Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

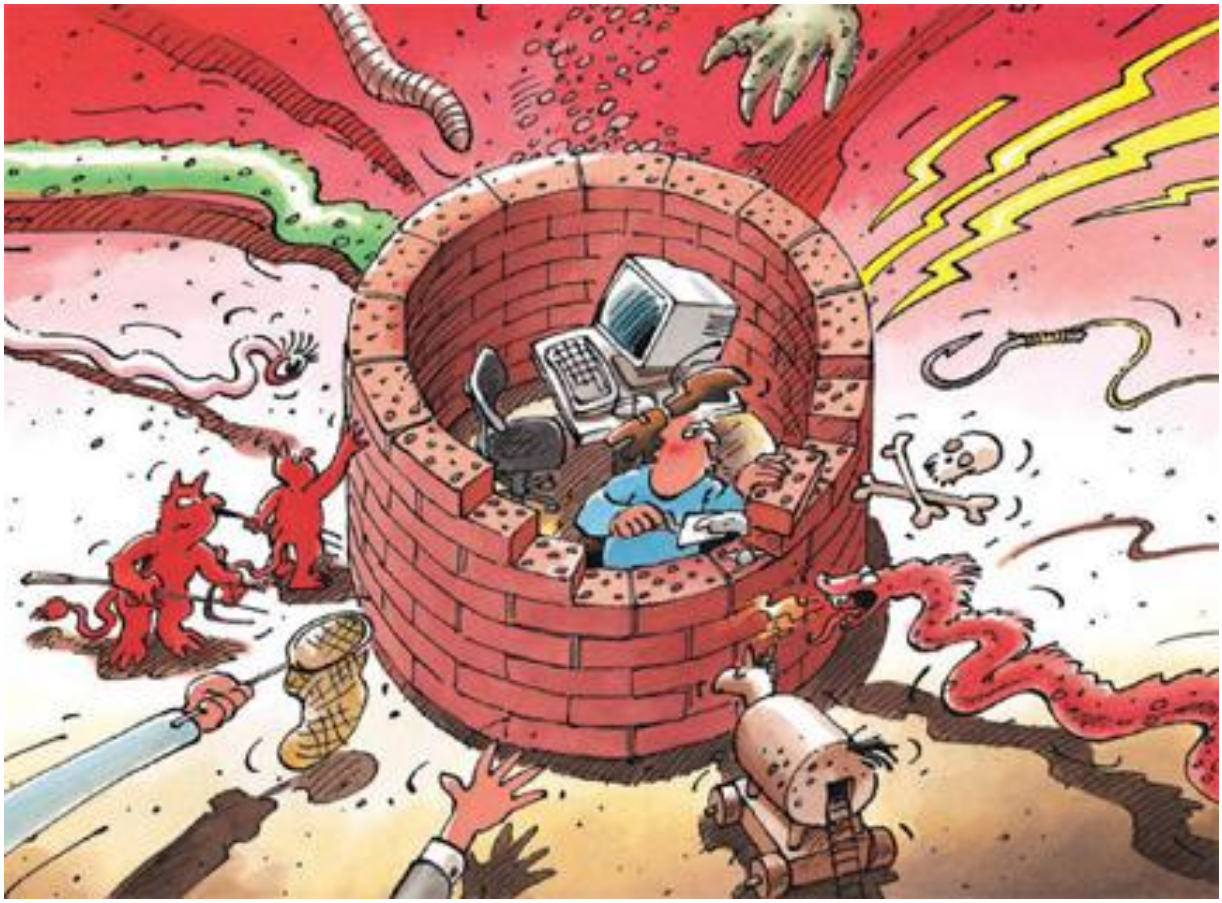
Informatikstrategieorgan Bund ISB
Bundesamt für Polizei fedpol

Melde- und Analysestelle Informationssicherung MELANI

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2007/I (Januar – Juni)



In Zusammenarbeit mit:

KOBIK SCOCI CYCO

Koordinationsstelle zur Bekämpfung der Internet-Kriminalität

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

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

The Swiss Coordination Unit for Cybercrime Control

Inhaltsverzeichnis

Schwerpunkte Ausgabe 2007/I

- **Angriffe auf Schweizer Finanzdienste**
  „Klassische“ *Phishing*-Angriffe per E-Mail mit der Aufforderung Passwörter einzugeben, haben in der Schweiz stark abgenommen. Zudem waren alle erfolglos. Dafür haben erfolgreiche Angriffe mit *Malware* zugenommen. *Zwei-Faktor-Authentisierungssysteme* (z.B. Streichlisten, SecurID, usw) bieten keinen Schutz gegen solche Angriffe und müssen als unsicher betrachtet werden, sobald der PC des Kunden mit Malware verseucht worden ist.
  ► Aktuelle Lage: Kapitel 2.1 (siehe auch 2.4)
  ► Tendenzen für das nächste Halbjahr: Kapitel 3.1
  ► Beispiele / Vorfälle Schweiz: Kapitel 4.2; international: Kapitel 5.2

- **Industriespionage und Datendiebstähle**
  Die Bedrohung durch gezielte staatliche oder private Industriespionage bleibt bestehen. Gefährdet sind nicht nur Betreiber *kritischer Infrastrukturen*, die Rüstungsindustrie oder staatliche Stellen. Auch mittelständische Industrieunternehmen sowie Luxusartikel- und Modehersteller sind im Visier. Die Angriffe erfolgen mit gezielt an einzelne Mitarbeitende verschickten E-Mails, die *Malware* im Anhang oder Links zu präparierten Webseiten enthalten.
  ► Akutelle Lage: Kapitel 2.3
  ► Beispiele / Vorfälle Schweiz: Kapitel 4.1; international: Kapitel 5.2

- **Angriffe auf Webserver: Malware-Verteilung, Phishing, Datendiebstahl**
  Kompromittierungen von Webservern haben zugenommen. Zweck ist die Nutzung der Webserver zur *Malware*-Verteilung wie z.B. per *Drive-by-Infektion*, zum Diebstahl von Daten (vor allem auf kommerziell genutzten Servern), zur (Zwischen-)Speicherung von Daten (z.B. im Zusammenhang mit *Phishing*) oder zur Verbreitung meist politischer Botschaften.
  ► Aktuelle Lage: Kapitel 2.2 (siehe auch 2.4)
  ► Beispiele / Vorfälle Schweiz: Kapitel 4.1; international: Kapitel 5.1 und 5.2
  ► Prävention: Kapitel 6 (zum Thema Drive-by-Infektionen)

- **Malware / Angriffsvektoren**
  Malware wird noch immer meistens durch Anhänge in E-Mails oder E-Mails mit Links auf präparierte Webseiten verteilt. Mit geschickten *Social-Engineering*-Techniken wird das Opfer dazu verleitet, den Anhang zu öffnen oder den Link anzuklicken.
  Als Infektionsweg stark zugenommen haben Webseiten, bei deren Besuch Malware ohne Dazutun des Benutzers auf dem Rechner installiert wird (*Drive-by-Infektion*). Dabei werden *Sicherheitslücken* im Betriebssystem, im Browser oder in einer anderen Applikation ausgenützt. Längst geschieht dies nicht mehr nur auf dubiosen, sondern auch auf (kompromittierten) seriösen und bekannten Seiten.
  Die Erkennungsrate der Malware durch Antiviren-Software bleibt tief.
  ► Aktuelle Lage: Kapitel 2.4 (siehe auch 2.2)
  ► Beispiele / Vorfälle Schweiz: Kapitel 4.2; international Kapitel 5.1 und 5.2.
  ► Prävention: Kapitel 6 (Drive-by-Infektionen)

1 Einleitung

Der fünfte Halbjahresbericht (Januar – Juni 2007) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet einen Schwerpunkt im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

Kapitel 2 beschreibt die aktuelle Lage sowie Gefahren und Risiken des letzten Halbjahres. Ein Ausblick auf zu erwartende Entwicklungen wird in **Kapitel 3** gegeben.

Kapitel 4 und 5 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der ersten sechs Monate des Jahres 2007 aufgezeigt. Der Leser findet hier konkrete Beispiele und ergänzende Informationen zu den allgemeinen Kapiteln zwei und drei.

Kapitel 6 befasst sich jeweils mit einem aktuellen Thema aus dem Bereich der Prävention, das in engem Zusammenhang mit den in Kapitel 2 erwähnten Gefahren steht.

Kapitel 7 legt den Schwerpunkt auf staatliche und privatwirtschaftliche Aktivitäten zum Thema Informationssicherung im In- und Ausland.

Kapitel 8 fasst Änderungen in den gesetzlichen Grundlagen zusammen.

Kapitel 9 fasst wichtige Studien und Statistiken zu IKT-Themen zusammen.

2 Aktuelle Lage, Gefahren und Risiken

2.1 Angriffe gegen Schweizer Finanzdienste

„Klassische“ *Phishing*-Angriffe – E-Mails mit gefälschtem Absender und Link, der auf eine Phishing-Seite im Internet führt, um dort Streichlistennummern für E-Banking-Portale abzufragen – haben in der Schweiz im ersten Halbjahr stark abgenommen. Die wenigen beobachteten Angriffe waren zudem erfolglos. Kriminelle Gruppen gehen nun neue Wege, um E-Banking-Systeme anzugreifen, wie bereits im letzten Halbjahresbericht (Kapitel 3.1) vorausgesagt worden ist. Dabei werden Kundenrechner mit *Malware* infiziert, welche *Man-in-the-Middle*-Angriffe ermöglicht. Solche Angriffe haben auch gegen Schweizer E-Banking-Portale erfolgreich stattgefunden.

Verteilt per E-Mails mit infiziertem Anhang oder Links zu präparierten Webseiten, gelangt die Malware unter Ausnützung von *Sicherheitslücken* im Betriebssystem oder in einer Applikation unbemerkt auf den Kundenrechner. In der Schweiz erfolgte die Verteilung durch E-Mails, welche mit gefälschtem Absender (Ricardo.ch und eine Berner Anwaltskanzlei) versendet wurden (siehe Kapitel 4.2). Denkbar ist aber auch eine Infektion durch den alleinigen Besuch einer präparierten Webseite (siehe Kapitel 2.2, 2.4 und 5.1), ohne dass zuvor ein Link in einer E-Mail angeklickt worden ist. Die Malware wird aktiv, sobald eine E-Banking-Seite aufgerufen wird. Entweder leitet die Malware den Kunden auf eine gefälschte Bankenseite um oder manipuliert die im Browser angezeigten Daten.

Im ersten Fall wird auf der gefälschten Seite die echte Bankenseite „nachgebildet“, welche nach Benutzernamen und Passwort fragt. Nachdem der Kunde diese eingegeben hat, fragen Bankenseiten nach einem zweiten Authentisierungsmerkmal (z.B. eine Streichlistennummer oder ein von einem *Token* generierter Code). Auch diese Angaben werden über die gefälschte Seite in Erfahrung gebracht. Danach trennt die gefälschte Seite die Verbindung zum Kunden und zeigt eine Störungsmeldung an. Gleichzeitig nutzt der Angreifer die so erhaltenen Zugangsdaten, um sich (in Echtzeit) bei der richtigen Bankenseite anzumelden und illegale Finanztransaktionen abzuwickeln.

Im zweiten Fall nistet sich die Malware im Browser ein. Bevor die Transaktionseingaben des Benutzers verschlüsselt über das Internet an die Bank gelangen, verändert der Angreifer Kontonummer, Empfängername und Betrag. Die Bestätigung der Bank wird ebenfalls durch die Malware abgefangen und im Browser falsch angezeigt. Das Opfer glaubt, die gewollte Überweisung getätigt zu haben, während in Wahrheit die Zahlung an einen anderen Empfänger erfolgt und allenfalls in ihrer Höhe verändert worden ist.

Malware dieser Art kann ausserdem jederzeit auf bereits infizierte Rechner – z.B. solche in einem *Botnetz* – nachgeladen werden. So können infizierte Systeme, die ursprünglich von den Angreifern für andere Einsätze vorgesehen waren, plötzlich auch für Angriffe gegen E-Banking genutzt werden.

Ohne dass E-Banking-Kunden auf eine Phishing-Mail reagiert und dadurch Streichlistennummern oder Passwörter auf einer Phishing-Seite eingegeben haben, ist es mit Malware heute möglich, erfolgreiche Angriffe gegen die Kunden durchzuführen. Sobald der PC des Kunden mit Malware kompromittiert worden ist, müssen *Zwei-Faktor-Authentifikationssysteme*, wie sie heute von Schweizer und ausländischen Banken

eingesetzt werden (wie z.B. Streichlisten, indizierten Streichlisten, Token mit wechselnden oder kryptographisch errechneten Codes, usw.), als unsicher betrachtet werden.[1]

Computerbenutzer sollten daher Verhaltensregeln im Umgang mit E-Mails sowie beim Surfen im Internet befolgen, ihr Betriebssystem und die Applikationen auf dem aktuellen Stand halten sowie aktuelle Antiviren- und Firewall-Software einsetzen (siehe dazu die Empfehlungen auf der MELANI-Homepage).[2] Unregelmässigkeiten beim E-Banking, wie beispielsweise das unerwartete Abbrechen einer E-Banking-Sitzung, sollten dem entsprechenden Institut umgehend gemeldet werden.

Eine Einschätzung der weiteren Entwicklung wird in Kapitel 3.1 vorgenommen; die Lage in der Schweiz ist in Kapitel 4.2, die internationale Situation in Kapitel 5.2 erläutert. Die ergaunerten Gelder werden häufig durch so genannte „Money Mules“ ins Ausland transferiert – siehe dazu Kapitel 4.3.

2.2 Angriffe auf Webserver zwecks Malware-Verteilung, Phishing oder Datendiebstahls

Im ersten Halbjahr 2007 haben Webserver-Kompromittierungen zugenommen.[3] Google fand beispielsweise unter etwa 4,5 Millionen URLs ungefähr 450'000, welche *Malware* zu verteilen versuchten; Sophos berichtete allein im Juni von fast 30'000 neu infizierten Webseiten pro Tag, wobei die meisten davon nicht dubioser Natur, sondern Seiten mit durchaus seriösem Inhalt seien.[4] So wurde beispielsweise über die folgenden kompromittierten Homepages Malware verteilt: Diejenige der Miami Dolphins (die Gewinner des US-Superbowls), des koreanischen Hardware-Herstellers Asus, der US-Disease-Control oder des Opernhauses und des Museums für zeitgenössische Kunst in Sidney.[5]

Die Kompromittierungen finden häufig über nicht geschlossene *Sicherheitslücken* in Web-Applikationen statt; ebenfalls verbreitet sind Angriffe gegen Datenbanken, welche über den Webserver angesteuert werden können. Im Falle eines Angriffs in Italien wurden mehrere tausend auf einem Server liegende Webseiten kompromittiert. Dies gelang unter Ausnutzung

---

[1] Siehe dazu: http://www.schneier.com/blog/archives/2005/03/the_failure_of.html; http://www.schneier.com/essay-083.html; http://www.zdnetasia.com/news/security/0,39044215,62010658,00.htm; http://www.darkreading.com/document.asp?doc_id=116456; http://www.itseccity.de/?url=/content/virenwarnung/aktuellemeldungen/070329_vir_akt_trendmicro.html (Stand: 18.07.2007).

[2] Siehe: http://www.melani.admin.ch/themen/00166/index.html?lang=de (Stand: 26.07.2007).

[3] Siehe z.B.: http://blogs.iss.net/archive/WebBrowserExploitati.html; http://blog.washingtonpost.com/securityfix/2007/05/cyber_crooks_hijack_activities_1.html; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9017261; http://googleonlinesecurity.blogspot.com/ (Stand: 26.07.2007).

[4] Siehe dazu: http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf, http://www.sophos.com/sophos/docs/eng/marketing_material/sophos-security-threats-update-2007_wsrus.pdf; http://www.heise.de/newsticker/meldung/93334; http://www.darkreading.com/document.asp?doc_id=120373, http://www.siteadvisor.com/studies/map_malweb_mar2007.html sowie den neusten Bericht der Anti-Phishing Working Group: http://www.antiphishing.org/reports/apwg_report_may_2007.pdf (Stand: 17.07.2007).

[5] Siehe: http://www.smh.com.au/news/security/virus-blight-spreads-to-museum-site/2007/06/13/1181414340831.html; http://www.heise.de/newsticker/meldung/84761; http://www.theregister.co.uk/2007/02/08/cdc_malware/; http://www.heise.de/newsticker/meldung/87965 (Stand: 26.07.2007).

einer Sicherheitslücke auf einer einzigen Seite in Kombination mit einem Konfigurationsfehler durch den Hosting-Provider (siehe Kapitel 5.1 zu MPack).[6]

Angriffe gegen Webserver dienen mehreren Zwecken: Erstens kann der Webserver zur Malware-Verteilung benutzt werden, so dass er die Computer der Besucher zu infizieren versucht. Zweitens ermöglicht die Kontrolle über einen für den E-Commerce genutzten Webserver häufig, dass wertvolle Daten gestohlen werden (wie z.B. Kreditkartendaten). Drittens kann ein kompromittierter Webserver für das Hosting illegaler Daten verwendet werden, sei dies nun für eine *Phishing*-Seite, als Speicherort für raubkopierte Software oder für illegal beschaffte Daten. Oft werden auf kompromittierten Webseiten auch Änderungen angebracht, um politische Botschaften zu verbreiten (*Defacement*).

Betreibern von Web-Seiten wird empfohlen, die Web-Applikationen aktuell zu halten und sicherzustellen, dass auch der Hosting-Provider die nötigen Aktualisierungen und Sicherheitsvorkehrungen vornimmt.[7]

Infektionen über Webseiten werden in Kapitel 2.4 nochmals aufgegriffen, Beispiele sind in den Kapiteln 4.1 und 5.1 zu finden, während sich Kapitel 6 mit entsprechenden präventiven Massnahmen zum Thema befasst.

2.3 Spionage mit gezielter Malware

Die Bedrohung durch gezielte, teilweise wohl staatlich verübte Industriespionage war bereits Schwerpunkt im Halbjahresbericht 2005/II und wurde in sämtlichen Berichten seither thematisiert (siehe auch im Halbjahresbericht 2006/II Kapitel 2.3 und 5.2). Sie ist auch heute noch aktuell.

In den USA haben Spionageangriffe gegen Regierungssysteme, insbesondere gegen Netzwerke des Aussen- sowie des Verteidigungsministeriums, zugenommen.[8] Auch für die Privatwirtschaft wird das Problem immer aktueller. MELANI hat in der Vergangenheit mehrmals vor gezielten Angriffen gegen die Schweizer Privatwirtschaft gewarnt. Das Thema wird auch in anderen Ländern zunehmend öffentlich diskutiert. Wie das Magazin Der Spiegel schätzt, entstehen dadurch alleine in Deutschland Schäden in Milliardenhöhe.[9]

In der Industriespionage wird meistens ähnlich vorgegangen: Zuerst wird über Mitarbeitende und das Umfeld des Unternehmens recherchiert (z.B. über Social-Networking-Seiten wie Xing, Linked-In etc., offizielle Firmenseiten, private Mitarbeiter-Homepages, Jahres- oder Presseberichte, usw.). Dann erfolgt ein gezielter Versand von E-Mails an nur wenige Mitarbeitende. Meistens handelt es sich dabei um Angestellte in Kaderpositionen mit Zugang

---

[6] Häufig sind die gleichen Hosting-Provider betroffen, siehe: http://blogs.stopbadware.org/articles/2007/05/04/stopbadware-identifies-hosting-providers-of-larged-numbers-of-sites-in-badware-website-clearinghouse (Stand: 26.07.2007).

[7] Empfehlungen zur sicheren Konfiguration von Webservern sind beispielsweise zu finden unter: http://www.cpni.gov.uk/docs/re-20030801-00726.pdf; http://www.cpni.gov.uk/ProtectingYourAssets/applications.aspx sowie http://www.stopbadware.org/home/security (Stand: 19.07.2007).

[8] Siehe z.B.: http://www.fcw.com/article97658-02-13-07-Web&printLayout; http://seclists.org/isn/2007/Jan/0023.html; http://www.heise.de/newsticker/meldung/91571/ (Stand: 30.07.2007).

[9] Siehe: http://www.manager-magazin.de/unternehmen/mittelstand/0,2828,464284,00.html; http://www.ftd.de/unternehmen/industrie/159669.html; http://www.spiegel.de/wirtschaft/0,1518,465041,00.html; http://www.vnunet.com/vnunet/news/2184744/intellectual-property-theft (Stand: 30.07.2007).

zu vertraulichen Daten.[10] Die E-Mails enthalten gefälschte Absender, sind sprachlich und inhaltlich auf die Aufgaben des Opfers abgestimmt und beinhalten *Malware* im Anhang oder einen Link zu einer Malware-verteilenden Webseite (siehe Kapitel 2.2, 2.4 und 5.1). Häufig werden dafür Dokumente der Microsoft-Office-Familie (Word, Excel, Powerpoint) sowie PDF-Dateien verwendet.[11] Teilweise erfolgten die Angriffe auch mit so genannten *0-day-Exploits,* welche bisher unbekannte *Sicherheitslücken* ausnutzen.[12]

Im staatlichen Bereich und gegen die Betreiber *kritischer Infrastrukturen* werden vor allem vertrauliche Daten mit Bedeutung für die Rüstungsindustrie ausspioniert oder solche, die für terroristische oder militärische Aktivitäten von Nutzen wären (siehe für ein Schweizer Beispiel Kapitel 4.1).

Immer mehr Unternehmen, insbesondere aus dem Mittelstand und dem Industriesektor (v.a. Maschinen- und Anlagenbau), sehen sich mit – in erster Linie chinesischer – Industriespionage konfrontiert. Ebenfalls im Visier sind Hersteller von Luxusartikeln und Mode.[13] Firmen aus der Privatwirtschaft sind vor allem dann gefährdet, wenn sie einen Know-how-Vorsprung gegenüber der Konkurrenz aufweisen oder aber geschäftliche Kontakte in Regionen unterhalten, die wirtschaftlich rückständig sind und/oder über unklare Gesetze zu geistigem Eigentum verfügen.

Bei den Angreifern kann es sich um organisierte oder kleinere Cyberkriminelle handeln (die in Geld ummünzbare Informationen suchen), um die Konkurrenz (welche Know-how und Wissensvorteile beschaffen oder sabotieren will), um staatlich gesponserte Akteure (die v.a. militärische und volkswirtschaftlich bedeutsame Daten beschaffen) oder aber um Terroristen (welche z.B. für Attentate Informationen über Infrastrukturen sammeln).

Da die Angriffe gezielt erfolgen und dafür speziell für diese Zwecke programmierte Malware eingesetzt wird, werden solche Angriffe durch Antiviren- und Antispyware-Software meistens nicht erkannt. Weiter ist davon auszugehen, dass die Verteilung von Malware über kompromittierte, seriöse Internetseiten zunehmen wird. Die Angreifer suchen sich diejenigen Webseiten aus, welche für die anzugreifenden Ziele relevant sind (siehe dazu auch Kapitel 2.2, 2.4 und 5.1).

---

[10] Siehe dazu auch die Berichte von MessageLabs zu gezielten Angriffen: http://www.messagelabs.com/mlireport/messagelabs_intelligence_special_report__targeted_attacks_april_2007_5.pdf und http://www.messagelabs.com/mlireport/MessageLabs%20Intelligence%20-%20Jun%20Q2%20Report%20-%20FINAL.pdf (Stand: 30.07.2007).

[11] Siehe vorige Fussnote sowie: http://www.usatoday.com/tech/news/computersecurity/2007-04-22-cyberspies-microsoft-office_N.htm; http://www.heise.de/security/news/meldung/84311; http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=software&articleId=9018519&taxonomyId=18&intsrc=kc_top (Stand: 30.07.2007).

[12] Siehe dazu z.B.: http://www.theregister.co.uk/2007/04/19/us_state_dept_rooted/. Eine technische Beschreibung eines durchschnittlichen Angriffs ist zu finden unter: https://isc.sans.org/diary.html?storyid=2894; Tipps zur Abwehr sind ebenfalls beim ISC SANS erhältlich: http://isc.sans.org/diary.html?storyid=2967 (Stand: 30.07.2007).

[13] Siehe z.B. folgenden Artikel der Washington Times (Archiv-Link): http://nl.newsbank.com/nl-search/we/Archives?p_product=WT&p_theme=wt&p_action=search&p_maxdocs=200&p_text_search-0=chinese%20AND%20hackers%20AND%20get%20AND%20the%20AND%20drop%20AND%20on%20AND%20fashion%20AND%20houses&s_dispstring=chinese%20hackers%20get%20the%20drop%20on%20fashion%20houses%20AND%20date(last%20180%20days)&p_field_date-0=YMD_date&p_params_date-0=date:B,E&p_text_date-0=-180qzD&p_perpage=10&p_sort=YMD_date:D&xcal_useweights=no (Stand: 30.07.2007).

2.4 Malware / Angriffsvektoren

Abgesehen von einer Zunahme der Infektionen über Webseiten, hat sich im Vergleich zum letzten Halbjahr nicht viel geändert. Am häufigsten gelangt *Malware* noch immer durch E-Mail-Anhänge oder E-Mails mit Links auf infizierende Webseiten auf den Computer. Die Absenderadressen sind gefälscht und die Mails weisen, um ihre Glaubwürdigkeit zu erhöhen, häufiger einen regionalen Bezug auf als früher. In der Schweiz sind die Mails von Ricardo.ch und diejenigen von einem Berner Anwalt die wichtigsten Beispiele (siehe Kapitel 4.2).

Zugenommen als Infektionsweg haben Webseiten, bei deren Besuch Malware ohne Dazutun des Benutzers auf den Rechner geladen wird. Diese Art der Infektion wird als "*Drive-by-Infektion*" bezeichnet. Offenbar sind auch Webseiten gefunden worden, die ihre Malware pro Opfer nur einmal verteilen – beim zweiten Besuch ist der Seite keine Auffälligkeit mehr anzumerken.[14] Sind bisher vor allem dubiose Webseiten für die Verteilung von Schadsoftware genutzt worden, kann man sich zunehmend auch auf Seiten mit seriösem Inhalt Malware einfangen. Diese Webseiten verteilen die Malware nicht bewusst – vielmehr werden Schwachstellen oder Konfigurationsfehler in den Webapplikationen ausgenutzt, um entweder den Schadcode direkt auf der Webseite zu platzieren oder den Besucher zu Webseiten mit eingebetteter Malware umzuleiten (siehe Kapitel 2.2). Die Infektion des Clients erfolgt über *Sicherheitslücken* im Webbrowser oder anderen Applikationen, wie beispielsweise Antiviren-Software oder *Plugins* (Adobe Reader, Flash, QuickTime u.a.). Vor allem das Tool MPack hat in diesem Bereich für Schlagzeilen gesorgt (siehe Kapitel 5.1). MPack ist eines von verschiedenen Malware-Kits, die in der Szene verkauft werden und es auch unversierten Personen erlauben, Systeme zu kompromittieren (siehe Kapitel 5.2).

Unglücklicherweise haben sich die Erkennungsraten der Antivirensoftware nicht merklich verbessert. Bei einigen der Malware-Varianten hat es über eine Woche gedauert, bis diese vom Grossteil der Antiviren-Lösungen erkannt worden ist.

Angreifer entwickeln laufend neue Versionen der gleichen Malware. Über kompromittierte Webseiten wird entweder pro Besucher eine neue Version abgegeben oder die Versionen ändern in kurzen Zeitabständen. Zudem wird die Malware auf dem infizierten Rechner zunehmend besser getarnt. Dieses Vorgehen hat zum Ziel, dass die Malware durch Sicherheitssoftware nicht entdeckt wird und die Spezialisten die Malware nur schwer erkennen und analysieren können. Die Erkennungsrate aktueller Malware durch Antivirensoftware liegt daher auf tiefem Niveau.

Beispiele sind in den Kapiteln 4.2, 5.1 und 5.2 zu finden.

[14] Siehe dazu: http://www.finjan.com/GetObject.aspx?ObjId=443 (Stand: 26.07.2007).

3 Tendenzen / Allgemeine Entwicklungen

3.1 Cyberkriminalität und Attacken gegen Schweizer Finanzdienste

Wie im letzten Halbjahresbericht erwähnt (Kapitel 3.2), hat sich der Untergrundmarkt für cyberkriminelle Dienstleistungen etabliert, der sich inzwischen in der Konsolidierungsphase befindet. Dies gilt insbesondere im Bereich des *Phishing* und Finanzdiebstahls mit *Malware.* Auch wenn sich genaue Zahlen nur sehr schwer bestimmen lassen, gibt es Schätzungen, dass mit Cyberkriminalität inzwischen mehr Geld verdient wird als im internationalen Drogengeschäft.[15]

In der Szene treten verschiedene Akteure auf, die arbeitsteilig und zunehmend professionell organisiert sind und über unterschiedliche Grade krimineller Energie verfügen (siehe dazu Kapitel 5.2). Insbesondere die Anzahl der technisch weniger qualifizierten unter ihnen, die dafür um so mehr kriminelle Energie aufbringen und mit (gekaufter) Malware die eigentlichen Diebstähle durchführen, dürfte zunehmen. Der Handel mit professionell entwickelter Malware nimmt laufend zu, wobei gleichzeitig ihre Erkennungsrate durch Antivirensoftware abnimmt (siehe dazu Kapitel 2.4 und 5.2).

Es ist ein Wendepunkt feststellbar: Die Zeit der punktuell auftauchenden Phishing-„Wellen“ mit klarem Anfang und Ende dürfte vorbei sein. Vielmehr ist in Zukunft davon auszugehen, dass Angriffe auf E-Banking-Lösungen mit Malware zu einem dauerhaften Geldabfluss führen werden – vergleichbar mit Kreditkartenbetrügereien.

Es ist zu erwarten, dass die Malware-Verteilung gegen Schweizer E-Banking-Portale bald auch über *Drive-by-Infektionen* erfolgen könnte, statt wie bisher bloss per E-Mail (siehe dazu Kapitel 2.1, 2.2, 2.4, 5.1 und 6). Opfer von Gelddiebstahl vom eigenen Bankkonto könnte also bald schon werden, wer ohne ausreichende Sicherheitsvorkehrungen (wie vollständig aufdatiertes Betriebssystem und Anwendungen) im Internet surft und dabei eine präparierte Homepage besucht. Es ist nicht mehr nötig, auf eine verdächtige Mail-Nachricht reagiert zu haben.

So lange international keine besser koordinierte Vorgehensweise bei der Strafverfolgung sowie eine harmonisierte Gesetzeslage implementiert werden können und keine technischen Verbesserungen im Bereich der Sicherheit von E-Banking-Lösungen umgesetzt werden, dürfte sich an der Verbreitung von Malware-Angriffen gegen Finanzdienste wenig ändern. In der Schweiz fehlt zudem eine Strafverfolgungshoheit auf Stufe des Bundes für solche typischerweise interkantonalen und internationalen Fälle. Die Koordination der Ermittlungen zwischen den verschiedenen betroffenen kantonalen Polizeien erschwert die Effizienz und müsste daher zwingend auf Stufe Bund stattfinden. Ausserdem wäre es wichtig, dass bei Vorfällen konsequent Anzeige bei der Polizei erstattet würde.

Die aktuelle Lage wird in Kapitel 2.1 thematisiert, Kapitel 4.2 analysiert Vorfälle in der Schweiz, während in Kapitel 5.2 die internationale Lage untersucht wird.

[15] Siehe z.B.: http://www.vnunet.com/articles/print/2189322; http://www.silicon.com/publicsector/0,3800010403,39166127,00.htm (Stand: 30.07.2007).

4 Aktuelle Lage ICT Infrastruktur national

4.1 Attacken

Webseite einer Schweizer Firma auf dem Gebiet der Weltraumtechnologie angegriffen

Im Juni 2007 wurde ein unautorisierter Zugriff auf den per Passwort geschützten Bereich einer Webseite festgestellt, welche Daten rund um die Forschung von Raketentriebwerken beinhaltet. Dank der installierten Sensoren konnte der illegale Zugriff rasch erkannt und unterbunden werden, so dass keine Daten heruntergeladen werden konnten. Der Zugriff auf die Seite erfolgte von *IP-Adressen* aus dem Nahen Osten, namentlich aus Palästina und Syrien. Ob der Angriff tatsächlich aus diesen Ländern kam oder nur über dortige Computer erfolgte, um die tatsächliche Herkunft zu verschleiern, ist unklar. In diesem Zusammenhang ist es aber erwähnenswert, dass etwa eine Woche vor dem Angriff eine E-Mail ebenfalls mit einer IP-Adresse aus Palästina versendet worden war, die um Zusammenarbeit mit der betroffenen Firma anfragte.

Dieses Beispiel zeigt, dass auch kleinere Betriebe Opfer von Industriespionage-Attacken werden können. Nur das vorbildliche Anwenden von Sicherheitsvorkehrungen konnte in diesem Fall den ungewollten Transfer von Wissen verhindern.

In Kapitel 2.2 nimmt MELANI eine Einschätzung von Angriffen gegen Webserver vor, Kapitel 2.3 thematisiert die gezielte Industriespionage gegen Schweizer Unternehmen.

4.2 Kriminalität

Malware-Angriffe auf Schweizer Finanzdienste

Wie in Kapitel 2.1 erwähnt, haben Angriffe auf schweizerische Finanzinstitute mittels Malware im ersten Semester 2007 stark zugenommen. Vor allem im Mai und im Juni ereigneten sich zwei grössere Vorfälle mit E-Mails, deren Absender gefälscht worden waren.

Eine erste *Spam*-Welle an Schweizer E-Mail-Adressen gab sich als offizielle Mitteilung von Ricardo.ch, einem bekannten Online-Auktionshaus, aus. In der E-Mail wies das vermeintliche Ricardo-Team den Empfänger darauf hin, dass noch eine offene Rechnung zu begleichen sei. Um Einzelheiten zur Rechnung einzusehen, sollte ein Anhang, dem Anschein nach ein Dokument im PDF-Format, geöffnet werden. In Wirklichkeit handelte es sich beim Anhang um ein ausführbares Programm: Durch das Öffnen des Dokuments wurde der eigene PC mit der *Malware* Nurech / Wsnpoem infiziert.

Ein ähnlicher Angriff ereignete sich einige Wochen später. Diesmal wurde die E-Mail im Namen einer Berner Anwaltskanzlei verschickt, die mit dem Angriff aber nichts zu tun hatte. Die Malware versteckte sich wiederum in einer vorgetäuschten Rechnung im PDF-Format. Die Anzahl gültiger elektronischer Adressen, an welche die Kriminellen ihre E-Mail versandt hatten, ist eindrücklich: Die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) erhielt innert weniger Tage über 600 Meldungen zu diesem Vorfall, was einen Rekord darstellt.

In beiden Fällen konnten Opfer nach Öffnen des Anhangs, der vermeintlichen Rechnung, kaum feststellen, dass sie infiziert worden waren: Die meisten Antiviren-Programme waren zur Zeit des Angriffs nicht in der Lage, diese Malware zu erkennen. Diese blieb inaktiv, bis das Opfer via E-Banking auf sein Bankkonto zugreifen wollte. Erst dann deuteten einige ungewöhnliche Vorgänge auf die Präsenz der Malware hin. So wurde beispielsweise eine leere Seite mit einem Balken, auf dem das langsame Laden der Seite in Prozenten angegeben wird, angezeigt oder es öffneten sich Pop-up-Fenster. Diese Anzeigen dienten dazu, das Opfer glauben zu machen, dass die E-Banking-Dienstleistung vorübergehend überlastet sei. In Tat und Wahrheit wurde die Verbindung zum Server unterbrochen, so dass die Kriminellen gleichzeitig illegale Finanztransaktionen im Namen des Opfers ausführen konnten.

Im Gegensatz zu den Fällen von „*Drive-by-Infektionen*“ (siehe dazu die Kapitel 2.2, 2.4, 5.1 und 6) infiziert der User in diesem Beispiel seinen Computer selber, indem er die vermeintliche Rechnung anklickt. Um die Glaubwürdigkeit der E-Mail zu erhöhen, setzten die Angreifer in der Schweiz regional angepasste Mailnachrichten ein – dieselbe Malware wurde auch im Ausland gegen Banken eingesetzt, wurde dort aber mit anderen Mails verschickt oder per Drive-by-Infektion verteilt (siehe dazu Kapitel 5.2). MELANI empfiehlt, Anhänge oder Links in E-Mails niemals ohne die Gewissheit anzuklicken, dass die E-Mail von vertrauenswürdigen Personen stammt und es sich tatsächlich um ein Dokument handelt, welches man erwartet.

Diese Angriffe zielen darauf, E-Banking-Sitzungen zu übernehmen. Wenn Sie einen zweifelhaften Anhang oder Link bereits angeklickt haben sollten, so versichern Sie sich vor der nächsten E-Banking-Sitzung, dass Ihr Computer frei von Malware ist. Suchen Sie dafür allenfalls Rat bei einem Fachmann. Wenn Ihnen während der E-Banking-Sitzung etwas Ungewöhnliches (wie oben beschrieben) auffällt, so wenden Sie sich damit am besten unverzüglich an Ihre Bank.

Die nach den Spamwellen erfolgten Angriffe waren teilweise erfolgreich. Genaue Zahlen über die Höhe der entwendeten Gelder bzw. die Anzahl der Vorfälle liegen MELANI nicht vor. Sie bewegen sich jedoch im Vergleich zu Kreditkarten- und EC-Karten-Betrug auf sehr tiefem Niveau.

Eine Bewertung von Malware-Angriffen gegen Finanzdienste nimmt MELANI in Kapitel 2.1 vor; Trends werden in Kapitel 3.1, die internationale Lage in Kapitel 5.2 thematisiert. Der nächste Beitrag thematisiert klassische Phishing-Angriffe gegen Schweizer Finanzdienstleister. Der Abtransport der Gelder erfolgt meist über „Money Mules“ – siehe dazu Kapitel 4.3.

Klassische Phishing-Angriffe gegen Schweizer Finanzdienste

Phishing-Wellen gegen Schweizer Visa-Kunden

Im ersten Halbjahr 2007 wurden drei *Phishing*-Wellen gegen Schweizer Visa-Kreditkarten-Kunden beobachtet. Diese liefen immer nach dem gleichen Muster ab. In einer *Spam*-E-Mail, welche angeblich von der Sicherheitsabteilung von Visa versendet worden war, wurde die Verifizierung der Kreditkartendaten verlangt, da die entsprechende Kreditkarte möglicherweise missbraucht worden sei. Zu diesem Zweck sollten Vorder- und Rückseite der Karte eingescannt und per E-Mail als PDF-Dokument an die von den Betrügern eingerichtete E-Mail-Adresse versandt werden.

Ein interessantes Detail dieser Spam-E-Mails war, dass jeder Empfänger mit seinem Nachnamen angesprochen wurde. Dieser Name konnte dabei nicht in jedem Falle aus der E-Mail-Adresse abgeleitet werden. Dies deutet daraufhin, dass die E-Mail-Listen der Betrüger

qualitativ besser werden und neben der E-Mail-Adresse durchaus auch andere Angaben enthalten können. Damit können die Täter den Betrug professioneller aussehen lassen und beispielsweise die Opfer, wie oben beschrieben, persönlich ansprechen. Bemerkenswert ist ebenfalls, dass die E-Mails der ersten beiden Wellen in Englisch verfasst wurden. In der dritten Welle haben die Betrüger den Text aber ins Deutsche übersetzt. Dies deutet darauf hin, dass die ersten beiden Versuche zu wenig erfolgreich gewesen waren und die Betrüger auf diese Tatsache reagierten. Anzumerken bleibt, dass es MELANI gelungen ist, die für den Betrug verwendeten Domänen (mit den E-Mail-Adressen) jeweils schnell zu deaktivieren, so dass die Zeitspanne, in der ein Betrug geschehen konnte, sehr klein war.

Keine erfolgreichen „klassischen" Phishing-Versuche gegen Schweizer Finanzinstitute mehr

Auch im ersten Halbjahr fanden zwar „klassische" Phishing-Versuche gegen Schweizer Finanzdienstleister statt. Diese waren von geringer Quantität und Qualität und blieben erfolglos. Die Angriffe zielten beispielsweise nur auf Loginnamen und Passwort, nicht aber auf die Streichlistennummer. Die schlechte Vorbereitung und das zeitweise dilettantische Vorgehen lässt auf eine andere, weniger professionelle Täterschaft als bei den beobachteten Malware-Angriffen schliessen (siehe dazu den letzten Beitrag oben). Eine interessante Erkenntnis ist allerdings, dass diese Angriffe auch gegen kleine, unbekanntere Finanzdienstleister zielten. Auch wurde eine Phishing-E-Mail-Welle in französischer Sprache beobachtet, was in der Schweiz neu ist.

Allgemein lässt sich sagen, dass von „klassischen" Phishing-Angriffen in der Schweiz praktisch keine Gefahr mehr ausgeht – diese liegt heute bei den mit Malware durchgeführten Angriffen.

Eine Bewertung von Malware-Angriffen gegen Finanzdienste nimmt MELANI in Kapitel 2.1 vor; Trends werden in Kapitel 3.1, die internationale Lage in Kapitel 5.2 thematisiert. Malware-Angriffe gegen Schweizer Banken wurden im letzten Beitrag (siehe vorige Seite) thematisiert.

4.3 Diverses

Pump and Dump, fiktive Banken und Money Mules: Diese Spam-Mails verstopfen die elektronischen Briefkästen in der Schweiz

Pump and Dump

Im zweiten Halbjahresbericht 2006 von MELANI ist bereits auf die Existenz der so genannten «Stock Pump and Dump *Spams*» hingewiesen worden (Kapitel 2.2). Solche Spamnachrichten raten zum Kauf von Aktien und dienen dazu, ihre Börsenwerte für kurze Zeit in die Höhe zu treiben. Während dieser Zeit verkaufen die Spammer ihre zuvor gekauften Aktien und profitieren so vom kurzeitig gestiegenen Kurs. Die anfänglich simplen Mitteilungen haben sich inzwischen zu wahren Finanzanalysen entwickelt, die durch ihre gepflegte Sprache bestechen und so ihre Glaubwürdigkeit steigern konnten. Manchmal kommen neue Techniken dazu, so unter anderem die telefonische Kontaktaufnahme.

Fiktive Banken

Der Ruf der Schweiz als Finanzplatz wirkt weiterhin als Magnet für die Gründung fiktiver Online-Banken, in deren Namenszug auf unser Land angespielt wird. Im ersten Halbjahr 2007 wurden mehrere URLs mit Namen wie www.swissbank-offshoreuk.page.tl oder

www.swissbank.page.tl registriert; auf diesen Webseiten wurden sogar Bilder des Direktoriums der Nationalbank platziert, um ihnen einen offiziellen Charakter zu verleihen.

Money Mules

Viele Menschen lassen sich durch die Aussicht auf einen Nebenverdienst, vor allem dann, wenn der Aufwand gering ist und keine besonderen Qualifikationen verlangt werden, dazu verleiten, sich von Kriminellen als sogenannte “Finanzagenten” einspannen zu lassen. Finanzagenten sollen jeden Tag ein bisschen Zeit übrig haben, sich Geld auf ihr Konto überweisen zu lassen, um es von dort aus an Dritte weiterzuleiten. Ein gewisser Prozentsatz des überwiesenen Betrags darf als Provision behalten werden. Diese so genannten Money Mules, also Geldkuriere, die sich für das Reinwaschen von Geldern aus Online-Betrügereien (vor allem *Phishing*) benutzen lassen, sind für Kriminelle immer begehrter. Die zahlreichen Fälle, die MELANI gemeldet werden, sind der Beweis für die Dimensionen, die dieses Phänomen in der Internetkriminalität inzwischen erlangt hat. Parallel zur Zunahme von *Malware*-Angriffen (siehe dazu Kapitel 2, 4.1 und 5.2) wächst auch die Anzahl der Job-Angebote für Geldkuriere, welche meist im Vorfeld von Malware-Angriffen auf E-Banking-Portale ausgeschrieben werden. In einschlägigen E-Mails wird für einfache und einträgliche Tätigkeiten geworben, wobei diese Angebote oft Links auf Internetseiten enthalten, die eigens zu diesem Zweck eingerichtet worden sind.

Im ersten Halbjahr 2007 wurden mehrere solcher Webseiten registriert. Alle wiesen ähnliche Namen und oft dieselbe Machart auf. Die dort auftretenden Unternehmen behaupten, auf den verschiedensten Gebieten tätig zu sein, vom Finanzsektor über das Spendenbusiness bis zum Internethandel. Sie treten mit professionell wirkenden Homepages auf, unter Namen wie Mimotrans, GammaFinance, Next Level oder Donation Europe und versuchen auf diese Weise, ihren potenziellen Kurieren allfällige Zweifel über die Rechtmässigkeit ihres Tuns zu nehmen.[16]

Viele (Cyber-)kriminelle nutzen Bargeld-Transfer-Systeme wie Western Union, MoneyGram etc., um ergaunerte Gelder ins Ausland zu transferieren. Dadurch soll der so genannte Paper-Trail, also die Nachvollziehbarkeit einer Geldüberweisung, unterbrochen werden. Es ist grundsätzlich Vorsicht geboten, wann immer eine unbekannte Person oder Organisation bei einer Finanztransaktion auf den Dienst von solchen Bargeld-Transfer-Instituten besteht. Dies gilt nicht nur für den beschriebenen Fall von Finanzagenten, sondern auch bei Online-Versteigerung von Waren, der Reservation von Hotelzimmern oder bei einem unerwarteten Lottogewinn. MELANI rät, möglichst viele Informationen über die Personen (oder Organisationen) einzuholen, welche einen Bargeld-Transfer verlangen. Im Zweifelsfall gilt: Hände weg! Es ist darauf hinzuweisen, dass Personen, die beim Verschieben von Geldern aus illegalen Aktivitäten mithelfen, sich der Geldwäscherei schuldig machen können.

Internet: Welle von Spam-E-Mails mit Morddrohungen

Anfang Mai wurde eine E-Mail versandt, in der von den Empfängern unter Morddrohungen eine Geldüberweisung verlangt wurde. In der ganzen Schweiz erhielten sehr viele Personen und mehrere Klein- und Mittelbetriebe solche E-Mails. Über Server im Ausland wurde die *Spam*-E-Mail in dilettantischem Deutsch versandt. Der Versand erfolgte zufallsgesteuert und

[16] Ein Beispiel eines solchen falschen Job-Angebots ist zu finden unter: http://www.melani.admin.ch/dienstleistungen/archiv/01023/index.html?lang=de sowie http://www.melani.admin.ch/dienstleistungen/archiv/00441/index.html?lang=de (Stand: 21.08.2007).

ohne erkennbares Muster betreffend Auswahl der Empfänger. Der Inhalt, auch die Drohung, war nicht mehr als ein schlechter Scherz.

Aufgrund des hohen Informationsbedarfes in der Bevölkerung hat das Bundesamt für Polizei in Absprache mit den Kantonen eine Medienmitteilung veröffentlicht. Darin wird den Empfängerinnen und Empfängern empfohlen, keinesfalls auf solche E-Mails zu antworten und irgendwelche persönliche Daten bekannt zu geben.

5 Aktuelle Lage ICT Infrastruktur International

5.1 Attacken

Politisch motivierte DDoS-Attacken gegen Estland werfen Fragen auf

Estland erlebte Ende April über mehrere Wochen andauernde *DDoS-Attacken* über das Internet. Die meisten der angegriffenen Ziele standen über längere Zeit nicht zur Verfügung. Um die Angriffe einzudämmen, sah sich Estland teilweise gezwungen, Internetverbindungen zum Ausland zu unterbinden. Ursache für die Attacken dürfte die Verschiebung eines russischen Denkmals für einen „unbekannten (russischen) Soldaten“ aus der estnischen Hauptstadt Tallinn auf einen Militärfriedhof am Stadtrand gewesen sein. Diese Umplatzierung hatte gewalttätige Demonstrationen der russischen Minderheit in Tallin sowie Angriffe russischer Jugendlicher gegen die estnische Botschaft in Moskau zur Folge. Während das Denkmal nämlich von den Russen primär als Symbol für den Sieg im Zweiten Weltkrieg betrachtet wird, dürfte es von den meisten Esten eher mit der russischen Besetzung während des Kalten Krieges in Zusammenhang gebracht werden. Estland gilt als eines der am weitesten fortgeschrittenen Länder Europas, wenn es um den Einsatz neuer Informations- und Kommunikationstechnologien geht.[17]

Kurz nach Beginn der Angriffe waren die Webseiten des estnischen Präsidenten, des Premierministers, des Parlaments sowie fast aller Ministerien nicht mehr erreichbar. Ab dem 30. April intensivierten sich die Angriffe und weiteten sich gegen estnische Internet Service Provider, Zeitungen, die Mailserver des estnischen Parlaments, Online-Banken, Universitäten und verschiedene andere Internetdienste aus. Am 9. Mai, dem Tag, an dem Russland seines Sieges über Nazi-Deutschland gedenkt, erreichten die Angriffe ihren Höhepunkt: Ausgehend von einem offenbar über eine Million infizierter „Zombies“ zählenden, weltweit verteilten *Botnetz* erfolgten weitere Attacken mit teilweise beträchtlicher Bandbreite. Am 10. Mai hörten die

[17] Siehe für Hintergrundinformationen zu diesem Vorfall:
http://www.economist.com/world/europe/displaystory.cfm?story_id=9163598;
http://www.hs.fi/english/article/Virtual+harassment+but+for+real+/1135227099868 (Stand: 16.07.2007).

heftigen DDoS-Attacken wieder auf, vermutlich weil die 24-stündige Mietzeit für das benutzte Botnetz inzwischen abgelaufen war.[18]

Kurz nach Beginn der Angriffe erklärten estnische Offizielle, es lägen Beweise für einen Ursprung der Angriffe im Kreml vor.[19] Doch spätere Analysen – auch von internationalen Experten, die von der NATO, den USA, Israel sowie der EU vor Ort geschickt worden waren – zeigten, dass der Angriff nicht auf Moskau zurückgeführt werden kann. Vielmehr muss davon ausgegangen werden, dass es sich um einen typischen Fall von „Hacktivismus" – also politisch motiviertem Hacken – handelte. Diese Vermutung wird dadurch gestützt, dass die Angriffe von verschiedenen Quellen stammten, in unterschiedlicher Intensität erfolgten sowie unterschiedlich lange dauerten. Zudem seien die Angriffe viel zu wenig elaboriert gewesen, als dass dahinter eine Regierung zu vermuten wäre.[20] Grundsätzlich verhält es sich in diesem Fall ähnlich wie bei der allgemeinen Cyberkriminalität: Es ist ausserordentlich schwierig, den Urheber eines Angriffs zweifelsfrei zu identifizieren.

Die DDoS-Angriffe gegen Estland waren nicht die einzig bedeutsamen in der ersten Jahreshälfte 2007: Nachdem im Februar ein (erfolgloser) Angriff gegen mehrere *DNS*-Rootserver erfolgte, gerieten im Juni auch Anti-Spam-Dienstleister ins Visier.[21] Diese Angriffe zeigen, über welche Ressourcen die Organisierte Kriminalität inzwischen verfügt: Ihre Botnetze werden nicht nur zwecks Versand von *Spam*-E-Mails vermietet. Auch Interessenten für DDoS-Angriffe sind bereit, für Botnetze zu bezahlen, wie dies mit grösster Wahrscheinlichkeit bei den Attacken gegen Estland der Fall war.

DDoS-Angriffe mit politischem Hintergrund – genauso wie Verunstaltungen von Homepages (so genannte „*Defacements*") mit politischen Pamphleten – sind nichts Neues. Anlässlich der versehentlichen Bombardierung der Chinesischen Botschaft im Kosovo-Krieg Ende der 1990er-Jahre, des Beginns des letzten Irakkriegs 2003 oder der Mohamed-Karikaturen in dänischen Zeitungen 2006 waren ähnliche Angriffe erfolgt. Auch dieses Mal konnte beobachtet werden, wie in einschlägigen Foren Anleitungen kursierten, wie auch technisch Unversierte auf einfache Art estnische Webseiten angreifen können. Neu ist hier jedoch das Ausmass des Angriffs, der in der Lage war, einen gesamten Kleinstaat in der Nutzung seiner Informationstechnologien massiv zu beeinträchtigen.

Die Angriffe auf Estland können nach heutigem Erkenntnisstand nicht mit dem offiziellen Russland oder einem anderen konkreten Akteur in Verbindung gebracht werden. Einige Hinweise lassen aber darauf schliessen, dass ihr Ursprung wohl eher im Kreis russischer Nationalisten zu finden sein dürfte. Inwiefern Absprachen, Anstiftungen, oder gegenseitige Unterstützung zwischen den vermuteten Akteuren bestanden haben, ist dabei nicht zu eruieren. Trotzdem werden wichtige Fragen aufgeworfen: Wie ist ein Angriff mit Cybermitteln gegen einen Staat im (Kriegs-)Völkerrecht zu berücksichtigen? Was bedeutet er für die NATO und den Artikel 5 des NATO-Vertrags, der im Falle eines militärischen Angriffs gegen

[18] Siehe http://www.nytimes.com/2007/05/29/technology/29estonia.html?hp sowie http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html (Stand: 16.07.2007).

[19] Siehe dazu: http://www.heise.de/tp/r4/artikel/25/25218/1.html; http://www.tagesspiegel.de/politik/International;art123,1785339 (Stand: 16.07.2007).

[20] Die ausführlichste Analyse lieferte Arbor Networks: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/; auch das US-CERT kommt zum selben Schluss: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/print_view/ (Stand: 16.07.2007).

[21] Siehe zu vergleichbaren DDoS-Angriffen auch den MELANI-Halbjahresbericht 2006/I, Kapitel 5.3; sowie zu den Angriffen gegen die DNS-Rootserver: http://asert.arbornetworks.com/2007/06/february-2007-root-server-attacks-a-qualitative-report/ (Stand: 16.07.2007).

ein NATO-Mitglied diesen automatisch auf einen gegen alle NATO-Mitglieder gerichteten Angriff eskaliert (der so genannte kollektive Verteidigungsfall)?[22]

Die NATO hat diese Frage um die sogenannten „Information Operations" bereits in ihre Agenda aufgenommen und will einerseits eine bessere Verteidigungsfähigkeit gegen Angriffe auf Informationssysteme erreichen und andererseits den Artikel 5 auf solche Vorkommnisse ausweiten.[23] Generell ist die Frage von Cyberangriffen im Völkerrecht ungeklärt – und dies, obwohl das Beispiel von Estland zeigt, wie abhängig heutige Volkswirtschaften von Informationstechnologien sind.

Nicht nur die NATO, sondern auch Nationalstaaten sind dabei, ihre Kapazitäten im Bereich des Informationskrieges auf- und auszubauen (siehe dazu auch Kapitel 7.1).

Angriffe über das World Wide Web (Drive-by-Infektionen): Beispiel „MPack"

So genannte „*Drive-by-Infektionen*" (Installation von *Malware* beim Besuch infizierter Webseiten) haben im ersten Halbjahr 2007 zugenommen und stellen eine der aktuellsten Bedrohungen dar (siehe Kapitel 2.2, 2.4 sowie den letzten Halbjahresbericht). Das prominenteste Beispiel zur Illustrierung dieses Trends ist „MPack" – eine Applikation für Webserver, mit der im Juni erfolgreich die Rechner von zehntausenden von Websurfern allein durch den Besuch von präparierten Webseiten mit Malware infiziert worden sind. MPack ist in der Untergrund-Malware-Szene als Toolkit mit Support und regelmässigen Updates erhältlich (siehe zur Malware-Szene, Preisen etc. Kapitel 5.2).[24]

Insbesondere Webseiten in Italien – offenbar über 10'000[25] – wurden von den Angreifern durch Hinzufügen einer Code-Zeile so manipuliert, dass während des Ladens der Seite Malware von einem anderen Server nachgeladen wird. Diese enthält MPack, ein Tool zur automatischen Infizierung. Zunächst prüft dieses, welches Betriebssystem und welchen Browser das Opfer einsetzt, um anschliessend je nach eingesetzten Applikationen passende *Exploits* der Reihe nach durchzuprobieren – also gleichzeitig mehrere *Sicherheitslücken* auszunutzen (z.B. in verschiedenen Microsoft-Produkten wie Internet Explorer, Windows Betriebssystem-Dienste, Media Player u.a., aber auch in WinZip oder Apples QuickTime). MPack nutzte bisher zwar nur bekannte Sicherheitslücken aus. Systeme, die vollständig – aufdatiert waren, konnten nicht infiziert werden. Denkbar ist aber auch, dass ein solches Tool jederzeit um *0-day-exploits* erweitert wird.

Sobald ein Exploit funktioniert, kann beliebig weitere Malware auf das infizierte System geladen werden. Dies kann auch solche wie beispielsweise „Torpig" (siehe dazu Kapitel 4.2 und 5.2), die gegen bisher nur ausländisches E-Banking gerichtet ist, oder Malware zur Sammlung persönlicher Daten sein. Denkbar ist auch eine Integration der infizierten Rechner in ein *Botnetz*, das anschliessend beispielsweise für *Spam*-Versand eingesetzt werden kann. Der Angriff über die italienischen Webseiten infizierte offenbar erfolgreich über 80'000

---

[22] Siehe dazu http://www.economist.com/world/international/displaystory.cfm?story_id=9228757 (Stand: 16.07.2007).

[23] Siehe http://www.nato.int/docu/pr/2007/p07-067e.html (Stand: 16.07.2007).

[24] Allgemeine Informationen zu MPack: http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=8656&ver=21&pagina=3&numprod=&entorno=; http://reviews.cnet.com/4520-3513_7-6745285-1.html; http://www.heise.de/newsticker/meldung/91542 sowie http://blog.washingtonpost.com/securityfix/2007/06/the_mother_of_all_exploits_1.html (Stand: 17.07.2007).

[25] Siehe dazu: http://www.websense.com/securitylabs/alerts/alert.php?AlertID=782 (Stand: 17.07.2007).

Rechner. Bei den manipulierten Webseiten handelte es sich zumeist um Tourismus-, Hotel-, Autovermietungs- oder andere keineswegs dubiose Angebote.[26]

Wie das ISC SANS berichtete, wurden die kompromittierten Webseiten zu tausenden auf nur wenigen physischen Servern gehostet. Die Kompromittierung sämtlicher Webseiten erfolgte offenbar durch eine Sicherheitslücke auf einer einzelnen Webseite, welche die Angreifer in Kombination mit einer mangelhaften Konfiguration des Servers auf Providerebene ausnutzen konnten. Mit anderen Worten reichte eine einzige schlecht gewartete Webseite auf diesem Server aus, um alle anderen darauf gespeicherten Webseiten zu gefährden.[27]

Bemerkenswert an dieser Art Angriff ist, dass immer mehr seriöse Webseiten Opfer von Hackerangriffen werden und anschliessend ohne das Wissen der verantwortlichen Webmaster Malware verbreiten (siehe dazu Kapitel 2.2). Surfen mit vollen Administrationsrechten wird somit zu einem erheblichen Risiko, insbesondere auch für Firmen.

Ohne etwas anzuklicken, ohne ein Attachment zu öffnen oder eine E-Mail erhalten und darauf reagiert zu haben, ist es möglich, mit Malware infiziert zu werden – theoretisch gar mit vollständig aufdatiertem Betriebssystem und Applikationen und dies alles allein durch den Besuch einer seriösen Homepage. In der Praxis werden jedoch heute fast ausschliesslich bekannte Sicherheitslücken ausgenutzt, die bei aufdatierten Computern nicht auftreten.

Kapitel 2.2 thematisiert die zunehmenden Angriffe gegen Webserver, während Kapitel 6 sich mit präventiven Massnahmen gegen Drive-by-Infektionen befasst.

5.2 Kriminalität

Phishing- und Malware-Angriffe gegen Finanzdienste: Internationaler Status

Nicht nur in der Schweiz (siehe Kapitel 2.1 und 4.2) sind *Phishing*- und *Malware*-Angriffe aktuell. Auch international setzt sich der Trend zu Angriffen gegen Finanzdienstleister per Malware durch. Die Anti-Phishing Working Group berichtet in ihren Statistiken für die erste Jahreshälfte 2007 beispielsweise von einer beträchtlichen Zunahme an Webseiten, die Malware zu diesen Zwecken verteilen.[28]

Der spektakulärste Zwischenfall wurde Anfang Jahr in Schweden bekannt, wo die grösste skandinavische Bank Nordea Opfer eines erfolgreichen Malware-Angriffs geworden war. Erbeutet wurden etwa 900'000 Euro von mindestens 250 Bankkunden. Zum Einsatz kam eine extra für diesen Angriff massgeschneiderte Malware, die auf dem russischen Untergrundmarkt für einige tausend US-Dollar von einem Programmierer namens „The Corpse“ gekauft werden konnte (siehe dazu den übernächsten Beitrag). Geliefert wird die Malware mit der Garantie, dass diese von Antivirensoftware nicht erkannt werden kann. Die von der Nordea-Bank eingesetzte *Zwei-Faktor-Authentifizierung* – vergleichbar mit den von Schweizer Banken eingesetzten Authentifikationssystemen – konnte erfolgreich umgangen

[26] Detailinformationen zu MPack sind zu finden bei: http://blogs.pandasoftware.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf?sitepanda=particulares sowie http://isc.sans.org/diary.html?storyid=3015 (Stand: 17.07.2007).

[27] Siehe: http://isc.sans.org/diary.html?storyid=3078 (Stand: 17.07.2007).

[28] Siehe: http://www.antiphishing.org; http://www.darkreading.com/document.asp?doc_id=123771 (Stand: 18.07.2007).

werden.[29] Auch in anderen Ländern erfolgten zahlreiche erfolgreiche *Man-in-the-Middle*-Angriffe (MITM-Angriff), wie beispielsweise in den Niederlanden gegen die ABN Amro Bank im April.[30]

Im ersten Halbjahr 2007, insbesondere im April, wurde eine starke Zunahme der Phishing-seiten beobachtet, wobei die Zahl der gemeldeten Vorfälle seit etwa einem Jahr konstant bleibt.[31] Ursache dafür dürfte die Tatsache sein, dass Phishing-Kits sich immer weiter ausbreiten.[32] Bei diesen Kits handelt es sich um Tools, oft mit einfacher grafischer Benutzer-oberfläche, die von Programmierern mit Expertenkenntnissen verkauft werden und mit denen auch Anfänger relativ leicht Phishing-Angriffe durchführen können (siehe dazu auch den Beitrag zu „RockPhish“ im letzten Halbjahresbericht sowie den übernächsten Beitrag). Mit den Tools lassen sich hunderte von Phishing-Seiten (oder Proxy-Seiten für MITM-Angriffe) aufsetzen, die allein aufgrund ihrer grossen Anzahl schwer zu bekämpfen und damit ziemlich ausfallsicher sind.[33] Die Anzahl Gruppen, die Phishing auf hohem Niveau betreiben, dürfte jedoch in etwa konstant geblieben sein.

Gegen einfachere Authentifikationssysteme sind nach wie vor klassische Phishing-Angriffe per E-Mail und Abfrage von Benutzernamen und Passwort im Gang, wie unter anderem ge-gen Nutzer von Social-Networking-Homepages wie z.B. MySpace.[34]

Einer der wichtigsten Gründe für die Zunahme von Malware-Angriffen dürfte die fortschrei-tende Einführung der Zwei-Faktor-Authentifizierung im angelsächsischen Raum sein: Pay-Pal, Ebay und Barclays, eine der grössten britischen Banken, sind dafür bloss die promi-nentesten Beispiele.[35] Ursache dafür ist eine im August 2006 erneut betonte Empfehlung der US-amerikanischen Bankenaufsichtsbehörde vom Oktober 2005, dass Banken Zwei-Faktor-Authentifizierung einsetzen sollten. Diese Empfehlung befolgen immer mehr Banken; bis Ende dieses Jahres dürften daher die meisten Banken im angelsächsischen Raum zu den in Europa und vor allem in der Schweiz hohen Sicherheitsstandards aufgeholt haben.[36] Während bisher aufgrund der weiten Verbreitung einfacherer Ziele Angreifer sich nicht die Mühe machten, zwei-faktor-geschützte Systeme zu attackieren, hat sich dies nun geändert.

Bemerkenswert ist ausserdem, dass im Ausland teilweise dieselbe Malware(-Familie) für Angriffe gegen Finanzdienste zum Einsatz kam wie in der Schweiz. Diese wurden aber über anders aufgemachte E-Mails oder teilweise gar per *Drive-by-Infektion* verteilt (siehe dazu

---

[29] Infos zum Nordea-Zwischenfall: http://www.nytimes.com/2007/01/25/technology/25hack.html?ex=1327381200&en=58990497ce27b2b2&ei=5088&partner=rssnyt&emc=rss (Stand: 18.07.2007).

[30] Siehe zum ABN Amro-Zwischenfall: http://www.theregister.co.uk/2007/04/19/phishing_evades_two-factor_authentication/ (Stand: 18.07.2007).

[31] Siehe die Berichte der Anti-Phishing Working Group: http://www.antiphishing.org (Stand: 18.07.2007).

[32] Siehe: http://blogs.iss.net/archive/PhishingIncreases.html; http://blogs.iss.net/archive/PhishingKits.html; http://www.rsa.com/solutions/consumer_authentication/intelreport/FRARPT_DS_0607.pdf; http://www.rsa.com/press_release.aspx?id=7667; http://asert.arbornetworks.com/2007/04/peeling-the-covers-off-of-rock/; http://blog.washingtonpost.com/securityfix/2007/05/phishing_attacks_soar_nets_wid_1.html (Stand: 18.07.2007).

[33] Eine anschauliche Übersicht über die Vorgehensweise ist zu finden unter: http://blogs.iss.net/archive/PhishingMicroscope.html (Stand: 18.07.2007).

[34] Siehe dazu: http://isc.sans.org/diary.html?storyid=2808; oder ein Interview mit einem MySpace-Phisher unter: http://ha.ckers.org/blog/20070508/phishing-social-networking-sites/ (Stand: 18.07.2007).

[35] Siehe dazu: http://www.infoworld.com/article/07/06/15/paypal-using-verisign-tokens_1.html (Stand: 18.07.2007).

[36] Siehe dazu: http://www.ffiec.gov/press/pr101205.htm; http://www.ffiec.gov/press/pr081506.htm; sowie http://www.darkreading.com/document.asp?doc_id=129868&f_src=darkreading_default (Stand: 18.07.2007).

Kapitel 2.2, 2.4 und 5.1). Die *Social-Engineering*-Methoden werden von den Angreifern also regional angepasst.

Eine Einschätzung zu Phishing- und Malware-Angriffen sowie zur Sicherheit der Zwei-Faktor-Authentifizierung ist in Kapitel 2.1 zu finden. Kommentare zu Vorfällen in der Schweiz sind in Kapitel 4.2 aufgeführt.

Ungewollte Datenoffenlegung durch gezielte Industriespionage oder Verlieren von Datenträgern bleibt aktuell: Beispiel TJX

Den meisten Datenverlusten liegen verlorene oder gestohlene Laptops, Backup-Bänder, CD-ROMs, USB-Sticks oder andere Speichermedien zu Grunde. Sogar das FBI hat in den letzten vier Jahren 160 Laptops verloren und war sich nicht sicher, auf welchen genau vertrauliche Daten gespeichert waren.[37] Wie in den Kapiteln 2.2 und 2.3 erläutert, erfolgen aber immer mehr Datenverluste auch durch gezielte (*Social-Engineering*) Angriffe gegen Mitarbeitende, auf Webserver und andere Systeme.

Ein prominentes Beispiel stellt der Vorfall bei der angloamerikanischen Kaufhauskette TJX dar. Wie Anfang Jahr bekannt wurde, waren seit Juli 2005 offenbar systematisch über 45 Millionen Kreditkartendatensätze aus den Zahlungsabwicklungs- und Speicherungssystemen des Unternehmens gestohlen worden. Der Einbruch in die Informationssysteme wurde erst im Dezember 2006 bemerkt. In der anschliessenden Untersuchung wurde festgestellt, dass die Angreifer immer wieder auf die Systeme zugegriffen hatten. Ihr Zugang konnte erst im Januar 2007 definitiv unterbunden werden. Es handelt sich bei diesem Vorfall um den bisher grössten Kreditkartennummerndiebstahl überhaupt: Nach Aussagen von Bankenvereinigungen waren vermutlich bis zu 30% der Bevölkerung Neuenglands betroffen. Offenbar wurde in Florida bereits ein Kartenhändlerring verhaftet, der von TJX beschaffte Kreditkartendaten missbräuchlich eingesetzt hatte. Die Kreditkartendaten wurden über einschlägige Seiten im Internet verkauft. Über die für TJX entstandenen Kosten ist lediglich bekannt, dass alleine die Untersuchung des Vorfalls sowie anschliessende Massnahmen zur Erhöhung der Informationssicherheit 5 Millionen US-Dollar gekostet haben. TJX dürfte aber aufgrund bereits eingegangener Klagen mit deutlich höheren Kosten konfrontiert werden, zumal Banken offenbar dutzende von Millionen US-Dollar an Kunden kompensieren mussten. Das Wall Street Journal schätzt die langfristigen Kosten für TJX auf bis zu einer Milliarde US-Dollar. Zugriff auf das Netzwerk erhielten die Täter offenbar über ungenügend geschützte WLANs und anschliessendes Mitlesen von Passwörtern sowie durch das Einsetzen von Spionagesoftware.[38]

Wie in Kapitel 2.3 erwähnt, erfolgen Angriffe gegen Unternehmen heute vor allem gezielt. Ausser geschickt gestalteten E-Mails, welche an ausgewählte Personen versendet werden und einen Link zu einer mit *Malware* verseuchten Webseite oder Malware im Anhang

[37] Siehe den Bericht des US-Department of Justice: http://www.usdoj.gov/oig/reports/FBI/a0718/exec.htm (Stand: 19.07.2007).

[38] Siehe:
http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/;
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009300;
http://www.infoworld.com/article/07/03/29/HNtjxfiling_2.html sowie
http://online.wsj.com/article_email/article_print/SB117824446226991797-lMyQjAxMDE3NzA4NDIwNDQ0Wj.html.
Eine Übersicht über Datendiebstähle in den USA ist zu finden unter:
http://www.privacyrights.org/ar/ChronDataBreaches.htm (Stand: 19.07.2007).

beinhalten (siehe Kapitel 2.3), finden auch häufig Angriffe auf Webserver (siehe Kapitel 2.2 und 5.1) oder wie im Fall von TJX über WLAN statt.

Sensible Daten sollten deshalb von Unternehmen verschlüsselt gespeichert werden (insbesondere auf Laptops, PDAs, USB-Sticks, CD-ROMs oder Backup-Bändern). Bezüglich des Vorfalls bei TJX ist auch anzumerken, dass WLANs verschlüsselt werden sollten.

Untergrund-Markt und Cyberkriminalität: Neuste Trends und Preise

Die Arbeitsteilung innerhalb der cyberkriminellen Szene wurde bereits im letzten Halbjahresbericht sowie in Kapitel 3.1 thematisiert. An dieser Stelle soll anhand aktueller Beispiele gezeigt werden, zu welchen Preisen einige Dienstleistungen erhältlich sind.

Im ersten Halbjahr 2007 konnte ein Trend hin zu „*Malware*-Kits“ festgestellt werden, wie das Beispiel von MPack (siehe Kapitel 5.1) zeigt. Das Toolkit, erhältlich mit Support und regelmässigem Update der verwendbaren *Exploits*, wurde von einem gewissen „$aSH“ auf dem russischen Untergrundmarkt ursprünglich für 1000 US-Dollar angeboten.[39] Mit zunehmender Bekanntheit tauchte es bald auch von Trittbrettfahrern angeboten zu Dumpingpreisen auf.[40] Das Entwicklungsteam besteht offenbar aus drei Personen, während $aSH von einem Entwickler als „Marketing Director“ bezeichnet wurde. Gemäss den Angaben des Entwicklers werden die für das Kit verwendeten Exploits getauscht, aus bekannten *Sicherheitslücken* abgeleitet oder aber selber auf dem Untergrundmarkt gekauft. Bei der Gruppe handelt es sich offenbar um Entwickler mit legaler Arbeitsstelle, die sich selber nicht als Kriminelle sehen, in der Freizeit aber dennoch Malware entwickeln und verkaufen.[41]

Auch die für den Angriff auf die schwedische Bank Nordea (siehe dazu den ersten Beitrag in Kapitel 5.2) verwendete Malware namens Haxdoor ist auf dem Untergrundmarkt erhältlich. Einem schwedischen Journalisten wurde für 3000 US-Dollar eine angepasste und für Antivirensoftware unerkennbare Version angeboten. Diese Malware stammt offenbar von einem allein arbeitenden Entwickler namens „Corpse“, der diese auch selbst anbietet – ebenfalls inklusive Support und, falls gewünscht, einem sicheren Online-Speicherplatz für gestohlene Daten (bullet-proof hosting).[42]

Für cyberkriminelle Bedürfnisse ist auf dem Markt beim „Experten“ (fast) alles erhältlich: Malware, Exploits, Wissen über Sicherheitslücken, *Botnetze* für den Versand von *Spam* oder zur Erpressung mit *DDoS*-Angriffen, sicherer Hostingplatz für Malware oder illegitime Daten.[43] Die Preise werden entweder pro Zeiteinheit verrechnet (DDoS-Angriff pro Stunde zwischen US$ 10 und 20), pro Spam-Server und versandte Spams (10'000’000 Mails pro Tag für US$ 600), pro Account (für russische E-Business-Seiten US$ 50, EBay- oder

---

[39] Eine Studie zur russischen Szene ist zu finden unter: http://www.verisign.com/static/042139.pdf (Stand: 26.07.2007).

[40] Siehe http://isc.sans.org/diary.html?storyid=3015; sowie http://www.theregister.co.uk/2007/07/06/pirate_mpack_toolkit/ (Stand: 24.07.2007).

[41] Siehe das Gespräch mit dem Entwickler namens DCT auf SecurityFocus: http://www.securityfocus.com/news/11476 (Stand: 24.07.2007).

[42] Siehe ein „Interview“ mit dem Anbieter „Corpse“: http://computersweden.idg.se/2.2683/1.93344 (Stand: 24.07.2007).

[43] Siehe dazu z.B.: http://asert.arbornetworks.com/2007/04/botconomics-the-monetization-of-your-digital-assets/; http://www.networkworld.com/news/2007/050907-fbi-organized-crime-cybercrime.html; http://www.theregister.co.uk/2007/06/13/black_hat_list/ sowie http://www.washingtonpost.com/wp-dyn/content/article/2007/03/13/AR2007031301522.html (Stand: 24.07.2007).

PayPal-Accounts für US$ 7) oder pro Karte (Kreditkartennummern inklusive PIN für US$ 500, ohne PIN aber mit allen für E-Business benötigten Daten für US$ 25). *Keylogger* sind ab US$40 erhältlich, ein *trojanisches Pferd* ist für einige hundert bis tausende von US$ zu haben, je nach Typ.[44] Unter den Anbietern herrscht offensichtlich starke Konkurrenz.[45]

Immer mehr IT-Sicherheitsdienstleister versuchen inzwischen einen legitimen Markt für Sicherheitslücken und Exploits zu schaffen, indem sie entweder selber dafür bezahlen oder aber Online-Versteigerungsplattformen[46] unterhalten. Wie hier allerdings dubiose Käufer ausgeschlossen werden können und ob dieser Schritt den florierenden Untergrundmarkt eindämmen kann, ist stark umstritten.[47]

Die Cybercrime-Szene ist arbeitsteilig und effizient organisiert. Für jeden Interessenten gibt es Aufgaben, je nach Kenntnisstand und krimineller Energie. Während „Experten" Malware, Exploits, Toolkits etc. entwickeln und meist auch selbst verkaufen, setzen andere diese ein, beispielsweise um Botnetze zu betreiben, Datendiebstähle zu begehen sowie Phishing- oder Industriespionageangriffe durchzuführen. Für erbeutete Daten stehen ebenfalls Untergrundmärkte zur Verfügung.[48]

Für ihre Arbeit müssen die „Experten" mit anderen Worten weniger kriminelle Energie aufbringen als die Käufer ihrer Produkte, welche dafür selbst über kein Expertenwissen verfügen müssen. Die Käufer begehen anschliessend die eigentlichen Daten- und daraus folgenden Geld- oder Identitätsdiebstähle oder rekrutieren dafür weiteres Personal.

Die wahren Umsätze der Szene können nur geschätzt werden – es handelt sich jedoch ohne Zweifel um ein lukratives Geschäft bei noch immer sehr tiefen Risiken.[49]

---

[44] Zahlen von: http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/04/23/Cybercrime_2E002E002E00_-for-sale-_2800_I_2900_.aspx; http://blogs.pandasoftware.com/blogs/pandalabs/archive/2007/05/03/Cybercrime_2E002E002E00_-for-sale-_2800_II_2900_.aspx; http://www.heise.de/security/news/meldung/82679; http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9025464&intsrc=industry_list (Stand: 24.07.2007).

[45] Siehe z.B. http://www.theregister.co.uk/2007/07/01/malware_gang_war/; http://www.viruslist.com/en/analysis?pubid=204791938#inet; http://www.darkreading.com/document.asp?doc_id=122116&WT.svl=news1_1 (Stand: 24.07.2007).

[46] Siehe z.B. http://www.wslabi.com/wabisabilabi/initPublishedBid.do? (Stand: 24.07.2007).

[47] Siehe dazu: http://www.economist.com/science/displaystory.cfm?story_id=9507422; http://www.theregister.co.uk/2007/01/25/bug_brokers_offering_higher_bouties/; http://www.securityfocus.com/news/11468 sowie den Bericht eines legitimen Wissenschaftlers über seine Erfahrungen im Verkauf seiner Ergebnisse: http://weis2007.econinfosec.org/papers/29.pdf (Stand: 24.07.2007).

[48] Siehe z.B.: http://blog.washingtonpost.com/securityfix/2007/03/stolen_identities_two_dollars.html; http://www.itseccity.de/content/virenwarnung/statistiken/070327_vir_sta_symantec.html (Stand: 25.07.2007).

[49] Siehe dazu z.B.: http://www.vnunet.com/2189322, http://www.theregister.co.uk/2007/03/19/fbi_crime_report_2006/ sowie den Bericht des FBI Internet Crime Complaint Center mit Zahlen zu den USA: http://www.fbi.gov/page2/march07/ic3031607.htm (Stand: 24.07.2007).

5.3 Terrorismus

London: Bombenangriff gegen Internetknoten vereitelt

Wie Scotland Yard im März bekannt gab, waren offenbar bereits 2006 während Hausdurchsuchungen bei Terrorverdächtigen Pläne auf Computerfestplatten gefunden worden, die einen terroristischen Angriff gegen den wichtigen Internetknotenpunkt „London Internet Exchange“ (LINX) nahe legten.[50]

Gemäss den gefunden Plänen beabsichtigten die Verdächtigen, sich in die Hauptquartiere der Telehouse Europe in den Telehouse Docklands einzuschleichen, wo sich ein grosser Teil von LINX physisch befindet, um mit einem Bombenattentat das britische Internet zu beeinträchtigen. Auch wenn in den Artikeln zum Thema behauptet wird, dies hätte die britischen Inseln quasi vom Internet getrennt, stimmt dies keinesfalls: LINX betreibt zwei vollständig voneinander getrennte Netzwerke, welche geographisch über sieben verschiedene Orte verteilt sind, so dass der Ausfall eines einzelnen Knotenpunkts nicht die beschriebenen dramatischen Auswirkungen gehabt hätte. Dies gilt auch für denjenigen bei den Telehouse Docklands, obwohl es sich dabei um den wichtigsten handelt. Zudem muss an dieser Stelle auch festgehalten werden, dass Internetknotenpunkte dieser Grössenordnung physisch ausgezeichnet geschützt sind, was einen Bombenangriff erschweren dürfte.[51] Neben dem Angriff gegen den Internetknotenpunkt wurden auch Pläne für Attentate gegen Gasleitungen, Öllager und Kommunikationsinfrastrukturen gefunden. Die Pläne befanden sich allesamt noch in einem Anfangsstadium.

Der aufgedeckte Plan zeigt, dass sich terroristische Kreise offenbar immer mehr auf Angriffe gegen *kritische (nationale) Infrastrukturen* vorbereiten. Wie in den letzten Halbjahresberichten (v.a. 2005/II) erwähnt, verfügen Terroristen jedoch (vorläufig) noch kaum über das nötige Know-how, um solche Angriffe über Netzwerke allein mit informationstechnologischen Mitteln durchführen zu können. Daher stehen Angriffe mit konventionellen Mitteln (auch gegen solche Ziele) offenbar noch im Vordergrund.

Die Auswahl der Ziele scheint jedoch neben einer Maximierung der Opferzahlen oder neben dem hohen Symbolcharakter nun zunehmend auch nach Kriterien der erzielbaren wirtschaftlichen Schäden zu erfolgen.

[50] Siehe dazu: http://www.timesonline.co.uk/tol/news/uk/crime/article1496831.ece; http://www.technologyreview.com/blog/garfinkel/17561/ sowie http://www.daniweb.com/blogs/entry1345.html (Stand: 25.07.2007).

[51] Siehe dazu: https://www.linx.net/pubtools/topology.html; http://en.wikipedia.org/wiki/London_Internet_Exchange; http://en.wikipedia.org/wiki/Telehouse (Stand: 25.07.2007).

6 Prävention

6.1 Schwerpunkt: Drive-by-Infektionen

Geht es um die Sicherheit eines Computers, ist das Verhalten jedes einzelnen Benutzers mitentscheidend. Der sorgsame Umgang mit E-Mails oder mit heruntergeladener Software ist dabei selbstverständlich. Jeder sollte inzwischen misstrauisch werden, wenn beispielsweise Rechnungen von Firmen via E-Mail eintreffen, speziell wenn man mit diesen Firmen noch nie zu tun gehabt hat. Ziel dieser E-Mails ist es, die Empfänger zum Öffnen eines Anhangs zu verleiten, bevor sich diese überlegt haben, ob die E-Mail überhaupt Sinn macht. Es gilt grundsätzlich, lieber einmal zu viel misstrauisch zu sein als einmal zu wenig. Doch selbst wenn man sich an die gängigen Verhaltensregeln hält, ist man heute nicht zu hundert Prozent vor Schaden sicher.[52]

Ein zunehmend wichtiger Grund dafür heisst *Drive-by-Infektion*. Gemeint ist eine Infektion mit einer *Malware* beim blossen Besuch einer Webseite. Die verbreitete Meinung, dass solche Infektionen nur auf Seiten dubioser Anbieter, wie beispielsweise Pornographie- oder Spielseiten stattfinden, stimmt dabei schon längst nicht mehr. Benutzer von Suchmaschinen – und das ist praktisch jeder von uns – setzen sich ebenfalls einem Risiko aus. Eine Stichproben-Untersuchung von durch Suchmaschinen indexierten Webseiten hat eine Verbreitung von Seiten mit Drive-By-Infektionen von rund 10% ergeben (siehe dazu auch Kapitel 2.2).[53] Die grosse Zahl liegt darin begründet, dass Kriminelle beginnen, ganze Webserver zu übernehmen und alle darauf gehosteten Seiten mit Malware zu versehen (siehe dazu Kapitel 5.1). Im Frühling dieses Jahres ist beispielsweise eine Webseite zum Thema Eishockey gehackt und anschliessend zum Verteilen von Malware missbraucht worden. Dies ist just an dem Wochenende geschehen, an dem das Finalspiel der Eishockeyweltmeisterschaft stattgefunden hat. Die Effizienz dieser Methode kann man sich gut vorstellen. Eine andere Vorgehensweise, um Malware über Webseiten zu verbreiten, ist der Einsatz so genannter Typodomains. Hierbei werden Domänen registriert, die sich ähnlich schreiben wie allgemein bekannte Seiten. Vertippt man sich beim Aufruf einer Webseite, wird versucht, auf dem Computer Malware zu installieren.

Wie wird der Computer infiziert?

Die Browser sind heute so konfiguriert, dass eine Datei nicht automatisch heruntergeladen und gestartet wird. Es ist jeweils eine Benutzerinteraktion notwendig und man wird auch auf die Gefahren eines Downloads hingewiesen. Eine Drive-by-Infektion funktioniert hingegen ohne Benutzerinteraktion. Möglich wird dies, da nahezu jedes Programm, das auf dem Computer eingesetzt wird, von *Sicherheitslücken* betroffen sein kann. Solange diese Lücken nicht geschlossen werden, sei es weil der Hersteller noch keinen *Patch* zur Verfügung gestellt oder der Benutzer diesen noch nicht installiert hat, können präparierte Seiten oder Dokumente eine Infektion mit einer Malware bewirken. Besonders gefährlich wird dies, wenn Schwachstellen den Web-Browser oder andere Programme betreffen, die auf das Internet zugreifen. Dies sind beispielsweise in den Browser integrierte *Plugin*-Programme wie Movie-Player (Flash, QuickTime, RealPlayer, Windows Media Player) oder der Adobe Reader. Ist

[52] Verhaltungsregeln zu finden unter: http://www.melani.admin.ch/themen/00166/00172/index.html?lang=de (Stand: 20.08.2007).

[53] Siehe: http://scmagazine.com/us/news/article/657903/google-450000-websites-launching-drive-by-attacks/ (Stand: 20.08.2007).

das entsprechende Programm nicht auf dem neuesten Stand, droht beim Ansurfen einer präparierten Web-Seite eine Infektion mit Malware.

Im ersten Halbjahr 2007 machte beispielsweise eine per Grusskarte verteilte Malware von sich reden. Die E-Mails enthielten einen Link zu einer *IP-Adresse*. Beim Anklicken dieses Links wurde versucht, über Sicherheitslücken im Browser, ohne Aktion des Benutzers, Malware einzuschleusen. Dabei wurden je nach Browser verschiedene *Exploits* ausprobiert. Fand sich kein passender Exploit, wurde schliesslich noch versucht, den Benutzer zu einer manuellen Installation der Malware zu verleiten.

Gefährlich wird es ebenfalls, wenn Exploits durch Bilder verbreitet werden können. Schleust man beispielsweise eine präparierte Bilddatei auf den Server einer Firma, welche sich auf das platzieren von Werbebannern spezialisiert hat, so werden unmittelbar auch bekannte Web-Seiten zu Malwareschleudern. Daneben sind Web2.0-Plattformen wie YouTube oder MySpace ebenfalls beliebte Orte, um Malware zu platzieren. Die Besucher dieser Seiten benutzen nämlich zum Abspielen der Filme die oben erwähnten, oft von Sicherheitslücken betroffenen Medien-Player.

Massnahmen

Eine der wichtigsten Massnahmen liegt im fortlaufenden Updaten des Betriebssystems sowie sämtlicher darauf installierter Programme. Die Zeit zwischen Veröffentlichung des Patches und dessen Installation ist entscheidend. Aufgrund der Professionalität und Arbeitsteiligkeit der cyberkriminellen Szene dauert es inzwischen nur wenige Stunden, bis der erste Exploit auftaucht, der eine anlässlich des Patch-Releases bekannt gewordene Sicherheitslücke ausnutzt. Es zeigt sich jedoch, dass sich auch ältere Sicherheitslücken bei Kriminellen hoher Beliebtheit erfreuen. Erstmals wurde kürzlich ein Tool veröffentlicht, das automatisch untersucht, ob Betriebssystem und Programme auf dem neuesten Stand sind.[54] Aufgrund der sich im Umlauf befindenden *0-day-Exploits* bietet aber auch ein vollständig aufdatiertes System keinen 100-prozentigen Schutz.

Eine Möglichkeit zur Reduzierung eines Teils der Gefahren bietet das Ausschalten oder zumindest die Einschränkung von ActiveX im Internet Explorer oder Javascript in anderen Browsern. Viele Seiten benötigen diese Komponenten jedoch. Eine Anleitung, wie man ActiveX ausschliesslich für vertrauenswürdige Seiten zulässt, ist auf den MELANI-Seiten publiziert.[55]

Eine erhöhte Aufmerksamkeit und ein gewisses Gefahrenbewusstsein jedes einzelnen Computerbenutzers kann Schaden verhindern. Werden Unregelmässigkeiten festgestellt, sollte man misstrauisch werden. Dazu gehören beispielsweise das Abstürzen des Browsers oder das ungewollte Öffnen von Fenstern beim Besuch einer Seite. Erkennt man Solches, sollte man als Mitarbeitende den Computeradministrator über die betreffende Seite informieren. Eine Meldung an MELANI kann helfen, da die Seite analysiert und gegebenenfalls der Provider darüber informiert wird, so dass die Malware entfernt werden kann.

Eine weitere Möglichkeit zur Minderung der Gefahr durch Drive-by-Infektionen ist das Einrichten eines speziellen Surf-Accounts auf dem Computer. Dieser Surf-Account muss so eingerichtet werden, dass die (Administrations-)Rechte so weit als möglich eingeschränkt werden, um damit eine automatische Ausführung von Malware zu verhindern. Arbeitet man ohne Internet, wechselt man in ein Konto mit weniger eingeschränkten Rechten.

---

[54] Siehe: http://secunia.com/software_inspector (Stand: 20.08.2007); noch ist nur die Beta-Version erhältlich.
[55] Siehe: http://www.melani.admin.ch/themen/00166/00172/00176/index.html?lang=de (Stand: 20.08.2007).

Die Gefahr durch Drive-by-Infektionen wird in den Kapiteln 2.2 und 2.4 eingeschätzt; Beispiele sind im Kapitel 5.1 zu finden.

7 Aktivitäten / Informationen

7.1 Staatlich

Schweiz: MELANI wird weitergeführt

Am 24. Januar entschied der Bundesrat, die Melde- und Analysestelle Informationssicherung MELANI weiterzuführen. MELANI ist seit dem 1.Oktober 2004 operativ und hat die Aufgabe, die *kritischen Infrastrukturen* der Schweiz zu schützen, insbesondere dort, wo diese vom Funktionieren der Informations- und Kommunikationsinfrastrukturen abhängen.

Der Bundesrat entschied aufgrund einer Evaluation, welche durch die ETH Zürich durchgeführt worden war. Die Resultate der Evaluation beruhen auf Umfragen bei den Betreibern kritischer Infrastrukturen der Schweizer Wirtschaft, bei vergleichbaren Stellen im Ausland sowie bei Bundesstellen. Die Wirksamkeit und Zweckmässigkeit der Aktivitäten von MELANI wird als äusserst positiv bewertet.[56]

EU: Verstärkte Zusammenarbeit im Bereich Innere Sicherheit

Im ersten Halbjahr 2007 trieb die Europäische Union die verstärkte Zusammenarbeit im Bereich Innere Sicherheit weiter voran. Unter deutscher Ratspräsidentschaft wurden die operativen Befugnisse von Europol sowie der Informationsaustausch auf EU-Ebene gestärkt. Konkret sind folgende Punkte zu erwähnen:

Die operative Stärkung Europols ist mit dem Inkrafttreten der Änderungsprotokolle zum Europol-Übereinkommen Realität geworden. In Zukunft können Europol-Bedienstete an gemeinsamen Ermittlungsgruppen der Mitgliedstaaten teilnehmen. Um den Informationsaustausch zwischen Europol und den Mitgliedstaaten zu verbessern, sollen neben den bisherigen nationalen Zentralstellen weitere Behörden der Mitgliedstaaten einen direkten Zugriff auf das Europol-Informationssystem erhalten. Zudem können Experten aus Drittstaaten in einer Analysegruppe der Mitgliedstaaten bei Europol direkt mitarbeiten. Letzter Punkt ist vor allem mit Blick auf die Zusammenarbeit der EU und der USA im Bereich Terrorismusbekämpfung von Bedeutung. Die zusätzlich geplante Überführung des Europol-Übereinkommens in den

[56] Siehe http://www.isb.admin.ch/aktuell/medieninfo/00126/index.html?lang=de&msg-id=10361 (Stand: 10.8.07).

Rechtsrahmen der EU soll den Mandatsbereich von Europol auf alle Formen der grenzüberschreitenden schweren Kriminalität ausdehnen.[57]

Eine zentrale Rolle soll Europol auch bei der Überwachung des Internets spielen. Über ein bei Europol angesiedeltes Informationsportal sollen die Beobachtungen und Analysen der Mitgliedstaaten im Bereich terroristischer Aktivitäten im Internet zusammenlaufen. Dieses Überwachungsprojekt, welches unter dem Namen „Check the Web" läuft, ist Anfang Mai offiziell in Betrieb genommen worden. Des Weiteren werden im Rahmen von „Check the Web" regelmässige Expertentreffen durchgeführt.[58]

Um die Massnahmen zur Bekämpfung der Internetkriminalität besser zu koordinieren, möchte die Europäische Kommission einen kohärenten politischen Rahmen der EU entwickeln. Im Mai hat die Kommission dazu die Mitteilung „Eine allgemeine Politik zur Bekämpfung der Internetkriminalität" angenommen. Die Mitteilung betont unter anderem die Notwendigkeit eines verstärkten Dialogs zwischen dem öffentlichem Sektor und der Privatwirtschaft.[59]

USA: Signifikante IT-Sicherheitslücken beim Department of Homeland Security (DHS) versus Bestrebungen, die „Cyberüberlegenheit" militärisch zu sichern

Das Department of Homeland Security (DHS) ist in den USA unter anderem für die Cyber-Sicherheit verantwortlich. Erst im September 2006 setzte das DHS einen Cybersecurity-Verantwortlichen ein, um die USA besser gegen Cyberattacken zu sichern.[60] Das DHS wird jedoch für seine eigenen mangelhaften Sicherheitsvorkehrungen in der Informationssicherung und für Lücken in den Sicherheitskontrollen immer wieder kritisiert. Diesen Juni bemängelte die US-amerikanische Aufsichtsbehörde Government Accountability Office (GAO) in einem Bericht an das Repräsentantenhaus erneut die Informationssicherheit des DHS. Die GAO liess verlauten, dass Fortschritte stattgefunden hätten, jedoch „signifikante Schwachstellen" bestehen blieben, welche die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationssystemen des DHS bedrohten.[61]

Gleichzeitig wird die militärische Bedeutung des Cyberraums in den USA ernst genommen. Dies zeigt sich unter anderem in der Einrichtung einer neuen Cyberspace-Einheit durch die US Air Force. Dieses so genannte „Cyber Command" hat zum Ziel, den Cyberspace zu kontrollieren und die Kapazitäten der Kriegsführung im Cyberspace zu verbessern. Dahinter steht die Überzeugung, dass der Cyberspace und die Informationsüberlegenheit die Voraussetzung für effektive Operationen in allen Bereichen der Kriegsführung darstellen.[62]

---

[57] Siehe: http://www.bmi.bund.de/cln_012/nn_175818/Internet/Content/Nachrichten/Pressemitteilungen/2007/04/JI__Rat__Europol__DE.html; http://www.heise.de/newsticker/meldung/88599 (Stand: 10.8.07).

[58] http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2007/05/Check__the__web.html; http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=de (Kapitel 7.1) (Stand: 10.8.07).

[59] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:DE:PDF (Stand: 10.8.07).

[60] Siehe MELANI-Halbjahresbericht 2006/2, Kapitel 7: http://www.melani.admin.ch/dokumentation/00123/00124/01019/index.html?lang=de (Stand: 10.08.2007).

[61] Siehe http://www.gao.gov/new.items/d071003t.pdf; http://homeland.house.gov/hearings/index.asp?ID=65 (Stand: 10.8.07).

[62] Siehe www.af.mil; http://www.heise.de/newsticker/meldung/91131 (Stand: 10.8.07).

Verschiedene andere Staaten haben ebenfalls bereits militärische Kapazitäten im Cyberbereich geschaffen. Für die USA bieten insbesondere die Rüstungsbestrebungen Chinas im Cyberspace einen konkreten Motivationsgrund, auch in diesem Bereich die amerikanische Überlegenheit zu sichern.[63]

Für eine Einschätzung zu den rechtlichen Fragestellungen, welche Angriffe mit Cybermitteln mit sich bringen, sowie für Informationen zur Cyber-Attacke gegen Estland vom April 2006, siehe Kapitel 5.1.

7.2 Privat

Schweiz: Provider sperren Zugang zu Kinderpornographie-Seiten

In einem gemeinsamen Projekt der Schweizerischen Kriminalprävention (SKP), der ECPAT Switzerland von Kinderschutz Schweiz sowie der Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) wurden die Schweizer Internet Service Provider zur freiwilligen Blockierung von kommerziellen Kinderpornographie-Webseiten angefragt. Mittlerweile hat sich ein wichtiger Teil der Schweizer Internet-Provider bereit erklärt, bei dem Projekt mitzumachen, und einige Sperrungen sind bereits aktiv. Ziel ist es, den Zugang zu Kinderpornographie zu erschweren und die Kinderporno-Konsumenten durch sichtbare Intervention abzuschrecken.

Die Blockade-Aktion richtet sich gegen kommerzielle Anbieter von Kinderpornographie im Ausland. Die Liste mit den zu sperrenden Webseiten wird vom Bundesamt für Polizei festgelegt und laufend ergänzt. Die Adressen der einschlägigen Webseiten werden in einen Filter eingegeben. Wird eine dieser Seiten von einem Internet-User aufgerufen, dann wird er auf eine Hinweis-Seite umgeleitet. Ein Teil der Kinderporno-Adressen ist nach erfolgter rechtlicher Überprüfung von den skandinavischen Behörden übernommen worden, welche bereits mit ähnlichen Sperrfiltern arbeiten. Die restlichen Adressen stammen aus KOBIK-Ermittlungen.

Kinderpornografie ist auch im Jahr 2007 bisher der häufigste Grund für eine Meldung bei der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK. Die Blockade-Aktion soll einen wichtigen Beitrag zur Eindämmung der Nachfrage im Gebiet der Kinderpornografie leisten und somit potenzielle neue Opfer schützen.

[63] Siehe dazu die Einschätzung der militärischen Stärke Chinas durch das US-Verteidigungsministerium: http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf (Stand: 10.08.2007).

8 Gesetzliche Grundlagen

Neue Anti-Spam-Gesetzgebung in der Schweiz

Seit dem 1. April 2007 ist *Spam* in der Schweiz grundsätzlich verboten. Fernmeldetechnisch gesendete Massenwerbung ist nur noch unter bestimmten Bedingungen zulässig. Laut dem Bundesgesetz gegen den unlauteren Wettbewerb muss Massenwerbung, welche nicht in direktem Zusammenhang mit vom Empfänger angeforderten Inhalten steht, grundsätzlich folgende drei Bedingungen erfüllen:

1. Die Massenwerbung muss nach Einwilligung des Empfängers gesendet werden (Opt-in-Modell),

2. sie muss einen korrekten Absender enthalten und

3. die Massenwerbung muss einen Hinweis auf eine kostenlose Ablehnungsmöglichkeit enthalten.

Einzige Ausnahme zur Opt-in-Bestimmung ist die Angabe der Adresse bei einem Kauf unter dem Hinweis einer Ablehnungsmöglichkeit. Diese Adresse kann vom Verkäufer für eigene Werbung genutzt werden. Erfüllt die fernmeldetechnisch gesendete Massenwerbung diese Kriterien nicht, dann handelt es sich um Spam und damit um unlauteren Wettbewerb.

Handelt es sich bei der Absenderkennung (*IP-Adresse*) um einen Schweizer Fernmeldedienstanbieter, dann kann ihm der Versand von Spam mitgeteilt werden. Fernmeldedienstanbieter sind verpflichtet, eine Meldestelle einzurichten und – wenn sie davon Kenntnis haben – zu verhindern, dass ihre Kunden Spam senden oder weiterleiten.

Spam ist strafbar, wenn er vorsätzlich versendet wird. Das Tatbestandsmerkmal des Vorsatzes setzt voraus, dass dies wissentlich geschieht. Handelt es sich beim Spam also um vorsätzlich versendete unlautere Massenwerbung mit Bezug zur Schweiz, dann besteht die Möglichkeit, Anzeige gegen die werbende Firma oder den Absender zu erstatten. Man sollte dabei allerdings abwägen, ob ein allfälliges Strafverfahren im Verhältnis zum entstandenen Schaden sinnvoll erscheint. Spam ist ein Antragsdelikt und die Strafverfolgung ist Sache der Kantone.

Zur einfachen Analyse der Spamherkunft hat die Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) ein Spam-Analyse-Formular bereitgestellt.[64] Damit kann jeder herausfinden, ob der Spam von der Schweiz aus gesendet oder weitergeleitet wurde und wenn ja über welchen Fernmeldedienstanbieter (Internet-Provider). Für die Spam-Analyse wird die Kopfzeile des Spam-E-Mails benötigt. Eine genaue Anleitung, wie diese Kopfzeile herausgelesen werden kann, ist an derselben Stelle erhältlich.

Gegen Spam, der aus dem Ausland in die Schweiz versendet wird, greift die neue Gesetzgebung jedoch nicht. Da der grösste Teil der Spam-E-Mails aus dem Ausland stammt, dürfte sich im E-Mail-Postfach der Schweizer deshalb nur wenig ändern.[65]

[64] Siehe: http://www.cybercrime.ch/spamanalyse/spam.php#spam (Stand: 20.08.2007).

[65] http://www.bakom.admin.ch/dienstleistungen/info/00542/00886/index.html?lang=de (Stand: 20.08.2007).

Online-Durchsuchungen in Deutschland

Das Internet wird immer häufiger als Kommunikationsmittel eingesetzt. So auch durch Kriminelle oder Personen, welche die Sicherheit des Staates gefährden können. Zu diesem Thema sind sowohl in der Schweiz als auch im übrigen Europa heftige Diskussionen im Gang, wie weit der Staat in Sachen Überwachung von Internet und Computern gehen kann. Dabei muss jeweils unterschieden werden, ob es sich um eine Recherche ohne konkreten Verdacht handelt oder ob die Überwachung im Rahmen einer Strafverfolgung erfolgt.

In Deutschland entschied am 5. Februar 2007 der Bundesgerichtshof (BGH) in Karlsruhe, dass heimliche Online-Durchsuchungen durch die Polizei unzulässig seien, da keine klare Rechtsgrundlage vorhanden sei. Das Gericht erklärte, dass die Strafprozessordnung diese Fahndungsmethode nicht legitimiere. Online-Durchsuchungen können weder durch die Vorschriften zur Hausdurchsuchung gestützt, noch mit anderen Ermittlungsmassnahmen wie Telefonüberwachung oder Wohnraumüberwachung verglichen werden. Das Bundesinnenministerium hat angekündigt, auf eine Anpassung der gegenwärtigen Rechtsgrundlage hinzuarbeiten. Das Ministerium setzt im Zusammenhang mit der Bekämpfung des Terrorismus auf elektronische Fahndungsmethoden. Die Kontrolle des Internets und der Computersysteme wird als nötig erachtet, da Terroristen dieses moderne Kommunikationsmittel zunehmend nutzen.

Im Rahmen von Ermittlungsverfahren nutzen die deutschen Polizeibehörden auf Landesebene die Möglichkeit der Informationsbeschaffung mittels Eindringen in Computersysteme schon länger.

In der Schweiz sind Online-Durchsuchungen von Computersystemen ohne konkreten Tatverdacht momentan nicht zulässig. Das Eindringen in Computer unter strengen Auflagen ist jedoch im neuen Entwurf zum Bundesgesetz zur Wahrung der inneren Sicherheit (BWIS) enthalten. Allerdings steht eine Beratung dieses Gesetzesentwurfs in den Räten erst an. Der Einsatz von Spionagesoftware im Rahmen der Strafverfolgung kann jedoch erlaubt sein. Das Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sowie verschiedene Strafprozessordnungen können dafür als Rechtsgrundlage dienen.

Eine Einschätzung der Nutzung des Internets durch Terroristen ist in mehreren bisherigen MELANI-Halbjahresberichten thematisiert worden (Ausgaben 2006/2, 2006/1 und v.a. 2005/2, jeweils Kapitel 5.4).

9 Statistik

Sättigung bei Internetzugängen in der Schweiz

Das Bundesamt für Statistik hat im ersten Halbjahr 2007 eine Studie über die Internetnutzung in den Haushalten der Schweiz veröffentlicht. Die Ergebnisse der Erhebung von 2004 zeigen, dass rund 71% der Schweizer Haushalte mit einem Computer ausgestattet sind. Davon haben 61% einen Zugang zum Internet. Die Schweiz steht im internationalen Vergleich an fünfter Stelle. Laut Studie nimmt der Internet-Zugang von zu Hause aus weiter zu, jedoch deutlich langsamer als Ende der neunziger Jahre oder zu Beginn des 21. Jahrhunderts. Ein Fünftel der Schweizer Haushalte wollen überhaupt keinen Internet-

Anschluss oder sehen keinen Nutzen darin. Deshalb ist in nächster Zeit mit einer Sättigung der Neuanschlüsse zu rechnen. Andere Gründe für die Nichtnutzung eines Internetanschlusses von zu Hause aus sind der Mangel an einschlägigen Kompetenzen, die Kosten sowie die Möglichkeit eines alternativen Zugangs zum Internet.[66]

Die Angst vor Datensicherheitsproblemen und der Schutz der Privatsphäre spielen nur eine geringe Rolle in den Abwägungen zu einem Internetanschluss zu Hause, denn jedes dieser Argumente wird von weniger als 1% der Haushalte angeführt.

Schweizer Firmen praktisch flächendeckend elektronisch vernetzt

Informatik und Internet spielen in den Firmen in der Schweiz eine immer grössere Rolle. Insbesondere kleine und mittlere Betriebe (KMU) nutzen vermehrt qualifizierte Online-Dienstleistungen und sind wie Grossfirmen auf hohem Niveau vernetzt. Von den elektronischen Angeboten der Behörden sind bei den Unternehmen die Internetauftritte der Kantone am bekanntesten, wie eine repräsentative Studie des Forschungsinstituts gfs.bern ergeben hat. Insgesamt sind 1050 Firmen vom 5. bis 25. Februar 2007 im Auftrag des Staatssekretariates für Wirtschaft SECO und der Bundeskanzlei befragt worden.[67]

91 Prozent der Befragten in Firmen ab 10 Mitarbeitenden verfügen direkt am Arbeitsplatz über einen Internetzugang. In Firmen mit weniger als 10 Angestellten arbeiten 63% täglich mit dem Internet, in grösseren Unternehmen mindestens 71% der Mitarbeitenden. Als sehr bis eher wichtig beurteilen 72% ein E-Mail-Konto für alle Mitarbeitenden, und 76% halten mobile Dienste wie Mobiltelefon, Smartphones oder eine elektronische Agenda (PDA) für sehr bis eher wichtig.

Der Schutz der Informationsinfrastruktur ist auch bei den KMUs nicht mehr zu vernachlässigen und wird zunehmend wichtiger. MELANI hat eine Studie in Auftrag gegeben, welche die Informationssicherheit in Schweizer Unternehmen beleuchtet. Der Ausfall von Informatikmitteln bei einer Firma über mehrere Tage kann bereits existenzbedrohend sein.[68]

[66] http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.Document.87094.pdf (Stand: 20.08.2007).
[67] http://www.seco.admin.ch/aktuell/00277/01164/01980/index.html?lang=de&msg-id=12087 (Stand: 20.08.2007).
[68] http://www.melani.admin.ch/dokumentation/00123/00125/index.html?lang=de (Stand: 20.08.2007).

10 Glossar

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

0-day-Exploit	*Exploit*, der am selben Tag erscheint, an dem die *Sicherheitslücke* öffentlich bekannt wird.
Bot / Malicious Bot	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Botnetz	Eine Ansammlung von Computern, die mit Malicious *Bots* infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.
DDoS-Attacke	Distributed-Denial-of-Service Attacke Eine *DoS-Attacke*, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Defacement	Verunstaltung von Webseiten.
DNS	Domain Name System Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von *IP-Adressen* Namen verwenden können (z.B. www.melani.admin.ch).
DoS-Attacke	Denial-of-Service Attacke Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Drive-by-Infektion	Infektion eines Computers mit *Malware* allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von *Exploits* für vom Besucher noch nicht geschlossene *Sicherheitslücken*.
Exploit-Code	(kurz: Exploit) Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-

	Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Keylogger	Geräte oder Programme, die zwischen den Rechner und die Tastatur geschaltet werden, um Tastatureingaben aufzuzeichnen.
Kritische (nationale) Infrastrukturen	Infrastruktur oder Teil der Wirtschaft, deren Ausfall oder Beschädigung massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt einer Nation hat. In der Schweiz sind folgende Infrastrukturen als kritisch definiert worden: Energie- und Wasserversorgung, Notfall- und Rettungswesen, Telekommunikation, Transport und Verkehr, Banken und Versicherungen, Regierung und öffentliche Verwaltungen. Im Informationszeitalter hängt ihr Funktionieren zunehmend von Informations- und Kommunikationssystemen ab. Solche Systeme nennt man kritische Informationsinfrastrukturen.
Malware	Setzt sich aus den englischen Begriffen "Malicious" und "Software" zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). (Auch: Malicious Code).
Man-in-the-Middle-Attacke	Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt.
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.
Plugin	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat *Plugins* für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.

Token	Hardware-Komponente, die einen Authentifikationsfaktor (siehe *Zwei-Faktor-Authentifizierung*) ausgibt (z.B. SmartCard, USB-Token, SecureID etc.).
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.
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.)