Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

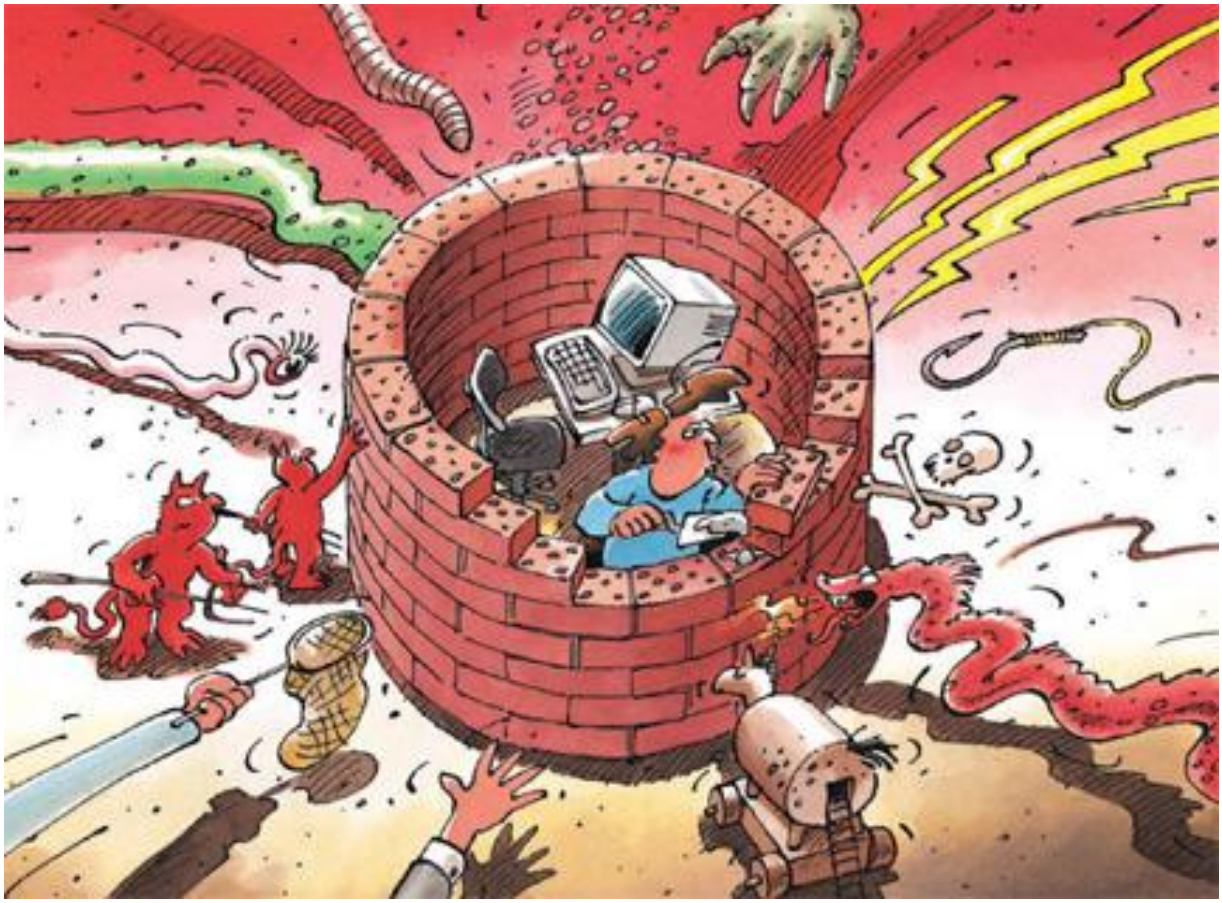
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2012/I (Januar – Juni)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2012/I

- **Massenweise Passwörter und Kreditkartendaten gehackt**
  Das erste Halbjahr 2012 war wiederum geprägt durch verschiedene grosse Angriffe auf bekannte Firmen, bei denen Kundendaten, meist Login und Passwort aber auch Kreditkartendaten, gestohlen wurden. Den zum Teil sehr spektakulären Fällen, stehen zahlreiche Angriffe auf kleinere Firmen und deren Daten gegenüber, die tagtäglich passieren und in den Medien nicht thematisiert werden. Laut einer Studie von Verizon richten sich mehr als 75% der Angriffe gegen KMUs mit einer Mitarbeiterzahl von unter 1000.
  ► Aktuelle Lage International: Kapitel 4.5
  ► Tendenzen / Ausblick: Kapitel 5.3

  Phishing in verschiedenen Varianten
  In der Schweiz werden tagtäglich Phishing-Angriffe beobachtet. In den meisten Fällen verleiten diese E-Mails die Kunden jeweils dazu, die Kreditkartendaten anzugeben. Wie ein aktueller Fall zeigt, durchforsten die Betrüger automatisch Schweizer Gästebücher und Foren, um an gültige E-Mail Adressen zu kommen, an die anschliessend die Phishing E-Mails gesendet werden. Aber auch Voice Phishing–Angriffe, die den Opfern vorgaukeln, dass es sich um IKT-Support Anrufe handle und man Zugriff auf den Computer gewähren solle, werden seit einem Jahr in der Schweiz häufig beobachtet. Erlangen Kriminelle durch Phishing die E-Mail Logindaten einer Person, verwenden sie diese, um gefälschte Hilferufe an alle Kontakte im kompromittierten E-Mail Adressbuch zu senden.

  All diese Ereignisse verlangen vermehrt eine grosse Sensibilität der Firmen in der Kundenkommunikation. Beachtet man seitens der Firmenkommunikation nicht einige Grundregeln, werden Newsletter von den Kunden schnell einmal als vermeintliche Phishing-E-Mail eingestuft.
  ► Aktuelle Lage Schweiz: Kapitel 3.2, Kapitel 3.4, Kapitel 3.5, Kapitel 3.6
  ► Tendenzen / Ausblick: Kapitel 5.4

  Cyberkonflikt in Nahost
  Ende Mai wurde das komplexe Schadprogramm «Flame» entdeckt, welches benutzt wurde, um Organisationen in mehreren Ländern im nahen Osten anzugreifen und auszuspionieren. Die technische Analyse durch Sicherheitsunternehmen zeigte verschiedene Gemeinsamkeiten von «Flame» «Stuxnet» und «Duqu» auf.

  Mit den offen ausgetragenen Konflikten seit Beginn des arabischen Frühlings nimmt auch der aggressive und offensive Einsatz der IKT-Mittel und des Internets zu. Regelmässig werden Fälle bekannt, in denen Webseiten zum Erliegen gebracht, staatliche oder private Dokumente entwendet und veröffentlicht oder Schadsoftware zur Sabotage eingesetzt wurde.
  ► Aktuelle Lage International: Kapitel 4.1, Kapitel 4.2
  ► Tendenzen / Ausblick: Kapitel 5.2
- **E-Voting Zwischenfälle**

  Es ist klar, dass im Internetzeitalter die Bürger vom Staat verlangen, auch Abstimmungen und Wahlen elektronisch anzubieten. Trotzdem gibt es einige grundlegenden Unterschiede zwischen E-Voting und anderen E-Services wie beispielsweise das E-Banking.
  ► Aktuelle Lage Schweiz: Kapitel 3.7
  ► Tendenzen / Ausblick: Kapitel 5.5
- **Nationale Strategie zum Schutz vor Cyberrisiken**
  Am 27.Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken gutgeheissen.
  ► Aktuelle Lage Schweiz: Kapitel 3.9

2 Einleitung

Der fünfzehnte Halbjahresbericht (Januar – Juni 2012) 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 2012 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 IKT-Pannen in Wirtschaft und Verwaltung

Pannen ausgelöst durch Fehlmanipulationen oder durch technisches Versagen sind eine der häufigsten Ursachen für Ausfälle bei Informationsinfrastrukturen. Kritische Systeme sind in der Regel redundant ausgelegt, was einen Ausfall verhindern soll. Wie einige Ereignisse in der Vergangenheit gezeigt haben, greift die Redundanz bei Hardwareausfällen in der Regel gut, bei Softwarepannen aber nur bedingt, da auf redundanten Systemen in etwa die gleiche Software und Konfiguration läuft, ist es möglich, dass bei einem Umschalten auf das Backup-System die gleichen Softwareprobleme wie auf dem Hauptsystem auftauchen und dieses System ebenfalls zum Absturz gebracht wird.[1] Auch im ersten Halbjahr 2012 haben einige Pannen in der Schweiz für Aufsehen gesorgt:

Informatikpanne beim Kanton Bern

Am 8. Mai 2012 fiel im Netzwerk der Verwaltung des Kantons Bern eine zentrale Komponente aus, welche für mehr als 24 Stunden einige wichtige Systeme lahmlegte und dafür sorgte, dass diverse Dienstleistungen nicht mehr verfügbar waren. So musste beispielsweise das Strassenverkehrsamt sämtliche Dienstleistungen einstellen. Betroffen war auch das Onlineportal (TaxMe), auf welchem man Zugriff auf die Steuererklärung hat und diese elektronisch ausfüllen kann, sowie das Grundstückdaten-Informationssystem (GRUDIS), das Geoportal, die Daten zu den Wasserständen von Flüssen und Seen oder die amtliche Gesetzessammlung. Ein Datenverlust konnte jedoch verhindert werden.

Die Störung wurde durch einen Softwarefehler des Betriebssystems (Microcode) bei einem zentralen Speichersystems verursacht. Dieser Fehler hat unter anderem auch die vorhandenen Redundanzen des Datenspeichers, wie zum Beispiel doppelte Systemkomponenten und die Datenspiegelung in ein entferntes Rechenzentrum, ausser Kraft gesetzt.[2]

Coop Filialen ohne Kassensysteme

Am 4. April 2012 hatten sämtliche Deutschschweizer Coop-Filialen mit Problemen bei den Kassensystemen zu kämpfen. Während zwei Stunden konnten diese nicht verwendet werden. Als Folge blieben die Geschäfte geschlossen oder es wurden Gratis-Gipfeli an die wartende Kundschaft verteilt. Grund der Panne war ein fehlerhaftes Software-Update, welches über Nacht eingespielt wurde und bei den nachfolgenden Tests nicht aufgefallen war.

Verspätete Handelsaufnahme der Schweizer Börse

Am Freitag dem 13. Januar 2012 konnte die Schweizer Börse den Handel nicht zu gewohnter Zeit aufnehmen. Während der Fehler noch vor dem gewohnten Zeitpunkt des Handels-

---

1 MELANI Halbjahresbericht 2009/1, Kapitel 4.6: http://www.melani.admin.ch/dokumentation/00123/00124/01093/index.html?lang=de (Stand: 31. August 2012).

2 http://www.be.ch/portal/de/index/mediencenter/medienmitteilungen.meldungNeu.html/portal/de/meldungen/mm/2012/05/20120509_1347_alle_dienstleistungensindwiederverfuegbar (Stand: 31. August 2012).

beginns behoben werden konnte, nahmen die Wiederanlaufverfahren aller am Handel beteiligten Parteien zusätzliche Zeit in Anspruch, so dass der Handel erst um 12 Uhr eröffnet werden konnte. Der Grund der Störung konnte zwar eruiert werden, die Betreiberin der Schweizer Börse, die SIX, wollte diesen aber nicht öffentlich kommunizieren. Gemäss Angaben der SIX sei nur eine Handvoll Börsenteilnehmer betroffen gewesen. Aus Gründen der Marktintegrität und Fairness habe man sich aber dazu entschlossen, den ganzen Handel auszusetzen

Dies war nicht das erste Mal, dass wegen technischen Problemen der Handel ausgesetzt werden musste. Am 12. November 2009 musste die Börse bereits um 15 Uhr geschlossen und der Handel gestoppt werden.[3] Trotz diesen Vorfällen ist der Ausfall einer Börse als extrem seltenes Ereignis zu verzeichnen.

Diese Beispiele zeigen deutlich, wie abhängig die Wirtschaft – aber auch die Verwaltung – von einem störungsfreien Betrieb der IKT ist. Schon kleine Ausfälle können grosse finanzielle Schäden verursachen. Es ist wichtig, eine solide IKT-Infrastruktur zu haben und vor allem auch in der Lage zu sein, Störungen möglichst schnell zu beheben. Laut einer schweizweit durchgeführten Studie von 2005 der ETH Zürich könnte ein landesweiter Ausfall des gesamten Internets während einer Woche der Wirtschaft Verluste in der Höhe von 5,83 Milliarden Franken verursachen.[4] Da Ausfälle nie ausgeschlossen werden können, ist eine genaue Kontinuitätsplanung gerade für solche Dienstleistungen unabdingbar.

3.2 E-Mail Kontoübernahme – Betrüger reagieren auf Massnahmen der E-Mail-Provider

Bereits seit mehr als drei Jahren werden Fälle beobachtet, bei welchen mit gestohlenen Zugangsdaten auf das E-Mail-Konto eines Opfers zugegriffen wird. Die Betrüger schauen sich danach im E-Mail Konto um und schreiben anschliessend alle oder gezielt Kontakte aus dem Adressbuch an. Meist handelt es sich bei diesen E-Mails um gefälschte Hilferufe. worin vorgegeben wird, der Sender sitze irgendwo im Ausland fest und ihm seien alles Geld sowie der Pass gestohlen worden. Schliesslich wird um die sofortige Überweisung von Geld gebeten:

«Ich hoffe, dass Du dies zeitig bekommst. Entschuldige bitte, ich habe Dich nicht über meine Reise nach Spanien informiert. Ich bin zur Zeit in Madrid und habe einige Probleme, weil ich mein Geldbeutel verloren habe.»

Bild 1: Text eines E-Mails von Betrügern, welches an alle Kontakte eines kompromittierten E-Mail Kontos versendet wurde.

Dass auch Politiker vor solchen Angriffen nicht verschont werden, zeigt der Fall der Könizer Politikerin Verena Koshy aus dem ersten Halbjahr 2012. Obschon bei einer Person, deren E-Mail Konto gehackt worden ist, kein direkter finanzieller Schaden entsteht, ist ein solcher Vorfall immer ärgerlich und mit einem Riesenaufwand verbunden - vor allem bei Leuten, die breit vernetzt sind und viele Kontakte gespeichert haben.. Entsprechend viele Adressaten haben somit auch den falschen Hilferuf von Frau Koshy erhalten. Wird ein solcher Vorfall bemerkt, sollten die Adressaten möglichst schnell informiert und gewarnt werden und man sollte sich sofort an den *Provider* wenden, der dann Massnahmen ergreift, um dem Opfer

[3] http://www.tagesanzeiger.ch/wirtschaft/unternehmen-und-konjunktur/Technische-Probleme-legen-Boerse-lahm/story/30392767 (Stand: 31. August 2012).

[4] http://www.ethz.ch (Stand: 31. August 2012).

wieder Zugang zu seinem Konto zu geben. Die Provider reagieren in der Regel zwischen 24 und 48 Stunden und die Betrüger haben anschliessend keine Kontrolle mehr über das gehackte Konto.

Leider haben sich auch die Betrüger darauf eingestellt, dass die Sperrung des Kontos und die Warnungen an die Empfänger ihre Erfolgschancen schmälern. Dementsprechend haben sie in den letzten Monaten Gegenmassnahmen getroffen und ihre Vorgehensweise angepasst: So stehlen sie zwar immer noch die Kontaktdaten im gehackten E-Mail Konto, ändern dann aber die Absender-Adresse in einem kleinen Detail - aus Meier wird beispielsweise Neier - so dass es den Empfängern nicht auffällt. Diese Adresse hat der Angreifer zuvor speziell für den Betrug gelöst. Im Gegensatz zum gehackten Konto hat er darauf auch nach den ergriffenen Massnahmen noch Zugriff und kann mit den Opfern so lange kommunizieren, bis der Betrug abgeschlossen ist.

Neu ist auch, dass die Betrüger anschliessend sämtliche Kontakte und alle E-Mail Nachrichten in den gehackten Konten löschen. Dies soll verhindern, dass der eigentliche Besitzer des Kontos nach der Wiedererlangung des Zugriffs sämtliche Kontakte warnen kann. Dieser Umstand ist für das Opfer mit grossem Ärger verbunden, da in den meisten Fällen kein *Backup* der Kontaktliste und der E-Mail Nachrichten vorhanden ist. In manchen Fällen kann der Provider die Daten noch retten, aber in vielen Fällen sind die Daten für immer verloren.

Nachfolgend einige Tipps, um den Schaden im Ereignisfall möglichst klein zu halten.

1. *Backup* der Kontakte erstellen, damit im Ereignisfall auf eine alternative E-Mail-Adresse ausgewichen werden kann. So können die Kontakte so rasch wie möglich vor den betrügerischen E-Mails gewarnt werden.
2. Sorgfältige Wahl des E-Mail Providers, besonders wenn die E-Mail geschäftlich verwendet wird.
3. Im Ereignisfall sofort versuchen, wieder die Kontrolle über das Konto zu erlangen. In den meisten Fällen wird die alternative E-Mail Adresse jedoch auch verändert: Ist dies nicht der Fall kann ein Ersatzpasswort an diese E-Mail-Adresse gesendet werden. Wurde jedoch auch die alternative Adresse verändert, muss ein *Recovery Prozess* gestartet werden. Hierzu stellen die meisten E-Mail Provider ein *Recovery*-Formular zur Verfügung. Nachfolgend eine nicht abschliessende Auswahl der gängigsten E-Mail-Anbieter:

Google	https://www.google.com/accounts/recovery/
Hotmail/ Live	https://account.live.com/resetpassword.aspx
Yahoo	https://edit.europe.yahoo.com/forgotroot
GMX	http://www.gmx.com/forgotPassword.html

3.3 Sperrtrojaner auf dem Vormarsch

Über *Sperrtrojaner* hatt MELANI schon im letzten Halbjahresbericht[5] berichtet. Dabei handelt es sich um so genannte *Ransomware* (erpresserische *Schadsoftware*), die den Computer

[5] MELANI Halbjahresbericht 2011/2, Kapitel 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012).

blockiert und anschliessend ein Lösegeld fordert. Zuerst tauchte diese Form im Frühjahr 2011 in Deutschland auf und war mit dem Logo des deutschen Bundeskriminalamts (BKA) versehen, was der *Schadsoftware* auch den Übernahmen BKA-Trojaner einbrachte.[6] Dieser eher unglücklich gewählt Name hat mit dem *Strafverfolgungstrojaner* der Deutschen Bundeskriminalpolizei natürlich nichts zu tun.

Die ersten Schweizer Versionen dieses Trojaners wurden im letzten Herbst im Namen des Eidgenössischen Justiz- und Polizei Departementes (EJPD) versendet. Anfang März 2012 folgte dann ein weiterer Typ *Sperrtrojaner,* welcher vorgibt, von der Genossenschaft der Urheber und Verleger von Musik SUISA, welche als Verwertungsgesellschaft für Urheberrechte in der Schweiz fungiert, zu stammen.[7] Seit Juni 2012 ist nun auch eine Version im Namen des (so nicht existenten) «Cyber Crime Investigation Department» im Umlauf. Hier wird sogar die Webcam angeschaltet und das Bild auf dem gesperrten Computer eingeblendet, um das Opfer zusätzlich einzuschüchtern.

Gefordert wurde die Bezahlung einer Busse meist über den Onlinebezahldienst Paysafe.

Paysafecard, die Anbieterin des durch die Betrüger in diesen Fällen verwendeten Prepaid-Zahlungsmittels, hat auf diesen Missbrauch reagiert und mittlerweile eine diesbezügliche Warnung auf den Paysafe Karten aufgedruckt.

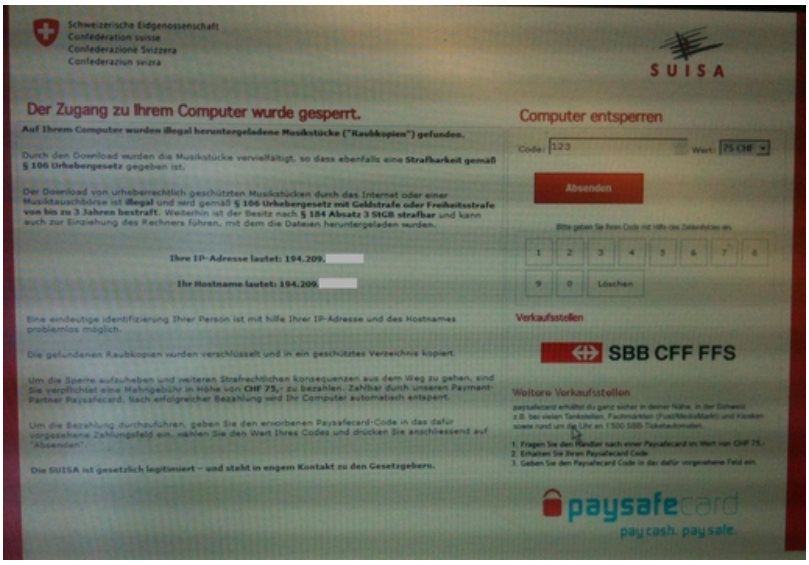


Bild 2: Sperrtrojaner mit SUISA Logo

[6] Siehe http://www.bka-trojaner.de – Auf dieser Webseite werden Angaben zu den verschiedenen Versionen bereitgestellt (Stand: 31. August 2012).

[7] http://www.suisa.ch (Stand: 31. August 2012).

Bild 3: Sperrtrojaner mit Logo der Schweizerischen Eidgenossenschaft

Seit dem Auftauchen der ersten Fälle in der Schweiz werden der Melde- und Analysestelle Informationssicherung MELANI regelmässig Fälle von gesperrten Computern gemeldet. Die Infektion findet meist über Videoportale statt oder über Seiten, welche multimedialen Inhalt verbreiten. Es ist anzunehmen, dass die Infektionen beispielsweise über verseuchte Videodateien oder kompromittierte Videoplayer durchgeführt werden.

Eine Infektion und Sperrung das Computers bringt in jedem Fall Unannehmlichkeiten mit sich insbesondere dann, wenn es sich um Geschäftscomputer von kleinen Unternehmen handelt, die zwingend benutzt werden müssen und nicht einfach ausgetauscht werden können. MELANI sind solche Fälle bekannt.

MELANI sind auch Fälle bekannt, bei denen die Sperre auch einfach umgangen werden konnte: Wird das System heruntergefahren und ohne Internetverbindung wieder gestartet, ist es in einzelnen Fällen möglich, die Sperrung zu umgehen.

3.4 Voice Phishing (Vishing)

Voice Phishing war in der Schweiz lange Zeit nicht existent, doch seit Sommer 2011 wurden nun vermehrt Fälle auch in der Schweiz registriert. Im letzten Halbjahresbericht ging MELANI auf diese Anrufe detailliert ein.[8] Dabei gehen die Betrüger momentan fast immer gleich vor: Man erhält ein Telefon von einer angeblichen Computer Support Firma (meist Microsoft), welche dem Opfer vorgaukelt, dass der Computer verdächtige Nachrichten aussende. Um dies zu «beweisen», werden die Angerufenen typischerweise angeleitet, auf ihrem Computer den *Event-Viewer* (Ereignisanzeige) aufzurufen, mit welchem interne Meldungen des Betriebssystems aufgezeigt werden können. Dazu muss man wissen, dass auch ein einwandfrei funktionierendes System gelegentlich Fehlermeldungen produziert. Je nach Alter und Konfiguration des Computers kann die Liste der Fehlermeldungen im Event-Viewer sehr lange sein, ohne dass das System ein grundsätzliches Problem hat. Das Aufrufen-Lassen dieses Programms wird von den «Support»-Anrufern typischerweise benutzt, um den Opfern eine glaubwürdige Kulisse zu präsentieren respektive Angst zu machen. Ziel der Betrüger ist, die angerufene Person dadurch zu überzeugen, ein Fernzugriffs-Programm (*Remote Access Tool*) herunterzuladen und ihnen dann Fern-Zugriff auf den Computer zu erlauben. Die Betrüger erlangen auf diese Weise vollen Zugriff auf das System und damit dieselben Möglich-

[8] MELANI Halbjahresbericht 2011/2, Kapitel 3.1: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012).

keiten, den Computer zu manipulieren, wie wenn sie selbst direkt davor sitzen würden. Schliesslich wird meistens versucht, dem Opfer eine Softwarelizenz oder eine Dienstleistung («Systemreinigung») zu verkaufen, wozu dann nach Kreditkarteninformationen gefragt wird.

Hat man auf einen solchen Telefonanruf reagiert und die Kreditkartendaten den Betrügern angegeben ist es vor allem wichtig, die Kreditkarte umgehend zu sperren.

Was die Betrüger auf dem Computer gemacht oder installiert haben, ist jeweils schwierig zu beurteilen. Wenn dem Betrüger via ein *Remote Access Tool* Zugriff gewährt wurde, hatte dieser dieselben Möglichkeiten, den Computer zu manipulieren, wie wenn er selbst direkt davor gesessen hätte (Kopieren/Manipulieren/Löschen von Daten, Installation von Programmen. etc., Er könnte so auch eine «*Hintertür*» einrichten, um später wieder auf das System Zugreifen zu können,).

Nach einem solchen Ereignis ist es deshalb empfehlenswert, den Computer von einer Fachperson untersuchen zu lassen. Dies garantiert jedoch nicht, dass eine allfällige *Schadsoftware* oder anderweitige Manipulation im System gefunden wird. Die sicherste Methode besteht darin, die Festplatte des Computers komplett zu löschen und das Betriebssystem neu zu installieren. Hierbei muss allerdings beachtet werden, die persönlichen Daten jeweils vorab zu sichern, damit diese nicht verloren gehen.

Zudem sollten nach der Säuberung/Neuinstallation des Computers (oder von einem anderen Computer aus) bei allen Internet-Diensten, welche zuvor damit genutzt worden sind, die Passwörter geändert werden.

Vishing im Namen der Swisscom

Im Juli 2012 wurde eine E-Mail im Namen der Swisscom in Umlauf gesetzt. In schlechtem Deutsch aber besserem Französisch wurden die Opfer darauf hingewiesen, dass etwas mit ihrem Konto nicht stimme, respektive dass ihr Konto «gehemmt» (sprich: blockiert) worden sei. Im Gegensatz zu den klassischen *Phishing*-E-Mails sollte nicht Username und Passwort angegeben, sondern für weitere Informationen auf eine Telefonnummer angerufen werden. Die angegebene Nummer mit der Vorwahl 0088 gehört einem Satellitentelefonbetreiber. Hohe Kosten sind also bei einem Anruf garantiert. Ob ein Opfer nach einem Anruf ebenfalls nach Benutzername und Passwort gefragt wurde, konnte nicht eruiert werden. Für Swisscom Email Accounts wurden diese Phishing Emails frühzeitig blockiert.

Gesendet: Dienstag, 10. Juli 2012 01:19

Betreff: Sie haben 1 neue Nachricht / Vous avez 1 nouveau message

Ihr Konto ist gehemmt worden.

Für mehr Informationen erreichen Sie uns unter der Telefonnummer:
00881835211648 oder 00881835211650

Votre compte a été suspendu.

Pour de plus amples informations, vous pouvez appeler le numéro de téléphone:
00881835211648 ou 00881835211650

Bild 4: E-Mails, wie Sie im Juli 2012 im Namen von Swisscom versendet wurden

3.5 Wie Phisher an E-Mail Adressen kommen

Es gibt verschiedene Möglichkeiten, wie eine E-Mail Adresse in eine Spamdatenbank gelangen kann. Eine dieser Möglichkeiten ist das automatische Durchforsten des Internets nach gültigen E-Mail-Adressen, die auf Websites (beispielsweise auf Foren oder Gästebüchern, usw.) publiziert sind. Ist die E-Mail Adresse einmal in einer solchen Spam Datenbank gelandet, wird diese durch die Kriminellen mehrfach verwendet und oft auch an andere Betrüger weiterverkauft.

Betreibern von Foren- und Gästebüchern kommt somit eine wichtige Bedeutung zu, welche oft unterschätzt und auch vernachlässigt wird,in den meisten Gästebüchern werden die E-Mail Adressen immer noch im Klartext angezeigt und sind durch die Kriminellen mit Hilfe der entsprechenden Tools sehr einfach zu extrahieren.

Dass diese Quellen auch tatsächlich genutzt werden, zeigt eine Analyse der Empfänger E-Mail Adressen einer aktuellen Phishing-E-Mail Welle. In diesem Fall konnten die durch die Betrüger verwendeten E-Mail Adressen Einträgen in Gästebüchern auf Schweizer Websites zugeordnet werden. Einige Gästebücher erwiesen sich als wahre Goldgruben für Adresssammler. Auf der Website eines Schweizer Musikers findet man im Gästebuch beispielsweise über 2‘700 im Klartext publizierte E-Mail-Adressen. Für die Betrüger hat dies zusätzlich den grossen Vorteil, dass diese Mail-Adressen mit erhöhter Wahrscheinlichkeit Schweizer Bürgerinnen und Bürgern oder zumindest deutschsprachigen Personen gehören. Mit dieser Information können die Phishing E-Mails zielgerichteter verfasst und damit die Wahrscheinlichkeit, dass der Angriff funktioniert, erhöht werden.

MELANI empfiehlt folgende Massnahmen im Umgang mit E-Mail Adressen auf Gästebüchern und Foren:

Auf Seiten Webadministrator

- In vielen Fällen ist eine Publikation der E-Mail Adresse nicht nötig und dient alleine als Authentifizierungsmerkmal für den Webseitenadministrator. Hier ist die Publikation der E-Mail Adresse zu unterlassen.

- Wenn eine Publikation zwecks Kontaktaufnahme notwendig ist, verzichten Sie auf die Publikation von E-Mail Adressen im Klartext. Es gibt mehrere Möglichkeiten, beispielsweise mit Hilfe von JavaScript, die automatisierte Auslesung der E-Mail Adresse zu verhindern.

- Die effizienteste Art ist es, die Adresse nicht zu publizieren und an dessen Stelle ein (gut gesichertes) Webformular zur Verfügung zu stellen, welches die Kontaktaufnahme ermöglicht.

Auf Seiten Benutzer

- Geben Sie Ihre E-Mail-Adresse nur an so wenige Personen wie notwendig weiter und verwenden Sie diese ausschliesslich für wichtige Korrespondenz.

3.6 Phishing-E-Mails – Angebliche Steuerrückerstattung der Eidgenössischen Steuerverwaltung

Mit verschiedenen Tricks versuchen Angreifer das Leben der Sicherheitsbehörden, die *Phishing* Angriffe verhindern, so schwer wie möglich zu machen. MELANI hat bereits im letzten

Halbjahresbericht darüber berichtet.[9] Eine weitere neue Variante ist die nachfolgend beschriebene Vorgehensweise.

Am Montag, dem 4. Juni 2012, versendeten Betrüger im Namen der Eidgenössischen Steuerverwaltung (ESTV) *Phishing*-E-Mails. Darin wurde dem Empfänger eine Steuerrückerstattung in Aussicht gestellt. An der E-Mail angehängt war ein *HTML*-Formular. Wurde dieses geöffnet, musste man Personalien und Kreditkartendaten eingeben. Im Gegensatz zu klassischen *Phishing* E-Mails, welche den Benutzer dazu auffordern auf einen Link zu klicken, um auf der anschliessend sich öffnenden Phishingseite persönliche und Kreditkartendaten einzugeben, war in diesem Fall die *HTML*-Seite gerade der E-Mail als *Anhang* angehängt. Beim Öffnen wird die *HTML*-Seite lokal auf dem Computer des Empfängers aufgebaut. Werden die Formularfelder ausgefüllt und auf den Knopf «Weiter» gedrückt, werden die Daten «direkt» an den Angreifer versendet.

Für den Angreifer hat dies den Vorteil, dass er keinen gehackten oder speziell für diese Zwecke aufgesetzten Webserver benötigt, worauf er sonst die Phishingseite platziert und die natürlich durch die Sicherheitsbehörden respektive den Hosting-Provider deaktiviert werden kann. Die ganze Information der Phishingwebseite befindet sich im *Anhang*. Das Einzige, was noch benötigt wird, ist ein sogenannter *PHP-Mailer*, welche sich zu tausenden ungeschützt im Netz befinden und worüber man sich Daten an beliebige E-Mail-Adressen senden lassen kann. Es ist klar, dass sich solche Mailer auch schlechter sperren respektive sichern lassen.

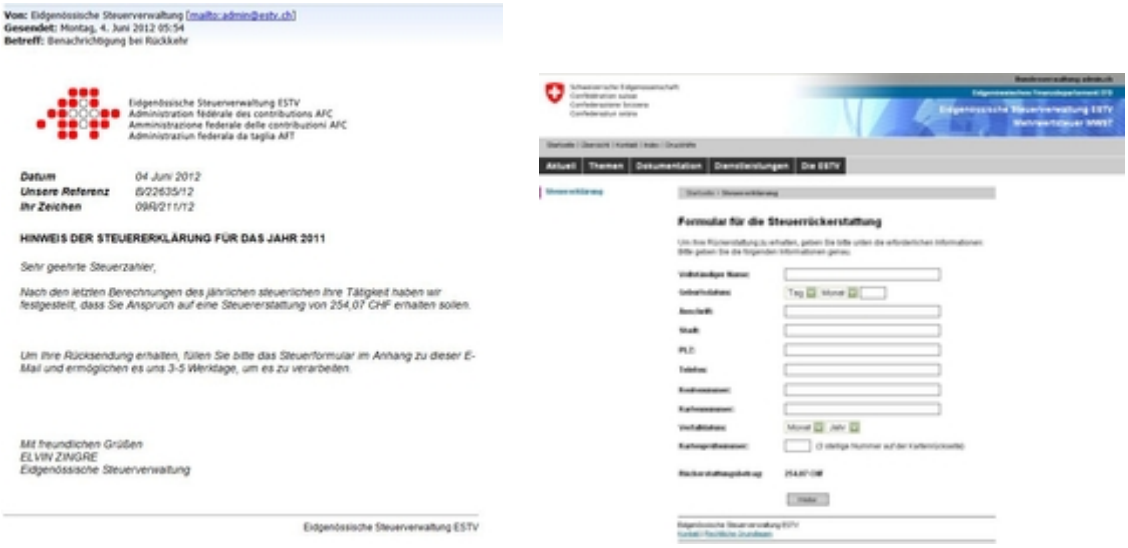
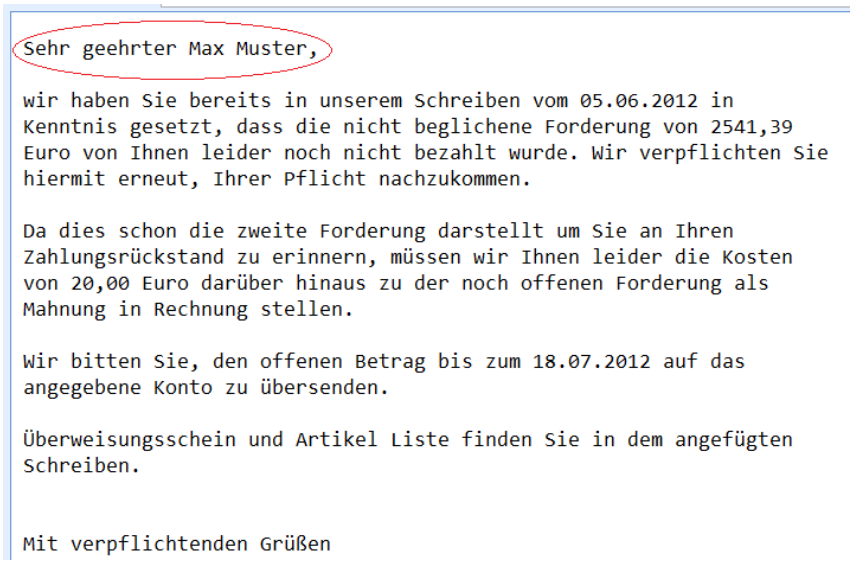


Bild 5: Phishing E-Mail mit dazugehörender Eingabe Maske im Anhang

Lange wurde bei Betrugs-E-Mails erwartet, dass diese eine persönliche Anrede enthalten, um beim Opfer einen vertrauenswürdigeren Eindruck zu hinterlassen. Erstaunlicherweise wurde dies aber bislang nur in Ausnahmefällen beobachtet. Ein Beispiel, bei dem diese Methode eingesetzt wurde, war eine E-Mail-Welle im Sommer 2012, mit der versuchte wurde, eine Schadsoftware im *Anhang* zu verbreiten:

[9] MELANI Halbjahresbericht 2011/2, Kapitel 3.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012).



Sehr geehrter Max Muster,

wir haben Sie bereits in unserem Schreiben vom 05.06.2012 in Kenntnis gesetzt, dass die nicht beglichene Forderung von 2541,39 Euro von Ihnen leider noch nicht bezahlt wurde. Wir verpflichten Sie hiermit erneut, Ihrer Pflicht nachzukommen.

Da dies schon die zweite Forderung darstellt um Sie an Ihren Zahlungsrückstand zu erinnern, müssen wir Ihnen leider die Kosten von 20,00 Euro darüber hinaus zu der noch offenen Forderung als Mahnung in Rechnung stellen.

Wir bitten Sie, den offenen Betrag bis zum 18.07.2012 auf das angegebene Konto zu übersenden.

Überweisungsschein und Artikel Liste finden Sie in dem angefügten Schreiben.

Mit verpflichtenden Grüßen

Bild 6: Beispiel eines E-Mails mit Schadsoftware und persönlicher Anrede

Grundsätzlich kann davon ausgegangen werden, dass seriöse Unternehmen nie per E-Mail nach Passwörtern fragen oder ihre Kunden via E-Mail dazu auffordern, ihre Kreditkarte, ihr Konto oder andere persönliche Angaben zu verifizieren oder zu aktualisieren. Entsprechende Mails stammen in der Regel von Betrügern. Die Betrüger denken sich aber immer wieder neue Szenarien aus, um die Empfänger dazu zu verleiten, unbedacht zu reagieren. Lesen Sie hierzu auch das Kapitel 5.4. «Kundenkommunikation im Zeitalter von *Phishing*».

Befolgen Sie jeweils bei unerwarteten verdächtigen Mail-Nachrichten oder Nachrichten von unbekannten Absendern keinesfalls die Anweisung im Text, klicken Sie keine Attachments an und folgen Sie keinen Links, sondern löschen Sie die Nachricht.

3.7 E-Voting Zwischenfälle

Die Ausübung der direkten Demokratie ist eines der höchsten Güter eines jeden Schweizers. Dazu gehört auch das E-Voting, also die Möglichkeit der elektronischen Stimmabgabe. Der Vorteil liegt auf der Hand: Die Teilnahme an politischen Meinungsbildungsprozessen wie z.B. Volksabstimmungen ist nicht an Öffnungszeiten von Stimmlokalen gebunden und kann überall auf der Welt sichergestellt werden.

Es ist daher nicht erstaunlich, dass neben der Schweiz auch ausländische Staaten, darunter insbesondere Norwegen, Estland und Frankreich, viel versprechende Versuche mit der elektronischen Stimmabgabe durchführen.

Allerdings können Manipulationsgerüchte die Vertrauenswürdigkeit des E-Voting in Frage stellen und nachhaltig gefährden. Bereits einfache Attacken wie *DDoS* Angriffe können weitreichende Folgen haben und eine demokratische Abstimmung verzögern oder gar verunmöglichen. Kapitel 5.5 geht näher auf diese Thematik ein.

Nachfolgend sind einige Beispiele von Zwischenfällen aufgeführt, welche im ersten Halbjahr 2012 im Zusammenhang mit E-Voting-Systemen standen:

Überzählige Stimme bei E-Abstimmung in der Schweiz

Im Anschluss an die Eidgenössische Volksabstimmung vom 11. März 2012 wurde bekannt, dass die Stimme eines im Kanton Luzern wohnhaften Stimmbürgers aufgrund eines Soft-

warefehlers irrtümlich zweimal gespeichert worden sei. Der Fehler sei sofort bemerkt worden und die Spezialisten konnten die überzählige Stimme aus dem System entfernen. Es habe nie Anlass gegeben, an der Richtigkeit des Endresultats zu zweifeln, und das Stimmgeheimnis sei jederzeit gewahrt gewesen, hiess es in der Medienmitteilung[10].

Attacke auf das E-Voting der kanadischen New Democratic Party

Bei der Wahl des Vorsitzenden der kanadischen New Democratic Party wurde das mehrstufige Wahlverfahren über E-Voting abgewickelt. Mehrere zehntausend Parteimitglieder stimmten online von zu Hause ab. Während der Wahl wurden dann aber die Server mittels *DDoS* angegriffen und dadurch das Wahlprozedere verzögert. Mehrmals wurde die Frist für die Stimmabgabe verlängert, einer der Wahlgänge musste sogar abgebrochen und später neu gestartet werden. Dies dürfte mehrere Wahlberechtige von der Teilnahme abgehalten haben.

Pilotprojekt für Online Wahlverfahren in der US Hauptstadt Washington gehackt

Im März 2012 publizierten Forscher der Universität Michigan die Nachricht, dass die Sicherheitsfunktionen eines Pilotprojekts für ein Online-Wahlverfahren der US-Hauptstadt Washington innerhalb kürzester Zeit ausgehebelt werden könne. 48 Stunden nach dem Aufschalten des Systems hatten die Forscher laut eigenen Angaben praktisch die vollständige Kontrolle über den Wahlserver. Dabei waren sie angeblich in der Lage, jede Stimmabgabe zu ändern und fast jede der geheimen Wahlurnen offenzulegen. Der Angriff sei erst zwei Tage später entdeckt worden und dies auch nur, weil die Forscher eindeutige Spuren hinterlassen hätten.

Österreichs Verfassungsgerichtshof hebt die Verordnung für E-Voting bei Österreichischen Hochschülerschafts (ÖH)-Wahl auf

Der österreichische Verfassungsgerichtshof hat die Verordnung zum E-Voting bei der Österreichischen Hochschülerschafts (ÖH)-Wahl 2009 als gesetzeswidrig aufgehoben, da nicht ausreichend präzise geregelt war, wie das fehlerlose Funktionieren des Systems überprüft werden kann. Gemäss Österreichischem Innenministerium hat das Urteil keine wegweisende Bedeutung, weil das E-Voting für Bundeswahlen zuerst sowieso verfassungsrechtlich verankert werden müsse. Eine Verfassungsmehrheit für eine entsprechende Anpassung zeichnet sich derzeit in Österreich nicht ab.[11]

3.8 Schadsoftware mit Zertifikat von angeblicher Schweizer Firma

Zwischen Dezember 2011 und März 2012 sind mehrere Versionen der *Schadsoftware* «Mediyes»[12] aufgetaucht, welche mit einem *Schlüsselzertifikat* einer Innerschweizer Firma mit

---

10 http://www.ge.ch/evoting/scrutin_20120311.asp (Stand: 31. August 2012).

11 http://www.heise.de/newsticker/meldung/Oesterreichs-Verfassungsgerichtshof-hebt-E-Voting-auf-1400214.html (Stand: 31. August 2012).

12 Bei der Schadsoftware Mediyes handelt es sich um eine so genannte Klickbetrug-Schadsoftware: Hierzu fängt sie die Suchmaschinenanfragen an Google, Yahoo und Bing beim Opfer ab und leitet diese an einen Server eines Anzeigen-Netzwerkes weiter.

Damit Webseitenbetreiber auf Ihrer Seite einfach Werbung schalten und somit Geld verdienen können, stellen Onlinewerbefirmen unter anderem Suchfunktionen zur Verfügung, welche auf der Seite einfach eingebunden werden können. Sucht nun ein Besucher nach einem Begriff, wird neben den Ergebnissen der Website zu-

Namen Conpavi AG versehen waren. Auf der Webseite gab sich die Firma als Partner der Stadt Luzern und der Berner Fachhochschule beim Aufbau von E-Government-Projekten aus.

Die Conpavi AG existiert zwar und ist im Handelsregister eingetragen, der Unternehmenszweck ist jedoch die Erbringung von Dienstleistungen und Handel mit Waren im pharmazeutischen Bereich. Dies hat mit E-Government wenig zu tun. Handelt es sich bei der Firma also um eine Scheinfirma, die durch Betrüger eigens zu diesem Zweck erfunden wurde, wie dies einige Medien berichteten?[13]

So einfach scheint dies allerdings nicht zu sein. Ein Blick in die *Internet-Achivierungsmaschine* archive.org zeigt, dass die Site conpavi.ch das erste Mal im Jahr 2002 auftauchte.

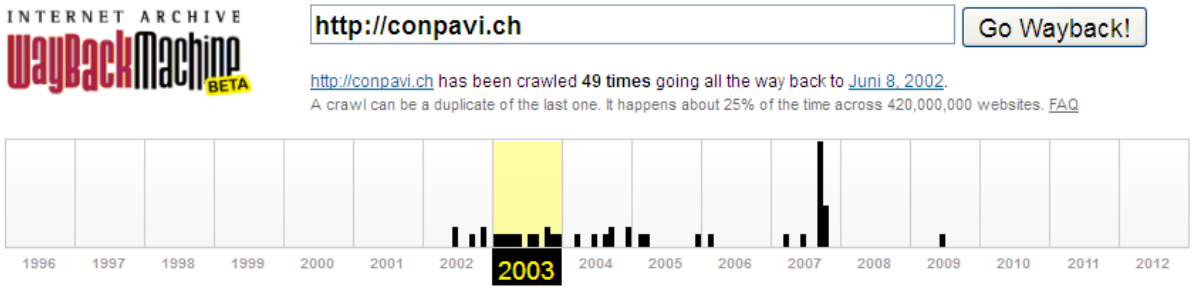


Bild 7: Archiveinträge von archive.org bezüglich der Firma Conpavi

Ein genauer Blick in das Handelsregister zeigt, dass die Firma am 20. März 2000 unter dem Namen netauc gegründet und am 11. Dezember 2001 in den Namen conpavi umbenannt wurde. Zweck der Firma war die Erbringung von Dienstleistungen im Zusammenhang mit elektronischen Kommunikationsmitteln, insbesondere in Internetbelangen für Behörden.[14] Am 16. Juni 2009 wurde Conpavi dann in eine Firma umgewandelt, welche Dienstleistungen und Handel mit Waren im pharmazeutischen Bereich erbringt. Die Website der alten Firma mit der alten Dienstleistungsbeschreibung wurde jedoch so belassen. Diese bot sich für die Kriminellen also nahezu als perfekte Plattform an, um ihre Betrügereien durchzuführen und um an *Zertifikate* zu kommen. Wer sich nicht genauer mit der Materie befasst hatte, konnte tatsächlich meinen, dass die Firma noch existiere und in Sachen *E-Government* agiere. Demzufolge war es anscheinend auch möglich, die Zertifizierungsstellen zu überzeugen, ein entsprechendes *Zertifikat* auszustellen.

Betrüger suchen nach allen Möglichkeiten, um ihre Aktionen für die Opfer möglichst glaubhaft durchzuführen. Dabei kommt es immer wieder vor, dass Firmennamen oder Firmenwebsites nach einer Firmenauflösung für Betrügereien missbraucht werden. Die Websites sind immer noch gut verlinkt und eine Google-Suche ergibt jeweils keine verdächtigen Aktivitäten. Oft übernehmen die Betrüger auch den *Domainnamen,* nachdem dieser durch die Firma gelöscht, respektive die Domainregistrierung nicht mehr verlängert worden ist. Die Betrüger

---

sätzlich noch eine Werbenachricht aufgeschaltet. Klickt der Besucher dann auf einen solchen vorgeschlagenen Link, bekommt der Webseitenbesitzer Geld.

Genau hier setzten die Betrüger an und verwendeten die kopierten Suchanfragen um solche Werbeeinblendungen (auf der eigens hierzu kreierten Webseite) zu erzwingen und dann im Hintergrund automatisch darauf zu klicken und Geld zu verdienen.

[13] http://www.nzz.ch/aktuell/startseite/zuger_scheinfirmaauf_krummer_tour_im_internet-1.16001018 (Stand: 31. August 2012).

[14] http://www.zefix.admin.ch (Stand: 31. August 2012).

können so die Reputation mitbenutzen, welche die Firma bis zu ihrer Liquidation, Zweck- oder Namensänderung aufgebaut hat.

3.9 Bundesrat heisst Nationale Strategie zum Schutz vor Cyber-Risiken gut

Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken gutgeheissen.[15] Der Bundesrat sprach sich unter anderem für eine personelle Verstärkung von MELANI im EFD und VBS ab 2013 aus. Mit der vorliegenden Strategie wird auch mehreren parlamentarischen Vorstössen Rechnung getragen, in denen verstärkte Massnahmen gegen Cyber-Risiken gefordert wurden.

Der Bundesrat verfolgt dabei die folgenden strategischen Ziele:

- die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich,
- die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen,
- die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.

Die Strategie bezeichnet die verantwortlichen Bundesstellen, welche 16 in der Strategie genannte Massnahmen im Rahmen ihres Grundauftrags bis Ende 2017 umsetzen. In diesen Umsetzungsprozess sollen Partner aus Behörden, Wirtschaft und Gesellschaft einbezogen werden. Eine Koordinationsstelle im EFD überprüft dabei die Umsetzung der Massnahmen und den Bedarf nach weiteren Vorkehrungen zur Risikominimierung.

Die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie die Kooperation mit dem Ausland bleibt dabei die Voraussetzung, um Cyber-Risiken minimieren zu können. Mit einem permanenten gegenseitigen Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden. Der Staat soll nur eingreifen, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt.

Der Umgang mit Cyber-Risiken soll gemäss der Strategie als Teil eines integralen Geschäfts-, Produktions- oder Verwaltungsprozesses verstanden werden, bei dem alle Akteure – von der technischen bis hin zur Führungsstufe – einzubeziehen sind. Jede Organisationseinheit aus Politik, Wirtschaft und Gesellschaft trägt die Verantwortung, die Cyber-Ausprägung ihrer Aufgaben und Verantwortlichkeiten zu erkennen und die damit einhergehenden Risiken in ihren jeweiligen Prozessen zu adressieren respektive soweit machbar zu reduzieren. Die dezentralen Strukturen in Verwaltung und Wirtschaft sollen für diese Aufgaben gestärkt und bereits bestehende Ressourcen und Prozesse konsequent genutzt werden. Die fortlaufende Zusammenführung von technischen und nicht technischen Informationen ist notwendig, um Cyber-Risiken umfassend zu analysieren und zu bewerten. Diese Erkenntnisse sollen möglichst zentral aufbereitet und Bedarfsgerecht an die Akteure zur Unterstützung ihrer Risikomanagementprozesse weitergegeben werden.

Die Strategie identifiziert Cyber-Risiken in erster Linie als Ausprägung bestehender Prozesse und Verantwortlichkeiten. Entsprechend sollen diese Cyber-Risiken auch in bereits bestehende Risikomanagementprozesse Eingang finden. Primär soll die Informationsgrundlage über Cyber-Risiken bei den Verantwortlichen und ihre Wahrnehmung dafür geschärft werden. Dazu erteilt der Bundesrat den Departementen den Auftrag, die Umsetzung der Massnahmen auf ihrer Ebene und im Verbund und Dialog mit kantonalen Behörden und der Wirtschaft an die Hand zu nehmen. Die Massnahmen erstrecken sich dabei von Risikoanalysen

[15] http://www.news.admin.ch/message/index.html?lang=de&msg-id=45138

zu kritischen IKT-Infrastrukturen bis zur stärkeren Einbringung der Schweizer Interessen in diesem Bereich auf internationaler Ebene.

Der Bundesrat anerkennt somit, dass in der Schweiz die Zusammenarbeit zwischen Behörden und Wirtschaft generell etabliert ist und gut funktioniert. Mit der Strategie zum Schutz der Schweiz vor Cyber-Risiken will er im Cyber-Bereich diese Zusammenarbeit vertiefen und das bereits gelegte Fundament weiter stärken, um so die Minimierung von Cyber-Risiken zielgerichtet anzugehen. Er setzt daher auf bestehende Strukturen und verzichtet auf ein zentrales Steuerungs- und Koordinationsorgan, wie es in anderen Ländern mit teils weniger ausgeprägter Zusammenarbeit zwischen den relevanten Akteuren nun aufgebaut wird. Stattdessen soll der Informationsfluss und die gesamtheitliche Auswertung vorliegender Informationen zu Cyber-Risiken und –Bedrohungen zur Unterstützung von Behörden, Wirtschaft und Betreibern kritischer Infrastrukturen intensiviert und bedarfsgerechter verbreitet werden. Zu diesem Zweck soll die Melde- und Analysestelle Informationssicherung MELANI gestärkt werden.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Iran im Fadenkreuz? Flame und Wiper

Am 28. Mai 2012 meldete Kaspersky Lab die Entdeckung eines sehr komplexen Schadprogrammes, welches benutzt wurde, um Organisationen in mehreren Ländern anzugreifen und auszuspionieren. Dessen Funktionen umfassen das Einsammeln von Informationen aller Art. Beispielsweise kann es Netzwerkverkehr überwachen, Tastatureingaben überwachen, Bildschirminhalte kopieren, Audiomitschnitte erstellen und sogar via *Bluetooth* Adressbücher von Mobiltelefonen in der Nähe auslesen, wenn beim Handy die Bluetooth-Funktion eingeschaltet ist. Das «Flame» genannte Schadprogramm war insbesondere im Mittleren Osten aktiv. Rund die Hälfte der nachgewiesenen Infektionen war im Iran. Erste Versionen datieren aus dem Jahr 2006 – folglich konnte das Spionagenetzwerk während über fünf Jahren unentdeckt agieren. Dies nicht zuletzt deshalb, weil die Angreifer stets nur einige Dutzend Systeme gleichzeitig infiziert und «Flame» nach der Datenbeschaffung auf den betroffenen Systemen jeweils wieder gelöscht hatten. Konsequenterweise haben die Angreifer nachdem die Entdeckung des Schadprogrammes durch Kaspersky Lab öffentlich bekannt wurde, die Kontrollinfrastruktur des Spionagenetzwerks abgeschaltet, um ihre Spuren zu verwischen.

Für die Kontrollinfrastruktur wurden während der Laufzeit des Angriffes über 80 *Domainnamen* registriert und Server rund um die Welt verwendet, darunter in Hong Kong, Vietnam, der Türkei, aber auch Deutschland, England und der Schweiz.

Verbreitet hat sich «Flame» über USB-Sticks und lokale Netzwerke. Bei der Infektion via USB-Sticks wurde die selbe Sicherheitslücke ausgenutzt wie bei Stuxnet. Die technische Analyse durch Sicherheitsunternehmen zeigte zudem verschiedene weitere Gemeinsamkeiten von «Flame», «Stuxnet» und «Duqu» auf.[16]

Die Schadsoftware «Wiper» störte im April 2012 die Kommunikationsnetze des iranischen Ölministeriums, las Daten aus dessen Netzen aus und löschte schliesslich auch Festplatten

[16] Siehe: MELANI Halbjahresbericht 2010/2, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de und MELANI Halbjahresbericht 2011/2, Kapitel 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012)

von infizierten Systemen komplett. Zur Eindämmung von «Wiper» und als Sicherheitsmassnahme wurden im Iran zwischenzeitlich die Computersysteme des Ölministeriums und verschiedener Ölverladeterminals vom Internet getrennt.

Diese Angriffe zeigen einmal mehr, dass es nicht mehr nur um vereinzelte Spionageangriffe geht, sondern vielmehr um ein dauerndes Interesse am Zugang zu Systemen, Daten und Informationen und dass der Druck auf sensible Daten und Systeme jeden Tag zunimmt. Dabei ist es möglich, Spionageinfrastruktur jahrelang unerkannt betreiben zu können. Es ist deshalb davon auszugehen, dass bereits jetzt weitere Spionagesoftware platziert ist und entweder parallel benutzt oder aber für den Fall der Aufdeckung eines Angriffs als Ersatz bereitgehalten wird, um einmal infiltrierte Systeme und Netzwerke weiterhin aushorchen und sabotieren zu können.

Siehe auch Kapitel 5.2

4.2 Hacktivismus in Nahost

Im Januar lieferten sich anti- und pro-israelische Hacker kleinere Scharmützel. Ein selbstdeklariert saudischer Hacker, der sich «0xOmar» nennt, veröffentlichte Kreditkarteninformationen tausender Israelis, welche er durch Angriffe auf Datenbanken von Internetdienstleistern erbeutet hatte. Als Antwort auf diese Aktion veröffentlichte ein israelischer Hacker Namens «0xOmer» Daten über saudische Staatsangehörige. Am Tag nach dem Aufruf eines Hamas-Sprechers, mit Angriffen auf israelische Websites gegen die Besatzung Palästinas zu protestieren, wurde die Website der israelischen Fluggesellschaft El Al sowie der israelischen Börse gestört, was mit Hacktivisten-Angriffen auf die Website der Börsen der Vereinigten Arabischen Emirate und Saudi-Arabiens vergolten wurde. Dies motivierte wiederum einen Fernsehprediger in Kuwait, via Twitter zum Cyber-Dschihad gegen Israel aufzurufen. Einige Tage später veröffentlichte ein pro-israelischer Hacker dann Facebook-Zugangsdaten von mehreren tausend Arabern, was Facebook dazu zwang, die Passwörter der betroffenen Konten zurückzusetzen. Nach einigen weiteren Hacks und Veröffentlichungen der erbeuteten Daten sowie Angriffen auf die Verfügbarkeit von Webseiten ebbten die offenen Feindseligkeiten Mitte Februar wieder ab.

Diese Vorkommnisse zeigen exemplarisch, wie politische Konflikte auch von nichtstaatlichen respektive beliebigen Akteuren angeheizt werden können. Wird einer Publikation von bei einem Hack erbeuteten Daten ein politisches Statement beigefügt, provoziert dies Reaktionen aus dem Lager der politischen Gegner. Auf diese Weise können sich Hacker gegenseitig aufwiegeln. Während im vorliegenden Fall die eine Seite klar bekannt war, stützte sich die andere Seite bei ihrer Zielauswahl zuerst auf die ungesicherte Selbstdeklaration des Erstangreifers. Im Verlauf der Ereignisse kamen aber Zweifel an der Herkunft des Initiators „0xOmar“ auf, worauf auch andere arabische Länder und der Iran ins Fadenkreuz der pro-israelischen Hacker geriet. Bei solchem Hacktivismus stellt sich wie bei staatlichen Angriffen das Problem der Zurechnung. Solange man einen Angreifer nicht eindeutig identifiziert hat, läuft man Gefahr, die Vergeltung an die falsche Adresse zu schicken und dabei nicht zuletzt eine grosse Zahl unbeteiligter Personen in Mitleidenschaft zu ziehen.

4.3 Anonymous kündigte an, das Internet anzugreifen – Messbare Beeinträchtigungen blieben aus

Anonymous hat am 12. Februar 2012 angekündigt, mit einem Angriff auf die 13 *DNS* Root-*Server* das Internet am 31. März lahmzulegen, um gegen das geplante US-Gesetz «SOPA - Stop Online Piracy Act», die Wallstreet, unverantwortliche Politiker, Banker und generell ge-

gen allgemeine Missstände zu demonstrieren. Der Aufruf hat zwar zu einem grossen Medieninteresse, aber wie erwartet, zu keinerlei messbaren Beeinträchtigungen geführt.

Mit Hilfe des Domain Name Systems (DNS) lassen sich das Internet und dessen Dienste benutzerfreundlich verwenden, da man anstelle von *IP-Adressen* Webadressen (*URL*s) verwenden kann. Ohne *DNS*-Server ist das Internet immer noch funktionsfähig, es müssen aber an Stelle der *URL*s die *IP-Nummern* eingegeben werden. In der Hierarchie zuoberst befinden sich die *Root-Server*, welche als oberste Instanz für Informationen betreffend *Top-Level-Domains* (z. B. .com, .net, .ch) zuständig sind.

Weil die *DNS-Root-Server* für das Funktionieren des Internets essentiell sind, sind diverse Sicherheitsmechanismen implementiert. So handelt es sich bei den 13 DNS-Root-Servern nicht nur um 13 einzelne Server. Insgesamt werden 259 Server bei unterschiedlichen Providern in verschiedenen Ländern betrieben.

Bei der von Anonymous in diesem Fall beschriebenen Angriffsmethode «*DNS-Amplification Attack*» wird ausgenutzt, dass Name-Server in bestimmten Fällen auf kleine Anfragepakete mit sehr grossen Paketen antworten. Theoretisch kann eine 60 Byte lange Anfrage eine mehr als 3000 Byte grosse Antwort provozieren. Diese grossen Antworten sollten dann auf die DNS-Root-Server gelenkt werden, sie überlasten und somit lahmlegen. Diese Server sind allerdings mit enormen Kapazitäten ausgestattet, um Lastspitzen abzufangen. So wird sichergestellt, dass das *DNS* auch dann noch funktioniert, wenn zwei Drittel der Root-Server ausfallen würden. Hinzu kommt, dass ein Ausfall der *DNS-Root-Server* nur dann Auswirkungen hätte, wenn er längere Zeit anhalten würde, da viele Provider *DNS* Anfragen lokal zwischenspeichern, um den Netzwerkverkehr zu reduzieren. Die *DNS-Root-Server* werden aber permanent überwacht. Würde eine Anomalie erkannt, würde der schadhafte Verkehr zu den *DNS-Root-Servern* sofort blockiert. Zuletzt gab es 2007 einen Grossangriff auf 2 der 13 *DNS-Root-Server*. Weil die übrigen einwandfrei funktionierten, blieben auch hier spürbare Folgen aus.

Ein Angriff auf das Internet passt nicht zum Vorgehen von Anonymous, das beispielsweise wiederholt erklärt hat, es werde keine Medien angreifen. Ein Angriff, der alle Internetnutzer betreffen würde, wäre wohl für Anonymous kontraproduktiv und Anonymous dürfte so auch Sympathisanten verlieren. Um einen solchen Angriff durchzuführen, wären zudem vorgängige Tests des angeblichen Tools nötig und eine grosse Zahl an Freiwilligen. Wie auch schon beim angekündigten Angriff gegen Facebook im November 2011 haben sich verschiedene Anonymous-Aktivisten von diesem Aufruf distanziert.

Die lockere Anbindung bei Anonymous resultiert in einer Reihe unkoordinierter, mehr oder weniger spektakulärer Ankündigungen und Angriffe. Da es strukturinhärent keine Mitgliedschaft bei Anonymous gibt und keine offiziellen Sprecher oder sonst wie für die gesamte Bewegung verantwortliche Personen existieren, kann prinzipiell jeder im Namen von Anonymous Mitteilungen veröffentlichen und so ein Medieninteresse generieren.

Anonymous hört Telefonkonferenz von Scotland Yard und FBI ab

Anonymous-Aktivisten ist es gelungen, eine vertrauliche Telefonkonferenz der Londoner Polizei Scotland Yard und der US-Bundespolizei FBI abzuhören. Anonymous hatte es anscheinend geschafft, eine E-Mail, welche die Zugangsdaten zu der Telefonkonferenz enthielt, abzufangen. Die Inhalte der Konferenz wurde von den Aktivisten unter anderem auf YouTube veröffentlicht.
Bei der Telefonkonferenz wurden neben vielen Nebensächlichkeiten auch Details über laufende Ermittlungen gegen Anonymous und «LulzSec»diskutiert, wie beispielsweise die Ter-

mine geplanter Festnahmen. Neben der Konferenz-Audiodatei veröffentlichte Anonymous auch die E-Mail, welche die Zugangsdaten zu der Telefonkonferenz enthält. Ein Strafverfahren wurde eröffnet.[17]

4.4 Proteste gegen ACTA – auch im Internet

Anfang des Jahres 2012 gab es in diversen Ländern heftige Proteste gegen die geplante Ratifizierung des ACTA-Vertrages. Das Anti-Counterfeiting Trade Agreement (ACTA) ist ein geplantes multilaterales Handelsabkommen auf völkerrechtlicher Ebene. Die teilnehmenden Nationen wollen mit ACTA internationale Standards im Kampf gegen Produktpiraterie und Urheberrechtsverletzungen etablieren.

Diese Proteste, die zum Ziel hatten den ACTA-Vertrag zu kippen, fanden vor allem in Form von traditionellen Demonstrationen statt, die im gesamteuropäische Aktionstag am 11. Februar 2012 ihren Höhepunkt erreichten. Aber auch im Netz wurden zahlreiche Protestaktionen beobachtet, von welchen hier einige (ohne Anspruch auf Vollständigkeit) erwähnt werden:

Tschechien

In Tschechien wurden 27.000 Datensätze über Mitglieder der Regierungspartei ODS gestohlen und veröffentlicht. Die Datensätze enthielten neben der privaten Anschrift auch die Telefonnummern der Parteimitglieder. Am 6. Februar 2012 wurde die ACTA-Ratifizierung in Tschechien bis auf weiteres gestoppt.

Polen

Verschiedene Webseiten der polnischen Regierung wurden zeitweise durch *DDoS* Attacken lahmgelegt. Der polnische Ableger von Anonymous und die Hackergruppe «Polish Underground» soll hinter diesen Attacken gesteckt haben. Einige Aktivisten haben ausserdem die Webseite der Gemeinde Kraszewniki[18] demaskiert und eine Nachricht hinterlassen. Auch hier hat die Regierung beschlossen, die ACTA-Ratifizierung auszusetzen.

USA

Im Zuge der Protestaktionen gegen ACTA hat Anonymous offenbar auch mehrere Webseiten der US-Handelskommission FTC gehackt. Sieben Webseiten sollen demnach von der Attacke betroffen gewesen sein – allerdings nicht die Hauptseite.

Griechenland

Hacker der Anonymous-Bewegung griffen am Freitag, 3. Februar 2012, die Website des griechischen Justizministeriums an. Dabei wurde gegen die Sparmassnahmen, aber auch gegen eine Teilnahme Griechenlands am ACTA-Abkommen protestiert. Vier Stunden lang wurden entsprechende Texte auf der Webseite des Ministeriums eingeblendet. Die Hacker gaben der Regierung zwei Wochen Zeit, aus dem ACTA-Abkommen auszusteigen. Andernfalls sollten neue Attacken folgen.

Slowenien

Der slowenische Ableger der Hackergruppe Anonymous hatte im Zuge der Protestaktionen gegen ACTA mehrere Webseiten vorübergehend lahmgelegt, darunter jene der führenden

---

[17] http://www.spiegel.de/netzwelt/web/anonymous-attacke-hacker-veroeffentlichen-fbi-gespraech-mit-scotland-yard-a-813224.html (Stand: 31. August 2012).

[18] http://www.kraszewniki.pl/ (Stand: 31. August 2012).

Regierungspartei SDS und auch anderer Parteien. Ein Ratifizierungsstopp erfolgte am 7. Februar 2012.

In der Schweiz waren die Proteste weit weniger ausgeprägt. Dies wohl auch, weil in der Schweiz dem Bürger mit dem Referendum und der Initiative auch noch andere Instrumente auf politischer Ebene zur Verfügung stehen. Zwar gab es kleinere Demonstrationen vor allem in Zürich – grosse Demonstrationen oder gar Angriffe im Netz wie in anderen europäischen Ländern wurden aber nicht beobachtet. Obwohl die Schweiz an der Ausarbeitung und den Verhandlungen von ACTA mitgewirkt hat, teilte der Bundesrat am 9. Mai 2012 mit, das Abkommen vorerst nicht zu unterzeichnen.

Die Proteste rund um das ACTA-Abkommen sind ein weiteres Beispiel, dass sich Proteste immer mehr auch in den virtuellen Raum verschieben. Es zeigt aber auch die grosse Sensibilität der Bürger gegenüber Internet-Themen. Jede Einschränkung und Regulierung wird hier mit besonderer Skepsis betrachtet, da mit dem Internet immer noch der freie und manchmal auch rechtsfreie Raum verbunden wird.

4.5 Massenweise Passwörter und Kreditkartendaten gestohlen

Das erste Halbjahr 2012 war wiederum geprägt durch verschiedene grosse Angriffe auf bekannte Firmen, bei denen Kundendaten – meist Login und Passwort aber auch Kreditkartendaten – gestohlen wurden.

So wurde beispielsweise in der Woche vom 4. Juni 2012 bekannt, dass über 6 Millionen *SHA*-1-*Hash* Werte von Passwörtern des Online-Berufsnetzwerk «LinkedIn» in einschlägigen Internet-Foren publiziert wurden. *SHA*-1 ist eine weit verbreitete kryptographische Hashfunktion, die aus einer beliebigen Nachricht einen 160-Bit-Hashwert (deutsch: Prüfsumme) erzeugt. Oft kann man aus diesem Hash-Wert das Passwort rekonstruieren. Viele Passwörter wurden bereits auch im Klartext publiziert. Zwar fehlten in den publizierten Dokumenten die dazugehörigen E-Mail Adressen (welche als Benutzername fungieren) – es muss allerdings davon ausgegangen werden, dass auch diese Daten gestohlen wurden und sich beim Angreifer befinden.

Wenige Stunden nach Bekanntwerden des Vorfalls, tauchten bereits Phishing-Webseiten auf, welche die Benutzer aufforderten, ihre LinkedIn Passwörter zu «überprüfen».

Zugriff auf die Datenbank von Amazon Tochter «Zappos»

Bei der Amazon Tochter «Zappos» haben sich Unbekannte Zugriff auf die persönlichen Daten von rund 24 Millionen registrierten US-Kunden verschafft und dabei auch Password Hashes der Kunden gestohlen. Glücklicherweise waren nur jeweils die letzten vier Ziffern der Kreditkarten in der angegriffenen Datenbank gespeichert. Auf die Server, auf denen weitere Zahlungsinformationen und die vollständigen Kreditkartennummern hinterlegt sind, konnten die Täter nach Unternehmensangaben nicht zugreifen.[19]

Angriff auf Kreditkartendaten bei Global Payments

Nicht so viel Glück hatte der Kreditkartenverarbeiter «Global Payments». Hier sollen über 1.5 Millionen Datensätze an Kreditkartennummern gestohlen worden sein. Anscheinend lag dem

[19] http://online.wsj.com/article/BT-CO-20120116-706917.html (Stand: 31. August 2012).

Datendiebstahl ein Hackerangriff auf ein New Yorker Taxiunternehmen zu Grunde.[20] Dabei war es den Angreifern gelungen, sich Zugang zu einem Administratoren-Konto dieses Unternehmens zu verschaffen und während einigen Monaten Kreditkartendaten abzugreifen. Die Daten wurden aber nicht sofort verwendet, sondern die Betrüger sammelten diese, um alle zu einem bestimmten Zeitpunkt zu verwenden. So viermieden sie, dass der Diebstahl auffällt und allfällige Gegenmassnahmen die Rendite schmälern würden.

450'000 Benutzernamen und Passwörter von der «Content Börse Yahoo! Contributor Networks» gestohlen

Yahoo wurde im ersten Halbjahr 2012 Opfer eines Hackerangriffs. Hierbei wurden knapp 450'000 Benutzernamen und Passwörter der «Content Börse Yahoo! Contributor Networks»[21] durch die Hackergruppe «D33Ds Company» gestohlen und ins Netz gestellt. Laut Yahoo wurde eine Sicherheitslücke im Computersystem des Konzerns missbraucht, welche nach eigenen Angaben sofort geschlossen wurde. Laut Hackergruppe «D33Ds Company» soll die Datenbank weder gut gesichert, noch die Passwörter verschlüsselt abgespeichert worden sein. Der Angriff sollte als Weckruf für die verantwortlichen Datenbankadministratoren verstanden werden.

50'000 Benutzernamen und Passwörter von Twitter aufgetaucht

Auch von Twitter-Konten tauchten am 9. Mai 2012 über 50'000 Benutzernamen und Passwörter auf. Twitter hatte danach versprochen, die Passwörter der betroffenen Konten zurückzusetzen. Es ist nach wie vor unklar, von wo die Daten stammten und wer diese veröffentlicht hatte. Anscheinend war die Qualität der Daten nicht sehr hoch, da sich darunter viele Doppeleinträge, bereits gesperrte Konten oder Accounts mit Falschangaben (Fake Accounts) befunden haben.[22]

GMX-Konten geknackt

Beim Mail-Anbieter GMX wurde festgestellt, dass in mindestens 3000 Fällen GMX-Konten geknackt wurden. Ursprünglich nahm man an, dass die Angriffe mittels *Brute-Force* Angriff durchgeführt wurden. Dieses Verfahren eignet sich jedoch bei Online-Dienstleistungen nur sehr bedingt, da ein Angriff in dieser Grössenordnung sehr schnell auffallen würde. Viel wahrscheinlicher ist es, dass die Angreifer im Besitz von Logins und Passwörtern waren. So bestätigte GMX, dass sehr gezielt Benutzername und Passwort eingegeben wurde. Wie die Passwörter entwendet wurden, ist nicht bekannt. Es könnte sich aber um Passwörter handeln, die in anderem Zusammenhang – sprich bei anderen Dienstleistern – gestolen wurden und dann bei den GMX-Konten «ausprobiert» wurden.[23] Da viele Personen für alle Dienstleistungen im Internet immer noch ein und das selbe Passwort verwenden, ist so ein Ansatz nicht abwegig.

Laut «Firehost» sind die Angriffe auf Internetseiten via *SQL-Injections* zwischen April und Juni 2012 um 69% gestiegen.[24] Bei einer *SQL-Injection* wird versucht, manipulierte Befehle an eine Datenbank zu senden. Meistens geschieht dies über ein schlecht programmiertes Interface, welches die gesendeten Befehle zu wenig oder gar nicht überprüft oder über eine Sicherheitslücke. So lassen sich Kundendaten ausspähen, Online-Shops manipulieren aber auch ganze Datenbestände einfach vernichten. Ein geglückter Angriff, der Verlust von Kun-

[20] http://blogs.gartner.com/avivah-litan/2012/03/30/new-credit-card-data-breach-revealed/ (Stand: 31. August 2012).

[21] http://www.focus.de/digital/internet/datenbank-muehelos-geknackt-hacker-veroeffentlichen-zugangsdaten-von-450-000-yahoo-nutzern_aid_781269.html (Stand: 31. August 2012).

[22] http://www.spiegel.de/netzwelt/web/twitter-passwoerter-im-netz-a-832171.html (Stand: 31. August 2012).

[23] http://www.zeit.de/digital/datenschutz/2012-07/gmx-passwort-account (Stand: 31. August 2012).

[24] http://www.heise.de/newsticker/meldung/Deutlicher-Anstieg-der-SQL-Injection-Angriffe-1651041.html (Stand: 31. August 2012).

dendaten und der damit einhergehende Reputationsverlust kann schnell viel Geld kosten und eine Firma sogar ruinieren. Wie überall hilft es auch hier, die Webseitensoftware immer auf dem neuesten Stand zu halten und diese gut vor Angriffen von aussen zu schützen.

Heutzutage ist es unabdingbar, bei den diversen Online-Dienstleistungen verschiedene Passwörter zu verwenden. Dies bringt einen enormen Sicherheitsgewinn, auch wenn diese Passwörter - zwecks Erinnerung - irgendwo (auf Papier) aufgeschrieben werden.

4.6 SCADA - Update

Eine Gruppe von Sicherheitsdienstleistern veröffentlichte im Januar 2012 Sicherheitslücken in Komponenten von Industriesteueranlagen. Dies sorgte sowohl bei den Herstellern als auch bei den Betreibern für Unruhe. Denn die Entdecker der Schwachstellen hatten die Hersteller zuvor nicht informiert, damit die Lücke im Vorfeld der Veröffentlichung bereits hätte geschlossen werden können. Sie gelangten direkt an die Öffentlichkeit. Diese Vorgehensweise brachte ihnen von verschiedener Seite Kritik ein.

Die Entdecker wollten auf der einen Seite den Betreibern von kritischen Infrastrukturen zeigen, wie leicht *SCADA*-Systeme kompromittiert werden können. Auf der anderen Seite war die Aktion scheinbar als Denkzettel für die Hersteller gedacht. Anscheinend hat die Gruppe bereits Erfahrungen gesammelt, dass Hersteller gewisse Sicherheitslücken zwar schon mehrere Jahre kennen, anstatt diese zeitnah zu beheben, die Veröffentlichung und das Update aber jeweils möglichst lange hinauszögern.[25] Fairerweise muss angefügt werden, dass ein Update von *SCADA*-Systemen nicht vergleichbar ist, mit dem Update eines PCs. So ergeben sich bei einem Update von Kontrollsystemen stets Risiken von Fehlfunktionen, welche unter Umständen gravierende Auswirkungen haben können.

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 Betreiber ihre Software- Komponenten selten aktualisieren. Dies liegt daran, dass bei konstant laufenden Prozessen nur in gewissen Wartungsfenstern ein Update vorgenommen werden kann. Auch können die Auswirkungen von *Patches* auf den Gesamtprozess 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.

Ursprünglich hatten *SCADA*-Systeme nur wenig Ähnlichkeit mit herkömmlicher IKT: Sie waren von den Computernetzwerken isoliert, benutzten proprietäre Hard- und Software und setzten zur Kommunikation mit dem Zentralrechner eigene Protokolle ein. Dies änderte sich in den letzten Jahren grundlegend, seit vergleichsweise günstige Geräte mit eingebauter Schnittstelle zum Internet-Protokoll breit zur Verfügung stehen. Diese Komponenten verfügen zwar meist (noch) nicht über eine Verbindung zum Internet, trotzdem ist es möglich, dass über verseuchte Laptops oder *USB-Sticks*, *Schadsoftware* in die abgeschotteten Systeme gelangt. Da die *SCADA*-Komponenten nicht darauf ausgelegt sind, Sicherheitselemente wie *Firewalls* und *Antiviren Schutzsoftware* zu unterstützen, haben Angreifer, die einmal im Netzwerk sind, deutlich geringere Barrieren.

[25] http://www.heise.de/security/meldung/Sicherheitsexperten-setzen-Hersteller-von-Industriesteuerungen-unter-Druck-1418292.html (Stand: 31. August 2012).

Möglicher Angriff auf US-Gleisanlagen

Laut einem Bericht der amerikanischen «Transportation Security Administration TSA» kam es am 1. Dezember 2011 zu einer Störung einer Gleisanlage im Nordwesten der USA, die anscheinend von zwei unbekannten Zugriffen mit nicht-US IP-Adressen ausgelöst worden war. Dabei sei es zu Verspätungen von 15 Minuten gekommen. Einen Tag später soll es zu einem zweiten Zugriff gekommen sein, der jedoch keine Störung verursachte. Was genau hinter diesen Zugriffen steckte, wurde nicht bekannt gegeben. Das Department of Homeland Security hielt allerdings fest, dass ein gezielter Angriff ausgeschlossen werden könne. Die Daten der drei zugreifenden IP-Adressen waren anderen Transportunternehmen in den Vereinigten Staaten und Kanada zur Verfügung gestellt worden.[26]

Implantate mit Schwachstellen

Das nicht nur bei erfolgreichen Angriffen auf grosse Systeme mit gravierenden Auswirkungen gerechnet werden muss, sondern dass kleine Systeme durchaus auch lebensbedrohliche Auswirkungen haben können, zeigt nachfolgendes Beispiel: In einer aktuellen Studie haben Sicherheitsexperten medizinische Implantate auf ihre Risiken hin geprüft. Wenig überraschend kam dabei heraus, dass zum Beispiel Herzschrittmacher ein erhebliches Sicherheitsrisiko aufweisen. Jedermann bekannt, sind die Warnhinweise an die Träger von Herzschrittmachern bei Geräten mit starker elektromagnetischer Strahlung. Bei einem Test bestrahlten die Forscher ein Defibrillator-Implantat mit Radiowellen, mit dem Ergebnis, dass sich das Implantat ausschaltete. Daneben wurden aber auch andere beängstigte Schwachstellen gefunden. So enthalten beispielsweise *WiFi*-Links, die für die Update-Funktion verwendet werden, Schwachstellen, die ausgenutzt werden können. Schlimmstenfalls führt dies zur Deaktivierung des jeweiligen Geräts (beispielsweise bei Insulinpumpen) mit all den gesundheitlichen Konsequenzen.[27]

4.7 Schaffung eines Europäischen Cybercrime Zentrums

Die europäische Kommission hat am 28. März 2012 vorgeschlagen, ein neues Europäisches Cybercrime Zentrum bei Europol, der europäische Polizeibehörde mit Sitz in Den Haag, zu errichten. Europol koordiniert bereits heute die Arbeit der nationalen Polizeibehörden Europas im Bereich der grenzüberschreitenden organisierten Kriminalität und fördert den Informationsaustausch zwischen den nationalen Polizeibehörden.

Das Zentrum soll den Fokus auf den Kampf in Europa gegen Cybercrime legen und am 1. Januar 2013 seinen Betrieb aufnehmen. Dabei sollen Informationen und Erfahrungen zusammengetragen werden, Kriminaluntersuchungen unterstützt, sowie EU-weite Lösungen und Cybercrime-Awareness gefördert werden. Zusätzlich wird das Zentrum eine Expertencommunity aus allen Gesellschaftszweigen aufbauen, um Cybercrime und Kinderpornographie effizienter zu bekämpfen.[28]

---

26 http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/ (Stand: 31. August 2012).

27 http://www.pcwelt.de/news/Sicherheitsrisiko-Medizinische-Implantate-als-Zielscheibe-fuer-Hacker-5708296.html (Stand: 31. August 2012).

28 https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417 (Stand: 31. August 2012).

Mit der stetig zunehmenden Kommunikation via Internet und dem steigenden kommerziellen Nutzen des Internets nehmen auch die Betrugsfälle und andere Delikte im Internet zu. Bei den Ermittlungen sind regelmässig hunderte Opfer in den verschiedensten Teilen der Welt involviert. Die Spur der Täter führt meist in mehrere Länder und entsprechend durch mehrere Gerichtsbarkeiten. Ermittlungen dieser Grössenordnung und Komplexität können nicht mehr ausschliesslich durch einzelne nationale Polizeikräfte gelöst werden und traditionelle, zeitaufwändige Rechtshilfeverfahren stossen an ihre Effizienzgrenzen. Keine Straftaten sind so international wie Cybercrime. Es braucht einen koordinierten, gemeinsamen und grenzüberschreitenden Ansatz, um Internetkriminalität effektiv verfolgen zu können. Genau hier soll das europäische Cybercrime Zentrum ansetzen und zusätzliche Hilfestellung anbieten.

4.8 Deaktivierung eines Zeus Botnetzwerks

Gemeinsam mit Finanzdienstleistern, dem Information Sharing and Analysis Center (FS-ISAC) der Electronic Payments Association (NACHA) und dem IT-Security-Spezialisten Kyrus zog Microsoft vor das New Yorker Bezirksgericht und organisierte eine Hausdurchsuchung, die am 23. März 2012 in zwei Bürogebäude in den Bundesstaaten Pennsylvania und Illinois von US-Marshals durchgeführt wurde. Dabei wurden mehrere Webserver beschlagnahmt. Sie standen im Verdacht, im Zusammenhang mit einem Zeus Botnetzwerk im Einsatz zu stehen. Damit die Durchsuchung überhaupt möglich war, ging Microsoft neue juristische Wege: In Zusammenarbeit mit Organisationen aus dem Finanzsektor wurde an Stelle eines Strafprozesses, eine Zivilklage gegen die Betreiber des Botnetzes Zeus angestrebt. Die ersten Klagen erhob Microsoft gegen Unbekannt. Dann publizierte Microsoft im Juli zwei Namen, welche mit dem Zeus-Botnetzwerk in Verbindung standen. Yevhen K. und Yuriy K sind bereits in Grossbritannien in Haft.[29]

Der Fokus lag bei diesem Vorgehen nicht bei der Zerstörung des Botnetzes. Ein Botnetz von der Komplexität von Zeus kann man nicht einfach abschalten. Es ging vielmehr darum, den Betreibern dieser Netze Arbeit und Kosten zu bescheren - in der Hoffnung, dass dadurch der Betrieb nicht länger rentabel sei.

Allerdings waren nach der Durchsuchung nicht nur positive Töne zu hören. Beispielsweise hat «FoxIT», ein Sicherheitsdienstleister aus den Niederlanden, eine kritische Analyse über diese Microsoft Operation publiziert.[30]

4.9 DriveBy-Infektionen – Verbreitung über Werbebanner

Über eine Lücke der *OpenX*-Werbebanner Software auf der Website www.wetter.com wurde Mitte Mai 2012 *Schadsoftware* verteilt. Wie lange diese Infektion auf der Seite von wetter.com aktiv war, ist nicht bekannt. Besuchern der Site wurde unter Umständen ohne ihr Wissen *Schadsoftware* installiert. Dem CERT.at ist bekannt, dass es verschiedene Varianten von *Schadsoftware* gab, die darüber verteilt wurde, eine davon war ein *Sperrtrojaner* (*Ran-*

[29] http://www.golem.de/news/botnet-microsoft-nennt-zwei-mutmassliche-betreiber-von-zeus-1207-92930.html (Stand: 31. August 2012).

[30] http://blog.fox-it.com/2012/04/12/critical-analysis-of-microsoft-operation-b71/ (Stand: 31. August 2012).

somware).[31] Siehe zu Sperrtrojanern auch Kapitel 3.5 sowie den MELANI Halbjahresbericht 2011/2, Kapitel 3.5[32].

Webseiteninfektionen sind momentan die meistgenutzten Verbreitungsvektoren für *Schadsoftware*. Dabei kommt den zentralen Servern, welche verschiedenen Webseiten Inhalte zur Verfügung stellen, eine zentrale Rolle zu. Besonders bei Online-Werbung, aber auch bei Statistikdiensten kann eine einzelne Kompromittierung weitreichende Konsequenzen haben. Bei Anbietern von Internetwerbung, aber auch anderer Inhalte, kommt dem Umgang mit der eingesetzten Software eine wichtige Bedeutung zu. Auch hier müssen alle Programme immer auf dem neuesten Stand gehalten werden. Am Ende gilt gerade bei solchen Diensten, dass eine Website nur so sicher sein kann, wie ihr schwächstes Glied. Und dies sind oftmals Angebote Dritter, welche in die Website eingespiesen werden und somit für die Websitebetreiber unkontrollierbar sind.

5 Tendenzen / Ausblick

5.1 Verschmelzung von Firmen und privater IKT – ein Sicherheitsrisiko?

Während früher strikte zwischen Privat- und Arbeitsleben unterschieden wurde, ist diese Grenze heute fliessend: Auf der einen Seite erwarten die Firmen, dass ein Mitarbeiter auch ausserhalb der Bürozeiten erreichbar ist oder bei Termindruck auch am Abend (von zu Hause aus) arbeitet, auf der anderen Seite benutzen Mitarbeiter im Büro die IKT auch zu privaten Zwecken. Sie rufen beispielsweise private E-Mails ab oder pflegen ihre sozialen Netzwerke. Dazu kommt, dass der Ruf nach den modernsten Geräten auch in der Arbeitswelt allgegenwärtig ist. Wieso soll sich ein Mitarbeiter mit einem Firmenmobiltelefon ohne Zusatzfunktionen begnügen, wenn er privat ein hochmodernes *Smartphone* benutzt? Reagiert die Firma nicht, wird der Mitarbeiter früher oder später das private *Smartphone* auch für Firmenaufgaben benutzen oder sonstige Ideen entwickeln, um Arbeitsabläufe mit seinen Wünschen und Bedürfnissen in Einklang zu bringen. Dass dies für IKT-Verantwortliche von Unternehmen eine zusätzliche Herausforderung mit sich bringt, liegt auf der Hand. Werden Computer nicht mehr nur im (kontrollierten) Firmennetzwerk verwendet, sondern auch ausserhalb des Arbeitsplatzes, birgt dies neue Gefahren.

Zusätzliche Gefahren birgt der Datenaustausch beispielsweise via *USB-Stick* oder CD zwischen privaten- und Firmencomputern. Wie die Erfahrung zeigt, werden *USB-Sticks* von Angreifern sehr gerne als Übertragungsweg für gezielte Angriffe genutzt, um in Firmennetzwerke zu gelangen. Der Angreifer infiziert demnach den (schlecht geschützten) privaten Computer eines Mitarbeiters und schlüpft dann mittels externem Speichermedium völlig unbemerkt auf den Firmencomputer. Dabei kommt erschwerend hinzu, dass sich - bei einem Vorfall auf einem privaten Computer - die Nachforschungen sehr viel schwieriger gestalten, da eine genormte Aufzeichnung der Computer- und Netzwerkaktivitäten typischerweise fehlt. Hat man beispielsweise bei gezielten *Schadsoftware*-Angriffen via Firmen E-Mail noch die Möglichkeit einer nachträglichen Überprüfung, ob die E-Mail überhaupt angekommen und geöffnet wurde, fällt diese Möglichkeit in privaten Netzwerken meist weg.

---

[31] http://www.cert.at/warnings/all/20120516.html (Stand: 31. August 2012).

[32] Siehe: MELANI Halbjahresbericht 2011/2, Kapitel 3.5: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012).

Diese Entwicklung zeigt exemplarisch, wie wichtig ein integraler Sicherheitsansatz ist. So stellen sich nicht nur die klassischen IKT-Sicherheitsfragen, sondern vielmehr organisatorische Fragen: Wer hat Zugriff auf welche Daten? Wissen die Mitarbeitenden, welche Daten aus dem Firmennetz genommen werden dürfen? Welche Geräte dürfen in die Firma genommen werden und auch dort angeschlossen werden. Reicht es in den Sicherheitszonen, die USB Ports zu sperren oder müssen auch Handycams verboten werden? Es stellt sich generell die Frage, ob Arbeitsgeräte nicht relativ breit abgegeben und mit weitgehenden Rechten auch für die private Nutzung ausgestattet werden sollten. Auch wenn dies unter anderem zu höheren administrativen Aufwendungen in einem Unternehmen führt, ist zumindest die Kontrolle über die Geräte und die darauf laufenden Applikationen gewährleistet, da diese noch immer dem Arbeitgeber gehören und seiner Kontrolle unterliegen.

Technische Sicherheitsmechanismen sind zwar unverzichtbar, können aber keinen 100%igen Schutz bieten. Vom ausschliesslichen Schutz der Computer und Netzwerke, auf denen die Informationen lagern, muss abgesehen und der Fokus auf den Informationsschutz gelegt werden. Dies wird ein verstärktes Informations- und Datenmanagement, Informationsklassifizierung und dergleichen nach sich ziehen. Zudem wird eine klare Risikoabwägung vorausgesetzt, die dazu führen muss, dass die Sicherheit von Verteil-Kanälen, Zugriffsrechten und Speicherorten dem tatsächlichen Wert einer Information angepasst werden. Nicht jeder Kanal oder Speicherort ist gleich sicher und nicht alle Dokumente sind in einem Betrieb gleich sensibel. In vielen Fällen wird die IKT prinzipiell als Kostenfaktor verstanden und entsprechend seitens der Geschäftsleitung als reine Logistik- und Supportfunktion betrachtet. Die IKT - als Teil des Informationssicherungsprozesses - muss jedoch zwingend auf Grund ihrer kritischen Faktoren in den geschäftlichen und strategischen Risikomanagement-Prozess eingebunden werden. Damit gehört auch die Informationssicherung zu einem integralen Bestandteil des strategischen Risikomanagements und Sicherheitskonzeptes und somit auf die gleiche strategische Stufe, wie Gebäude- und Personenschutz, Finanzcontrolling etc.

5.2 Cyberkonflikt in Nahost

Mit dem Beginn des arabischen Frühlings und dem Fall der ersten Regierungen kamen auch Dokumente und Hinweise an die Öffentlichkeit, die belegten, dass einzelne arabische Staaten zur Internetüberwachungen ihrer Regimekritiker hochwertige Technologien aus dem Westen einsetzten. Auch diejenigen Staaten, in denen keine oder weniger heftige Unruhen ausbrachen, sollen Programme und Infrastrukturen zur möglichst flächendeckenden Kommunikationsüberwachung einsetzen. Das Geschäft mit solchen IKT-Lösungen boomt und wie im Halbjahresbericht 2011/2[33] bereits beschrieben, handelt es sich dabei um eine komplexe Problematik, die keine einfache Schwarz-Weiss-Sicht zulässt. Verschiedene Vorkommnisse in den diversen Krisen- und Konfliktherden im Nahen Osten zeigen aber auf, dass im Bereich der IKT-Mittel aber ein noch sehr viel breiteres Feld an Akteuren und Mittel existiert, das weit über die Kommunikationsüberwachung hinausgeht:
So bewies das Schadprogramm «Stuxnet» und seine Nebenmodule eindrücklich die Effektivität IKT-basierter Mittel, wenn sie mit genügend Ressourcen und staatlicher Deckung entwickelt und zur Sabotage oder Spionage eingesetzt werden. Wie in Kapitel 4.2 beschrieben, beteiligen sich auch nicht-staatliche Gruppierungen virtuell an den Auseinandersetzungen im Nahen Osten. Dabei ist schwer abzuschätzen, wer genau hinter diesen Protestbewegungen

[33] Siehe: MELANI Halbjahresbericht 2011/2, Kapitel 5.3: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 31. August 2012).

steckt, inwiefern sie nicht doch mehr als nur ideologisch vom Staat unterstützt werden und wie sie sich gegenseitig zu Aktionen aufschaukeln. Sie bedienen sich dabei der ganzen Palette vom Datenklau, über Angriffe auf die Verfügbarkeit von Webseiten bis zu den allseits beliebten virtuellen Schmierereien, den so genannten Defacements. Aber auch auf der organisatorischen und propagandistischen Seite bedient man sich der Vorzüge des Internet. So organisieren sich Aktivisten jeglicher Herkunft über Facebook, Twitter und dergleichen, oder stellen Handy-Videos und Fotos zur Untermauerungen ihrer jeweiligen Aussagen und Forderungen aufs Netz, wobei der reale Kontext kaum umfassend beweiskräftig nachvollzogen werden kann.

Dementsprechend ist es keine Überraschung, dass in verschiedenster Form versucht wird, nicht nur gegnerische E-Mail-Konten, sondern auch Gruppen in Sozialen Netzwerken zu infiltrieren, um Angaben über geplante Aktivitäten und die Identität beteiligter Personen sowie weitere nützliche Informationen zu beschaffen: Schon vor dem arabischen Frühling wurden beispielsweise Aktionen bekannt, bei denen im Ausland lebende Regimekritiker gezielt mit IKT-Angriffen eingedeckt wurden. Aber auch Mitglieder von autoritären Regimes und deren Angehörige können durch Aktivisten oder ausländische Nachrichtendienste behelligt werden, wie das Beispiel der Veröffentlichung der iTunes-Einkäufe von Bashar al-Assad zeigt.[34]

Der steigende Bedarf an (zentralen) Überwachungstechnologien, IKT-Sabotage, den Einsatz von propagandistischem Bildmaterial bis hin zur Diskreditierung einzelner Personen auf Grund gestohlener, persönlicher E-Mails sind ein Ausfluss des Einsatzes aller verfügbaren IKT-Mittel und -Methoden durch die eine oder andere Partei in einer seit jeher angespannten und instabilen Region.

Nicht erst seit dem arabischen Frühling ist der Nahe Osten von Unruhen, Krisen und unterschiedlichstem Konfliktpotenzial durchzogen. Mit dem Ausbruch von Demonstrationen und Unruhen traten einige dieser unterschwelligen Konflikte in ein neues Stadium ein, oder alte bis anhin unter dem Deckel gehaltene Schwierigkeiten traten nun an die Öffentlichkeit. Nicht erst seit diesen Vorfällen und Entladungen wird auch im Nahen Osten IKT eingesetzt, sei es zur Kommunikation, zur (zentralen) Überwachung genau dieser oder aber im Bereich der *SCADA*-Systeme und zur Unterstützung von Produktions- und Geschäftsprozessen. Mit den offenen ausgetragenen Konflikten seit Beginn des arabischen Frühlings nimmt denn auch der aggressive und offensive Einsatz der IKT-Mittel und des Internets zu.

Regelmässig werden Fälle bekannt, in denen Webseiten zum Erliegen gebracht, staatliche oder private Dokumente entwendet und veröffentlicht oder Malware zur Sabotage eingesetzt wurde. Ganz abgesehen von der Flutung diverser Web 2.0-Dienste mit Meldungen, Videos und Informationsbruchstücken zur scheinbaren Lage vor Ort - wobei sich beide Konfliktparteien dieser Technik bedienen und eine Verifizierung und Nachvollziehbarkeit oft unmöglich ist. Verschärfend kommt dazu, dass IKT-basierte Mittel oft relativ billig sind, eine hohe Reichweite entfalten und somit attraktiv für alle Beteiligten sind.

Insofern ist der auf mehreren Ebenen ausgetragene Cyber-Konflikt im Nahen Osten in erster Linie eine Begleiterscheinung der realen Auseinandersetzungen und Realitäten vor Ort. So müssen denn auch Vorfälle in diesem Bereich und Zusammenhang nicht als Einzelereignisse verstanden und aufgefasst werden, als die sie medial gerne präsentiert werden, sondern gehören immer in einen Gesamtkontext eingebettet, der es erlaubt, eine umfassende Einschätzung des Gezeigten, Vorgefallenen und Vermeldeten vorzunehmen.

[34] http://www.guardian.co.uk/world/2012/mar/14/assad-itunes-emails-chris-brown (Stand: 31. August 2012).

5.3 Datendiebstahl: Angriffe auf viele kleine und wenige grosse Unternehmen

Immer wieder machen Angriffe auf Kundendaten von Grossfirmen und hier insbesondere auf Kreditkartendaten Schlagzeilen. Neben den aktuellen Ereignissen in Kapitel 4.5 sei an die zahlreichen Angriffe in der Vergangenheit erinnert: Beispielsweise an den Verlust von Kundendaten bei Sony im vergangenen Jahr, an den Vorfall bei der angloamerikanischen Kaufhauskette TJX im Jahre 2005, bei dem während 1 ½ Jahren systematisch mehr als 45 Millionen Kreditkartendatensätze gestohlen wurden oder an den Vorfall beim Kreditkartenverarbeiter Heartland im Jahre 2009.

Eine Studie des amerikanisches Sicherheitsunternehmen Verizon[35] mit Daten vom US Secret Service, der Australischen-, Niederländischen- und Irischen-Polizei aus dem Jahr 2011 hat jedoch gezeigt, dass Angriffe auf Grossfirmen nur einen kleinen Teil ausmachen. Von den 855 gemeldeten Vorfällen mit insgesamt 174 Millionen kompromittierten Datensätzen, betraf nur der kleinste Teil der Vorfälle grosse Unternehmen. Den zugegebenermassen zum Teil sehr spektakulären Fällen, stehen zahlreiche Angriffe auf kleinere Firmen und deren Daten gegenüber, die unter dem Radar der Medien tagtäglich passieren. Bei mehr als 75% handelt es sich um Angriffe auf KMUs mit einer Mitarbeiterzahl von unter 1000.

Während sich grosse Firmen gut auf Cyberrisiken vorbereiten und in den meisten Fällen ein IKT-Security Team und auch einen CSO haben, fehlt diese Sensibilität bei vielen kleineren Unternehmen noch. Viele Firmen gehen immer noch sehr unsensibel mit Kunden- und Kreditkartendaten um. Was nützt zum Beispiel eine sichere Übertragung bei der Bestellung über https, wenn die Daten anschliessend unverschlüsselt auf dem Computer abgespeichert werden?

Dies nutzt ein Teil der Kriminellen gnadenlos aus, da sie nach dem Prinzip des geringsten Widerstandes operieren und sich die «einfachsten» Ziele aussuchen. Dabei werden vielfach automatisierte Angriffsmethoden angewendet und systematisch nach bekannten Schwachstellen und Fehlkonfigurationen in Webseiten oder Datenbanken gesucht, um anschliessend die Daten zu stehlen. Es kann für die Kriminellen also durchaus ertragsreicher sein, anstelle eines grossen Unternehmens, viele verschiedene kleine Firmen mit geringerem Aufwand, aber auch geringerem Ertrag - sprich weniger Datensätzen - anzugreifen.

Grossfirmen sollten sich aber nicht auf der sicheren Seite wiegen. Für einige Kriminelle mit grösserem technischen Know How und guten Fähigkeiten, kann sich auch ein grosser Aufwand über längere Zeit lohnen. Im Bereich der Spionage hat sich hierbei der Begriff *Advanced Persistent Threat* (APT) eingebürgert und wird hauptsächlich für staatliche Akteure ohne direkten finanziellen Nutzen verwendet. Wenn der Ertrag am Schluss stimmt, kann sich aber auch ein gezielter, hochprofessioneller und über Monate vorbereiteter Angriff für Kriminelle lohnen. Im Gegensatz zur staatlichen Spionage steht hier jedoch die finanzielle Absicht im Zentrum.

5.4 Kundenkommunikation im Zeitalter von Phishing

«Keine seriöse Firma wird sie je per E-Mail nach Login und Passwörtern fragen.» Das ist die Standard-Antwort, die MELANI jeweils gibt, wenn Personen eine E-Mail melden, bei dem sie

[35] http://securityblog.verizonbusiness.com/category/ask-the-data/ (Stand: 31. August 2012).

sich nicht sicher sind, ob diese nun tatsächlich von der besagten Firma stammt oder nicht. Diese Aussage, die zunächst einfach klingt, stellt die Firmen im Zeitalter der elektronischen Kundenkommunikation aber manchmal vor gewisse Herausforderungen. Wie soll eine Firma mit den Kunden kommunizieren, damit diese die E-Mail nicht als betrügerische E-Mail auffassen. Und noch wichtiger: Eine allzu sorglose Kundenkommunikation durch eine Firma kann auch das Kundenverhalten bezüglich betrügerischen E-Mails negativ beeinflussen.

e-Bay Kundenverifikation

Ein Beispiel, welches exemplarisch aufzeigt in welchem Dilemma Firmen stecken, zeigt nachfolgendes Beispiel:
eBay versendet sporadisch E-Mails zur Mitgliederüberprüfung, wenn über längere Zeit nicht in das Benutzerkonto eingeloggt wurde. Es ist klar, dass dies ein notweniger Vorgang ist, da sich ansonsten über die Jahre viele unbenutzte Konten bei eBay ansammeln würden. Obschon nicht direkt zur Angabe von Benutzername und Passwort aufgefordert wird, erzeugt die E-Mail bei manchem sensiblen Empfänger sofort eine gewisse Skepsis, insbesondere wenn, wie in diesem Fall, das Kundenkonto erst kürzlich für eine Auktion verwendet wurde.

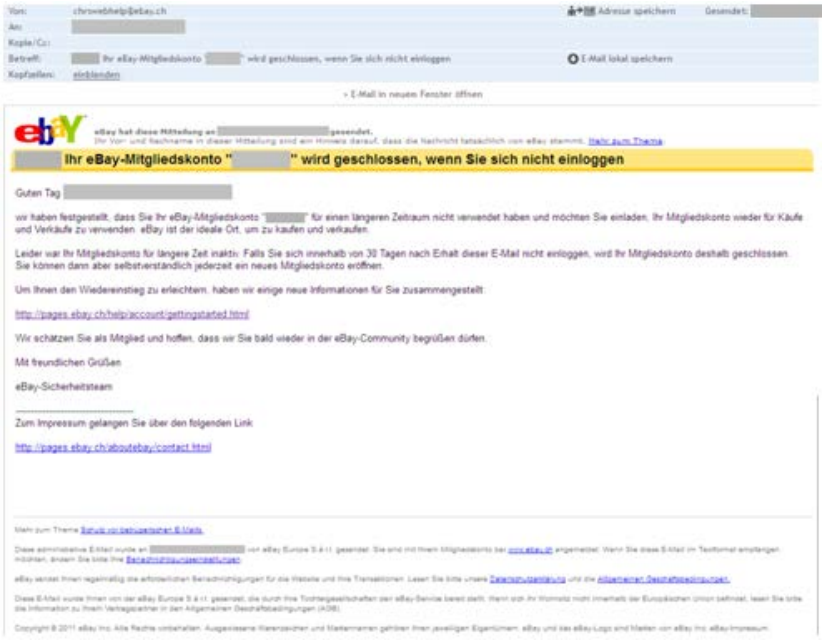

Von: chrowebhelp@eBay.ch
An:
Kopie/Cc:
Betreff: Ihr eBay-Mitgliedskonto wird geschlossen, wenn Sie sich nicht einloggen
Kopfzeilen: einblenden
Adresse speichern
Gesendet:
E-Mail lokal speichern
E-Mail in neuem Fenster öffnen
eBay hat diese Mitteilung an gesendet.
Ihr eBay-Mitgliedskonto " " wird geschlossen, wenn Sie sich nicht einloggen
Guten Tag
wir haben festgestellt, dass Sie Ihr eBay-Mitgliedskonto " " für einen längeren Zeitraum nicht verwendet haben und möchten Sie einladen. Ihr Mitgliedskonto wieder für Käufe und Verkäufe zu verwenden. eBay ist der ideale Ort, um zu kaufen und verkaufen.
Leider war Ihr Mitgliedskonto für längere Zeit inaktiv. Falls Sie sich innerhalb von 30 Tagen nach Erhalt dieser E-Mail nicht einloggen, wird Ihr Mitgliedskonto deshalb geschlossen. Sie können dann aber selbstverständlich jederzeit ein neues Mitgliedskonto eröffnen.
Um Ihnen den Wiedereinstieg zu erleichtern, haben wir einige neue Informationen für Sie zusammengestellt:
http://pages.ebay.ch/help/account/gettingstarted.html
Wir schätzen Sie als Mitglied und hoffen, dass wir Sie bald wieder in der eBay-Community begrüßen dürfen.
Mit freundlichen Grüßen
eBay-Sicherheitsteam
Zum Impressum gelangen Sie über den folgenden Link:
http://pages.ebay.ch/aboutebay/contact.html

Bild 8: E-Mail von e-Bay zwecks Kundenüberprüfung

AGB-Änderung bei Paypal

Ein anderer Fall, der ebenfalls zu Meldungen bei MELANI geführt hat, war eine AGB-Änderung, die von Paypal Ende Juni per E-Mail versendet worden ist. Trotz der Tatsache, dass in der E-Mail kein Link zu einer Loginseite vorhanden war, erzeugte allein die Tatsache, dass das Nutzer unerwartet ein E-Mail von Paypal erhalten haben, eine gewisse Verunsicherung.

Newsletter von Schweiztourismus

Ebenso Anfragen bei MELANI erzeugt hat eine E-Mail von Schweiztourismus, die am 31. Mai 2012 versendet worden ist. Die darin enthaltenen Links verweisen nicht auf die Domäne von Schweiztourismus sondern auf einen anderen Schweizer Server namens «crm.stnet.ch». Die Links waren zudem sehr kompliziert und lange, was Empfänger dazu bewogen hat, bei MELANI die Richtigkeit dieser E-Mail verifizieren zu lassen.

Betreff: Mit allen Wassern gewaschen

Falls der Newsletter nicht korrekt dargestellt wird, klicken Sie hier <http://crm.stnet.ch/crm/service/nlweb?bpid=[redacted]language=de&chk=iSXRD6ASZf> .

<http://crm.stnet.ch/content/campaign_data/content_804302666/Headerde.jpg>
<http://crm.stnet.ch/content/campaign_data/content_980099386/Mainimage.jpg>
<http://crm.stnet.ch/content/campaign_data/content_804302666/juerg-foto-Sommer.jpg>

Grüezi [redacted]

Freuen Sie sich auf Ferien, die prickeln. Unser Reiseland steht diesen Sommer ganz im Zeichen des Wassers. Spri
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Fempfehlungen%2Fstaedtereisen
3D47010&[redacted]-1&chk=3fJxLXXDLW&ganame=Newsletter+05%2F2012_CHdefr> oder geheimnisvo
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%2Fde%2Ferlebnisse%2Fwandern.html%3F
3D25527&[redacted]&chk=6VAZSFLJaD&ganame=Newsletter+05%2F2012_CHdefr> in einer atember
haben für Sie das Beste herausgepickt.

Finden Sie uns im Netz

<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.facebook.com%2FMySwitzerland&bpid=[redacted]
<http://crm.stnet.ch/crm/service/rdc?rtg=http%3A%2F%2Fwww.myswitzerland.com%
2Ftwitter&[redacted]&lid=4&chk=D6xD9RVRAR&ganame=Newsletter+05%2F2012_CHdefr> <http://crm.
2Fwww.youtube.com%2Fmyswitzerland&[redacted]&lid=5&chk=2DeDD32Te2> <http://crm.stnet.ch/cr
2Fwww.flickr.com%2Fphotos%2Fswitzerland_tourism%2F&b[redacted]lid=6&chk=XXWJhOFADF>
Viel Genussreiches wartet auf Sie. Lassen Sie sich erfrischen von unseren Ideen rund ums Element Wasser!

<http://crm.stnet.ch/content/campaign_data/content_804302666/Juerg.gif>

Jürg Schmid, Direktor Schweiz Tourismus

Bild 9: Werbe E-Mail von Schweiztourismus mit Links auf die Domäne stnet.ch

Neueinschreibung MELANI-Newsletter

Auch MELANI ist vor solchen Problemen nicht gefeit. Da der MELANI-Newsletter im Juni 2012 auf das Informationsportal des Bundes migriert wurde und es aus technischen Gründen nicht möglich war, die Datenbank mit allen eingeschriebenen E-Mail-Adressen zu transferieren, mussten sämtliche MELANI-Newsletter-Abonnenten informiert werden, dass bei weiterem Interesse an den MELANI-Newslettern eine Neueinschreibung erforderlich ist.

Ein solches Unterfangen ist schwierig und muss gut geplant werden. MELANI hat versucht dieses Problem zu lösen, indem der Vorgang in einem vorangegangenen E-Mail angekündigt und der genaue Zeitpunkt des E-Mail-Versandes definiert wurde. Die E-Mail wurde in reinem Textformat versendet und enthielt nur einen Link, der analog zu den früheren Newslettern auch zur MELANI-Domäne führte. Neuabonnenten wurden zu keiner Zeit aufgefordert, ihr Passwort einzugeben (aber ein neues zu wählen). Auf der Startseite der MELANI-Webseite wurde zudem deutlich auf den Versand hingewiesen. Trotz dieser Vorgehensweise blieben Reaktionen nicht aus – hielten sich aber trotzdem in Grenzen. Eine schnelle Reaktionszeit bei Fragen von Kunden während und nach dem Newsletter-Versand ist ebenfalls ein nützliches Instrument, um die Verunsicherung klein zu halten. Trotzdem gab es auch in diesem Fall Verbesserungspotential, wie beispielsweise die Verwendung eines Links in der E-Mail auf eine verschlüsselte Seite (https).

Folgende Punkte sollten beim Versand von Newslettern beachtet werden:

- Mails, wenn möglich im Textformat versenden.
- Newsletter-E-Mails möglichst regelmässig versenden.
- Mit Links in der E-Mail sparsam umgehen und nur auf die eigene Domäne verlinken. Wenn möglich Links auf verschlüsselte Seiten (https) benutzen und dies dem Empfänger auch mitteilen.
- Nicht auf Webseiten verlinken, die Benutzername und Passwort oder andere Daten verlangen.
- Auf der Startseite des Webauftrittes auf den Newsletter hinweisen oder die Information direkt verlinken, damit der Empfänger die Möglichkeit hat, die Hauptadresse manuell einzugeben und dann den Newsletter von dort anzuklicken.
- Kunden, mit Vor- und Nachnamen anschreiben, sofern diese Information vorhanden ist.

5.5 E-Voting in der Schweiz – Bisherige Erfahrungen

Im Jahr 2000 wurde das Projekt „Vote électronique“ – also die Möglichkeit der elektronischen Stimmabgabe – in der Schweiz gestartet.

Der erste Pilotversuch erfolgte 2003 in einer kleinen Gemeinde im Kanton Genf, wo eine überschaubare Zahl von Stimmbürgerinnen und Stimmbürgern die Möglichkeit hatte, bei Abstimmungen auf Gemeindeebene ihre Stimme elektronisch abzugeben. Dieser erste Pilotversuch warf international hohe Wogen und fand entsprechende Erwähnung in renommierten Zeitungen im In- und Ausland.

Seit diesem ersten Versuch hat der Bundesrat über hundert Versuche anlässlich eidgenössischer Volksabstimmungen bewilligt. Anlässlich der eidgenössischen Volksabstimmung vom 25. November 2012 soll der 115. Versuch mit der elektronischen Stimmabgabe durchgeführt werden. Zählt man jedoch die zahlreichen weiteren Versuche auf kommunaler und kantonaler Ebene sowie diverse Versuche anlässlich von Wahlen dazu, ist die Zahl der in der Schweiz mit E-Voting durchgeführten Versuche massiv höher.

Trotz dieser grossen Anzahl an Versuchen wurden bisher nur kleinere Zwischenfälle mit geringer Auswirkung (siehe das Beispiel in Kapitel 3.7) bekannt. Ist das Schweizer E-Voting aber tatsächlich so sicher? Folgende kurze Analyse soll dieser Frage nachgehen:

Zur Zeit darf nur eine beschränkte Anzahl von Schweizer Stimmberechtigten die elektronische Stimmabgabe nutzen. Inzwischen wurde die Berechtigung zwar auf die Auslandschweizerinnen und –schweizer ausgedehnt. Trotzdem ist es momentan aus mehreren Gründen unwahrscheinlich, dass ein fehlerhafter Versuch mit Vote électronique das Endergebnis beeinträchtigen würde:

1. Die Grösse des Elektorats ist so gewählt, dass auch bei knappen Resultaten davon ausgegangen werden kann, dass ein Teil- oder Totalausfall des elektronischen Systems mit grosser Wahrscheinlichkeit keinen Einfluss auf das Endresultat hätte. Zur Zeit machen hauptsächlich Auslandschweizerinnen und –schweizer von der elektronischen Stimmabgabe Gebrauch.

2. Die elektronischen Urnen müssen immer am Samstag vor dem Abstimmungssonntag geschlossen werden. Diese Massnahme soll ermöglichen, dass beispielsweise bei einem Totalausfall der elektronischen Systeme (z.B. infolge eines landesweiten Zusammenbruchs der Internetverbindungen oder einer erfolgreichen *DDoS*-Attacke) für die Stimmberechtigten die Möglichkeit bestünde, ihre Stimme physisch in einem der Stimmlokale abzugeben.

Neben diesen organisatorischen Massnahmen existiert eine ganze Reihe von technischen Massnahmen, die sicherstellen sollen, dass die im «Bundesgesetz über die Politischen Rechte» sowie in der «Verordnung über die Politischen Rechte» verankerten Grundsätze (Einmaligkeit der Stimmabgabe, Anonymität der Stimmabgabe, Vertraulichkeit der Stimmabgabe) gewährleistet sind.

Doch wie sieht es aus, wenn ein Grossteil der Bevölkerung diese Dienstleistung nutzt? Insbesondere beim flächendeckenden Einsatz von E-Voting in der ganzen Schweiz funktionieren die obenstehenden Massnahmen nicht mehr oder nur noch eingeschränkt:

- Ein Angriff auf die elektronische Urne ist sicherlich unwahrscheinlich: Hier werden die abgegebenen Stimmen bis zu ihrer Auszählung verschlüsselt aufbewahrt. Die relativ kurze Zeit, in der die elektronische Stimmabgabe möglich ist, dürfte auch unter Einsatz einer massiven *Brute Force*-Attacke nicht ausreichen, um die Stimmen rechtzei-

tig zu entschlüsseln und zu verfälschen. Selbst ein erfolgreicher Angriff würde wahrscheinlich nicht zur Beeinflussung des Abstimmungsresultats führen: Die bestehenden Limiten (maximal 10% des eidgenössischen Elektorats dürfen elektronisch abstimmen) sind so ausgerichtet, dass das Endresultat selbst bei einem Totalausfall von E-Voting resp. der Manipulation der elektronischen Stimmen nicht beeinträchtigt würde.

- Trotzdem kann selbstverständlich nicht ausgeschlossen werden, dass irgendwann ein Angriff auf eines der Vote électronique-Systeme erfolgreich sein könnte. Denkbar wäre z.B. eine *DDoS*-Attacke auf die elektronischen Systeme, so dass beispielsweise die Auslandschweizerinnen und –schweizer ihre Stimme nicht mehr rechtzeitig abgeben könnten.

- Das grösste Problem bilden aber sicherlich unsichere Eingabegeräte (Client-Systeme) gekoppelt mit der fehlenden Nachvollziehbar- und Beweisbarkeit. Viele Angriffsmöglichkeiten (-vektoren), die zur Zeit das Internet Banking betreffen, können direkt oder sogar in vereinfachter Form auch auf das E-Voting abzielen. Die im Internet Banking eingesetzten Schutzmassnahmen – Transaktionsauthentifikations- und überwachungsverfahren – greifen hier nicht. Entsprechend ist die Bedrohungslage erheblich und der Client stellt die Achillesferse im E-Voting dar.[36] Ist es gelungen, eine *Schadsoftware* auf dem Computer des Wählers zu installieren, kann diese die abgegebene Stimme nach Belieben manipulieren. Dabei bewirkt der in den Browser eingeführte Schadcode, dass z.B. immer dann, wenn ein Parameterwert «Ja» an den E-Voting-Server gesendet werden soll, dieser Parameterwert noch vor der Verschlüsselung in den Parameterwert «Nein» umgewandelt wird. Der Schadcode kann ebenfalls das vom E-Voting Server zurückgelieferte Sicherheitsbild nach der Entschlüsselung so manipulieren, dass der Stimmberechtigte von der Manipulation nichts bemerkt. Ein solches Angriffsszenario ist insbesondere dann gravierend, wenn es flächendeckend eingesetzt wird und eine grosse Anzahl von Stimmen manipuliert werden kann.[37] Moderne E-Voting Technologien, wie beispielsweise die sogenannte „Verifizierbarkeit“, erlauben es aber, solche Angriffe rechtzeitig zu erkennen.

Die Verifizierbarkeit dient dazu, Manipulationen an Stimmen feststellen zu können. Verändert beispielsweise eine Schadsoftware auf dem Computer eines Wählers eine Stimme, so kann der Wähler die Manipulation mit einem verifizierbaren System bemerken. Die Verifizierbarkeit kann in einem ersten Schritt beispielsweise dadurch umgesetzt werden, dass dem Wähler nach dem Abschicken der Stimme am Bildschirm pro Vorlage (oder Kandidat bei Wahlen) ein Code angezeigt wird. Diesen Code vergleicht er mit seinen persönlichen Codes, die Teil des Stimmmaterials bilden. Da die Codes pro Vorlage (bzw. Kandidat) und Wähler unterschiedlich sind, „weiss“ die Schadsoftware nicht, welchen Code er anzeigen muss, um den Wähler fehlzuleiten.

Der grosse Unterschied zwischen E-Voting und E-Commerce liegt in der Fehlertoleranz der Systeme. Während bei elektronischen Dienstleistungen ein gewisser Prozentsatz an Betrügereien durchaus toleriert und durch die Firmen auch bezahlt wird – Firmen sparen durch den Einsatz von E-Dienstleistungen ja auch Geld – muss das Ergebnis von Abstimmungen und Wahlen unbedingt den Willen des Elektorats widerspiegeln. Alles andere würde das Vertrauen des Bürgers in die Demokratie vermindern.

---

[36] https://www.e-voting-cc.ch/index.php/de/workshops/workshop09/programm09/87 (Stand: 31. August 2012).

[37] http://data.rrb.zh.ch/appl/rrbzhch.nsf/0/C12574C2002FAA1FC1257942004EB439/$file/Evaluation_E-Voting_Z%C3%BCrich.pdf (Stand: 31. August 2012).

Eine Erweiterung des zu Vote électronique zugelassenen Elektorats ist an die Einführung der Verifizierbarkeit zu knüpfen.

6 Glossar

Advanced Persistent Threat (APT)	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
Anhang/Attachment	Ein Dateianhang (engl.: “attachment”) ist eine Datei, die als Anlage an den Text einer E-Mail verschickt wird.
Antiviren Software	Programm, das den Computer vor Viren, Würmern oder Trojanischen Pferden schützt.
Backup	Backup (deutsch: Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Bluetooth	Eine Technologie, die eine drahtlose Kommunikation zwischen zwei Endgeräten ermöglicht und vor allem bei Mobiltelefonen, Laptops, PDAs und Eingabegeräten (z.B. Computermaus) zur Anwendung gelangt.
Brute-Force Angriff	Angriffsmethode bei der einfach alle potenziellen Lösungen/Passwörter durchprobiert werden, bis die/das richtige gefunden ist.
DDoS-Angriff	Denial-of-Service Attacke. Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
DNS	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich verwenden, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
DNS-Amplification-Attack	Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und als Amplifier (Verstärker) benutzt.
DNS-Root Server	Root-Nameserver, kurz Root-Server, sind Server zur Namensauflösung an der Wurzel (Root) vom Domain Name System im Internet. Die Zone der Root-Server umfasst Namen und IP-Adressen al-

	ler Nameserver aller Top-Level-Domains.
Domainname	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.
E-Commerce	Umfassend wird der Begriff E-Commerce im Rahmen der Internetwirtschaft als Elektronischer Handel zusammengefasst.
E-Government	Unter E-Government versteht man die Vereinfachung und Durchführung von Prozessen durch den Einsatz von digitalen Informations- und Kommunikationstechniken zwischen staatlichen, kommunalen und sonstigen behördlichen Institutionen sowie zwischen diesen Institutionen und Bürgern bzw. Unternehmen.
Event Viewer	Programm, das Fehler- und Hinweismeldungen des Windows-Betriebssystems anzeigt.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf Computer – installiert.
Geoportal	Webportal, welches geographische Informationen zur Verfügung stellt.
Hashfunktion	Algorithmus, welcher aus einem beliebigen Text eine immer gleichlange Zahlenfolge generiert. Hashfunktionen werden in drei Bereichen verwendet: - In der Kryptografie. - Bei Datenbanksystemen. Diese verwenden Hashfunktionen, um in grossen Datenbankbeständen effizient zu suchen. - Bei Prüfsummen. Jeder Datei kann ein Hashwert zugeordnet werden. Ein veränderter Hashwert deutet auf eine Manipulation hin.
Hintertür/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.
HTML	HyperText Markup Language. In HTML werden die Webseiten erstellt. Damit lassen sich die Eigenschaften der Webseiten (z.B. der Seitenauf-

	bau, das Layout, die Links auf andere Seiten, usw.) vorgeben. Da HTML aus ASCII-Zeichen besteht, kann eine HTML-Seite mit einem gewöhnlichen Textverarbeitungsprogramm bearbeitet werden.
Internet-Archivierungsmaschine	Internetdienst, welcher von allen/vielen Webseiten im Internet in gewissen Zeitabständen eine archiviert und diese dann zur Verfügung stellt. Alte nicht mehr erreichbare Webseiten sind damit immer noch sichtbar.
IP-Nummer	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
OpenX	OpenX ist eine Open-Source Software, welche ein Werbebanner Management zur Verfügung stellt.
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
PHP-Mailer	PHP-Programm, welches Text mittels einer E-Mail Funktion versendet. PHP ist eine Skriptsprache, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird.
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Recovery Prozess	Recovery (deutsch: Datenwiederherstellung) bedeutet die Wiederherstellung von Originaldaten nach einem Datenverlust.
Remote Access	Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar.

SCADA	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Schadsoftware	Programm, das auf einem Computer Schaden anrichtet.
SHA	Secure Hash Algorithm. (engl. für sicherer Hash-Algorithmus), Der Begriff SHA bezeichnet eine Gruppe standardisierter kryptologischer Hash-Funktionen. Diese dienen zur Berechnung eines eindeutigen Prüfwerts für beliebige elektronische Daten.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
Sperrtrojaner	Malware, die eine Sperrung des Computer bewirkt und anschliessend vom Besitzer ein Lösegeld fordert.
Spoofing	Spoofing (deutsch: Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.
SQL-Injections	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.
Strafverfolgungstrojaner	Software, welche von der Polizei im Zuge einer Strafuntersuchung verwendet wird, um beispielsweise VoIP-Gespräche abzuhören.
Top Level Domain	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
URL	Uniform Resource Locator. Die Web-Adresse eines Dokuments bestehend aus Protokoll, Server-Name, sowie Dateiname mit Pfad (Beispiel:

	http://www.melani.admin.ch/test.html).
USB-Sticks	Kleine Datenspeichergeräte, die über die USB-Schnittstelle an einen Rechner angeschlossen werden.
Voice Phishing	Betrugsart, bei welcher ein Opfer mittels Telefongespräch dazu verleitet wird, seine Zugangsdaten preiszugeben.
WiFi/WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Zertifikat	Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.