechtigte Anfragen reagiert. Die Anfragenzahl pro IP zeitlich beschränken und somit verhindern, dass jeder Bot pro Sekunde Hunderte von Anfragen erzeugen kann.

Scrubbing
Implementation eines komplexen und verteilten Serversystems, das auch Verkehrsspitzen verarbeiten kann. Alternativ können auch CDN-Dienste (Content Delivery Network) wie Akamai verwendet werden[81].

Load Balancing und Cache verwenden.
Verwendung verschiedener Server, die an mehreren Netzen (mehrere Provider) angeschlossen sind und sich den eingehenden Verkehr teilen. Zusätzlich kann die Cache-Funktion von Reverse-Proxy-Servern wie beispielsweise nginx[82] oder squid[83] verwendet werden.

Dynamic Rerouting verwenden.
Mit dieser Methode wird den angreifenden Computern mitgeteilt, dass keine gültige Route existiert, um die Maschine des Opfers zu kontaktieren (Null-Route oder Blackhole-Route).

Nur vom Protokoll bewilligten Verkehr erlauben.
Wenn es sich bei den erlaubten Anfragen an einen Webserver um TCP:80 und TCP:443 handelt, kann UDP:80 blockiert werden, da dieses Protokoll vom HTTP-Protokoll nicht verwendet wird.

Den Provider fragen,
ob er Lösungen wie beispielsweise IDMS[84] oder RTBH (Remotely Triggered Black Hole[85]) zur Verfügung stellt, um die DoS-Angriffe abzuwehren.

---

78 http://nfsen.sourceforge.net/ (Stand: 10. Januar 2011).

79 http://nfdump.sourceforge.net (Stand: 10. Januar 2011).

80 Beim Angriff von Anonymous gegen verschiedene Ziele wurde das Tool LOIC (Low Orbit Ion Cannon) verwendet. Dieses sandte die Mitteilung “wikileaks.org” als Payload der TCP- und UDP-Pakete. Somit war es möglich, Filtrierungsregeln aufzustellen.

81 http://www.akamai.com (Stand: 10. Januar 2011).

82 http://nginx.net/ (Stand: 10. Januar 2011).

83 http://www.squid-cache.org/ (Stand: 10. Januar 2011).

84 http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigation-systems/download.html (Stand: 10. Januar 2011).

85 http://www.google.ch/url?sa=t&source=web&cd=1&sqi=2&ved=0CBcQFjAA&url=http%3A%2F%2Fwww.cisco.com%2Fen%2FUS%2Fprod%2Fcollateral%2Fiosswrel%2Fps6537%2Fps6586%2Fps6642%2Fprod_white_paper0900aecd80313fac.pdf&rct=j&q=remotely%20triggered%20black%20hole&ei=1iMwTZPZO4ztsgbq8P2lCg&usg=AFQjCNEZ-kPQ3RiLBBecuEFuKAQ2fQO4OQ&cad=rja (Stand: 10. Januar 2011).