Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

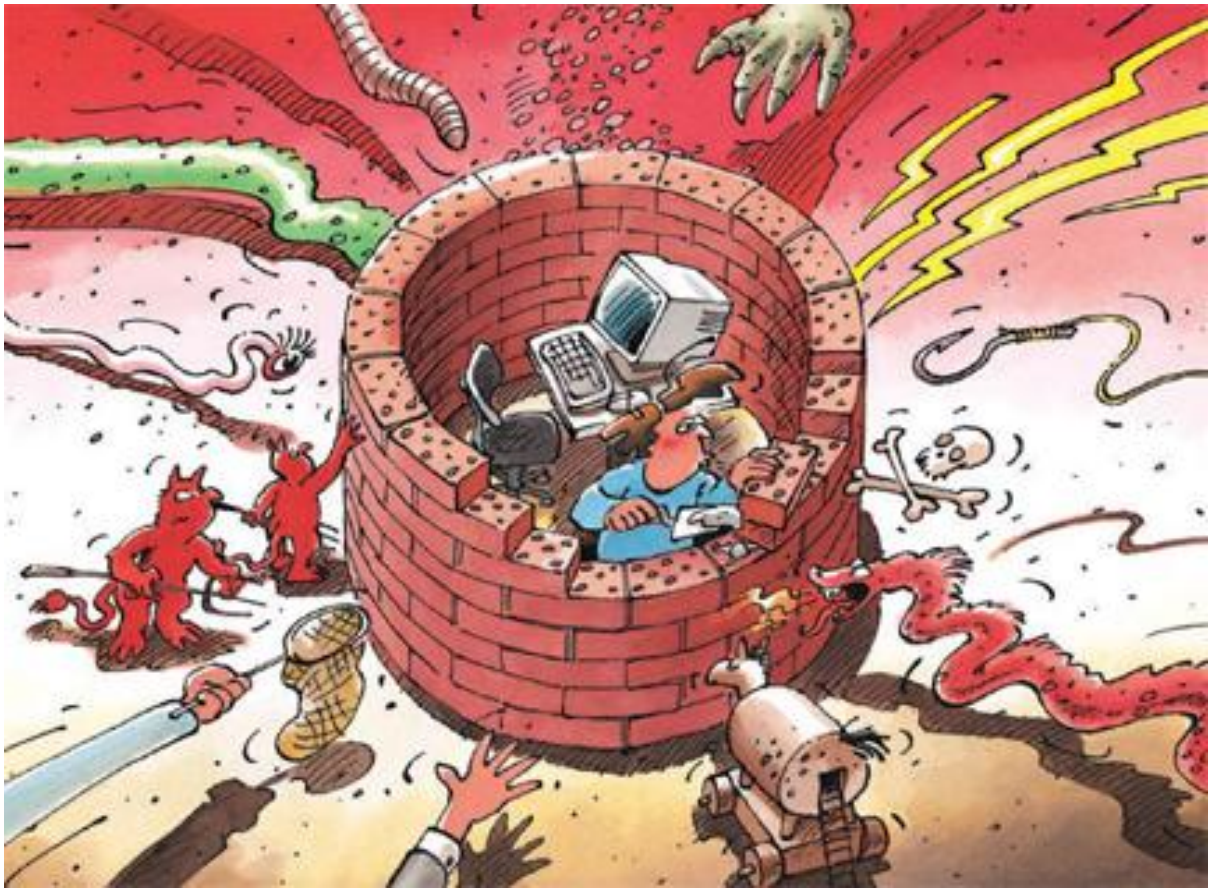
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2011/II (Juli – Dezember)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2011/II

- **Angriffe auf Anbieter von Zertifizierungsdiensten und deren Auswirkungen**

  Bei einem Angriff auf DigiNotar, eine niederländische Zertifizierungsstelle, wurden missbräuchlich über 530 Zertifikate ausgestellt, darunter für die Domäne windowsupdate.com, welche die Update Funktion aller Windowsprodukte von Microsoft beherbergt und verschiedene Google-Domänen.

  ► Aktuelle Lage International: Kapitel 4.1
  ► Tendenzen / Ausblick: Kapitel 5.5

- **Cyberaktivismus**

  «Anonymous» hat in den vergangenen Monaten wiederum mit diversen Operationen im Cyberspace für Medieninteresse gesorgt. Doch wer steckt eigentlich genau hinter «Anonymous»? Gemäss verschiedenster Aussagen ist «Anonymous» keine eigentliche Organisation, sondern eher eine Lebenseinstellung. Die Unterstützung ist an keine Form gebunden: Jede Aktivistin und jeder Aktivist macht, was sie oder er für richtig hält. Dies kann mitunter auch zu Aktionen führen, die von breiten Kreisen in der Bewegung keine Unterstützung erfahren und so widersprüchliche Aussagen provozieren.

  ► Aktuelle Lage International: Kapitel 4.3
  ► Tendenzen / Ausblick: Kapitel 5.2

- **«Gute» und «Böse» Überwachung im Internet**

  Mit der Analyse des deutschen Strafverfolgungstrojaners (häufig undifferenziert als «Bundestrojaner» bezeichnet) durch den «Chaos Computer Club» wurden die Diskussionen rund um dessen Einsatz nicht nur in Deutschland, sondern auch in der Schweiz entfacht. Zudem begann WikiLeaks am 1. Dezember 2011 mit der Publikation zahlreicher Dokumente, die darlegen sollen, dass private Sicherheitsunternehmen IKT-Lösungen an Staaten mit vorwiegend autokratischen Regierungen und mangelndem Menschenrechtsbewusstsein verkaufen. Diese an sich alte Diskussion, welche neu lanciert wurde, liegt eines der fundamentalen Probleme des Internet, der vernetzten Gesellschaft und der IKT zu Grunde. Das Aufkommen immer neuer Möglichkeiten zu kommunizieren, Daten und Informationen auszutauschen und diese stets überall und jederzeit verfügbar zu haben, hat Folgen: Die Massnahmen zur Ortung und Beschaffung von Informationen und ganz generell die Arbeit der Sicherheitsbehörden eines Staates werden dadurch komplizierter.

  ► Aktuelle Lage International: Kapitel 4.7, Kapitel 4.8
  ► Tendenzen / Ausblick: Kapitel 5.3

- **Phishing, Betrug und Ransomware im Aufwind**

  Ein neues Phänomen, dass in der Schweiz seit Sommer 2011 beobachtet wird, sind Anrufe von Betrügern, die sich als Mitarbeitende des Microsoft-Kundenservice ausgeben und sich so Zugriff auf den Computer verschaffen wollen. Auch hat Phishing in den vergangen 6 Monaten stark zugenommen und richtet sich vor allem gegen E-Mail Provider und Kreditkartenfirmen. Um betrügerische Webseiten möglichst lange aktiv zu halten, versuchen Kriminelle neue Methoden, die das Abschalten von Phishingseiten erschweren sollen. Anfang November verbreitete sich erpresserische Schadsoftware (Ransomware), welche vorgibt, vom Eidgenössischen Justiz- und Polizeidepartement zu stammen.

  ► Aktuelle Lage Schweiz: Kapitel 3.1, 3.2, 3.3, 3.4, 3.5

2 Einleitung

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

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

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

Kapitel 5 enthält vertiefte Analysen und Trends zu aktuellen Themen.

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Anrufe von Betrügern, die sich als Mitarbeitende des Microsoft-Kundenservice ausgeben

In letzter Zeit häufen sich weltweit, auch in der Schweiz, Anrufe von Betrügern, welche sich als Mitarbeitende von Microsoft oder anderen IKT-Support-Firmen ausgeben. Die Anrufer sprechen meist englisch und stammen nach eigenen Angaben aus den USA, England oder Australien. In vielen Fällen weisen die Anrufer auf Fehlermeldungen hin, die angeblich von den Computern des angegangenen Unternehmens oder der Privatperson übermittelt worden sind. Die Angerufenen werden dann zum Beispiel angeleitet, auf ihrem Computer den *Event-Viewer*[1] aufzurufen, mit welchem jegliche Ereignisse und Aktivitäten des Computers 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 sogar sehr lang 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, ihnen durch das Herunterladen eines Programms einen Fern-Zugriff auf den Computer zu erlauben. Wird dieser gewährt, hat der Anrufer dieselben Möglichkeiten, den Computer zu manipulieren, wie wenn er selbst direkt davor sitzen würde (Kopieren/Verändern/Löschen von Daten, Installation von Programmen, Einrichten einer «*Hintertür*» um später wieder auf das System Zugreifen zu können, etc.).

Manchmal bieten die Anrufer auch den Abschluss eines Support-Abonnements respektive einer Garantie an und verlangen dafür die Angabe von Kreditkartendaten oder eine andere Form von Bezahlung.

Die Opfer suchen sich die Anrufer offensichtlich über öffentlich zugängliche Verzeichnisse aus, wie beispielsweise das Schweizerische Handelsregister oder öffentliche Telefonbücher.

Grundsätzlich ist festzuhalten, dass Microsoft nie unangemeldete oder unaufgefordert Support-Anrufe tätigt, um Computerprobleme zu beheben. Mehr zu diesem Thema findet sich auch auf dem *Blog* des Sicherheitsberaters von Microsoft Schweiz.[2]

Wurde den Anrufern tatsächlich Zugang zum Computer gewährt, ist es empfehlenswert, den Computer von einer Fachperson untersuchen und gegebenenfalls säubern zu lassen. Dies garantiert jedoch auch nicht, dass eine allfällige *Schadsoftware* gefunden wird, respektive vorgenommene Manipulationen entdeckt werden.

Die sicherste Methode besteht darin, die Festplatte des Computers komplett zu löschen und das Betriebssystem neu zu installieren. Es ist deshalb wichtig, regelmässig ein *Backup* aller wichtigen Daten auf einem externen Speichermedium zu machen, damit diese Daten bei Problemen mit dem Computer nicht verlorengehen.

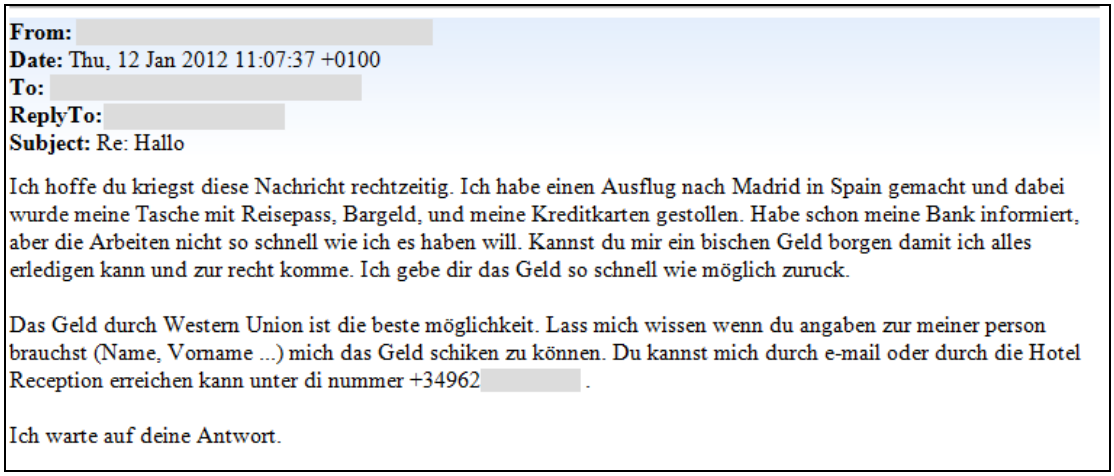
---

1 dt. Ereignisanzeige, ein Windows-Systemprogramm

2 http://www.retohaeni.net/2011/07/microsoft-does-not-call-you/ (Stand: 23. Februar 2012).

3.2 Vermehrt E-Mail-Konten gehackt

Bei der Melde- und Analysestelle Informationssicherung MELANI häufen sich die Meldungen, dass in E-Mail Konten eingebrochen worden ist. Die Kriminellen ändern dann typischerweise das Passwort und andere persönliche Angaben im Konto (alternative E-Mail-Adresse, Handynummer etc.), damit der rechtmässige Eigentümer nicht mehr darauf zugreifen kann. Danach werden alle oder gezielt Kontakte aus dem Konto angeschrieben. Meist handelt es sich bei diesen E-Mails um gefälschte Hilferufe, dass der Sender irgendwo im Ausland festsitze und ihm alles Geld sowie der Pass gestohlen worden sei. Schliesslich wird um die Überweisung von Geld gebeten.



From:
Date: Thu, 12 Jan 2012 11:07:37 +0100
To:
ReplyTo:
Subject: Re: Hallo

Ich hoffe du kriegst diese Nachricht rechtzeitig. Ich habe einen Ausflug nach Madrid in Spain gemacht und dabei wurde meine Tasche mit Reisepass, Bargeld, und meine Kreditkarten gestollen. Habe schon meine Bank informiert, aber die Arbeiten nicht so schnell wie ich es haben will. Kannst du mir ein bischen Geld borgen damit ich alles erledigen kann und zur recht komme. Ich gebe dir das Geld so schnell wie möglich zuruck.

Das Geld durch Western Union ist die beste möglichkeit. Lass mich wissen wenn du angaben zur meiner person brauchst (Name, Vorname ...) mich das Geld schiken zu können. Du kannst mich durch e-mail oder durch die Hotel Reception erreichen kann unter di nummer +34962 .

Ich warte auf deine Antwort.

Figur 1: Beispiel einer E-Mail, welche von einem gehackten Konto versendet wurde.

Neben den Unannehmlichkeiten für den Empfänger gibt es weitere Ärgernisse beim E-Mail Besitzer, da dieser keine Kontrolle mehr über sein Konto hat und nicht mehr auf E-Mails und Kontakte zugreifen kann. Dies kann verheerend sein und zu äusserst unangenehmen Situationen in der realen Welt führen, falls kein *Backup* der Daten und Kontakte erstellt wurde und alle Geschäftskontakte über diese E-Mail Adresse laufen.

Mit dem Zugriff auf ein fremdes E-Mail-Konto sind natürlich noch zahlreiche andere Betrügereien möglich. Viele Dienstleistungen im Internet können mittels einfacher Eingabe von Benutzername und Passwort aufgerufen werden. Vergisst der Kunde sein Passwort, kann er dieses über einen Link «Passwort zurücksetzen» neu anfordern. Er erhält das neue Passwort per E-Mail zugestellt. Gelingt es einem Angreifer, das E-Mail-Konto zu hacken, kann er sich diesen Service zunutze machen, um auf verschiedenste Dienste des Opfers zuzugreifen und diese für seine Zwecke zu missbrauchen.

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 Betrugsmails 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 seltenen Fällen wird die alternative E-Mail Adresse nicht verändert: In diesem 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

Am besten ist, es gar nicht so weit kommen zu lassen, dass in das Konto eingebrochen werden kann. Beachten Sie hierzu unsere Empfehlungen zur Passwortnutzung.[3] Generell gilt zudem, dass kein seriöser Dienstleister seine Kunden jemals per Mailnachricht zur Angabe des Passwortes auffordern wird. Klicken Sie deshalb nie auf einen Link in einem E-Mail, um auf die Seite eines Providers, Finanzdienstleisters, Kreditkartenunternehmens usw. zu gelangen. Siehe dazu unserer Informationen zu *Phishing*.[4] Seien Sie immer aufmerksam, wenn auf einer Webseite ein Passwort abgefragt wird. Siehe dazu auch den nächsten Beitrag in Kapitel 3.3.

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

Auch sollten bei Mails von bekannten Absendern Dateianhänge nicht unbedacht geöffnet oder Links angeklickt werden – insbesondere dann nicht, wenn die Mail unpersönlich erscheint, respektive keine persönliche Note des Absenders im Text erkennbar ist.

3.3 Eine Karte zum Fest, um Passwörter zu stehlen

Über die Festtage ist das Versenden und Empfangen von elektronischen Postkarten stark verbreitet. Doch längst nicht alle elektronischen Postkarten, die versendet werden, sind seriös. Über die Weihnachtstage sind zwei besonders professionelle Betrugsfälle beobachtet worden, die direkt auf Schweizer Opfer abzielten.

Im ersten Fall wurden im Namen von Swisspostcard[5] E-Mails versendet, deren Absender dem Empfänger bekannt war und welche die Empfänger dazu verleiten sollten, auf einen Link zu klicken. Den Empfängern wurde vorgegaukelt, dass sie eine elektronische Weihnachtskarte bekommen hätten und diese auf der Webseite unsereweihnachtskarten.com heruntergeladen werden könne.

[3] http://www.melani.admin.ch/themen/00166/00172/01005/index.html?lang=de (Stand: 23. Februar 2012).

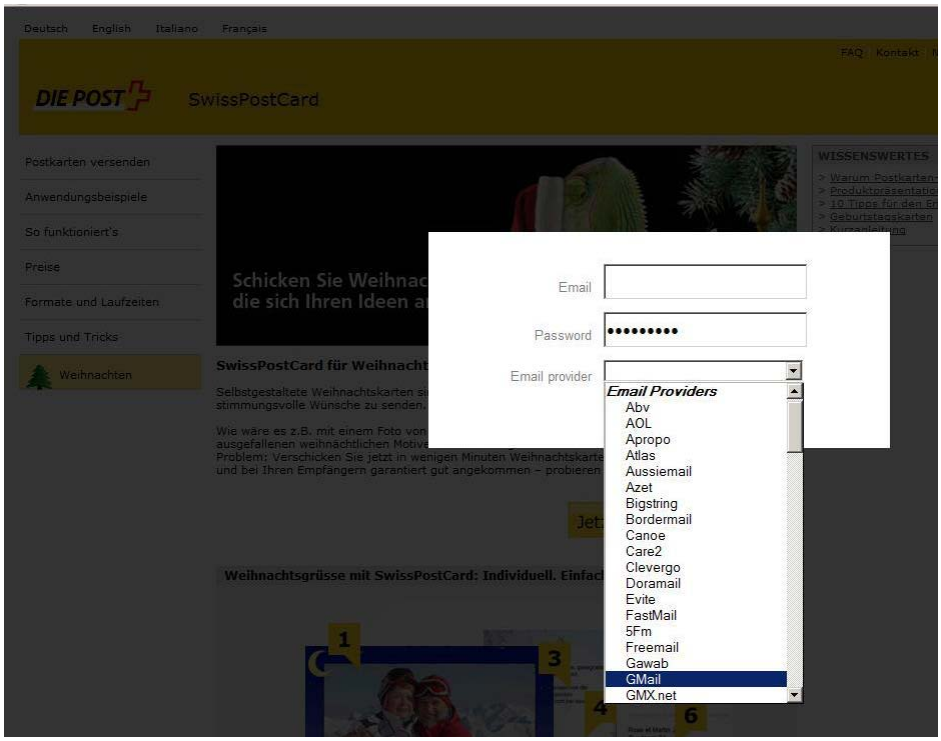
[4] http://www.melani.admin.ch/themen/00103/00203/index.html?lang=de (Stand: 23. Februar 2012).

[5] Über Swisspostcard (eine Dienstleistung der Schweizerischen Post) können Postkarten elektronisch erstellt werden. Diese werden dann von Swisspostcard physisch gedruckt und auf dem regulären Postweg dem gewünschten Empfänger zugestellt.

```
-------- Original-Nachricht --------
Datum: Mon, 26 Dec 2011 07:02:29 -0800
Von:
An:
Betreff: Du hast eine Weihnachtskarte erhalten!

Lieber,

Du hast eine Weihnachtskarte von "einem anonymen Absender" erhalten.

Was kannst Du tun?
Gehe zu: http://www.unsereweihnachtskarten.com?e=

Nachdem Du die Weihnachtskarte empfangen und gelesen hast, kannst du darauf antworten. Wenn du
eine Weihnachtskarte versenden möchtest, gehe zur genannten Webseite.


Viel Spaß,

Julia Emmrich
Unsereweihnachtskarten.com

Swiss Post International
swisspostcard.ch
```

Figur 2: Beispiel des Phishing E-Mails, das vorgaukelt, der Empfänger habe eine Weihnachtskarte bekommen.

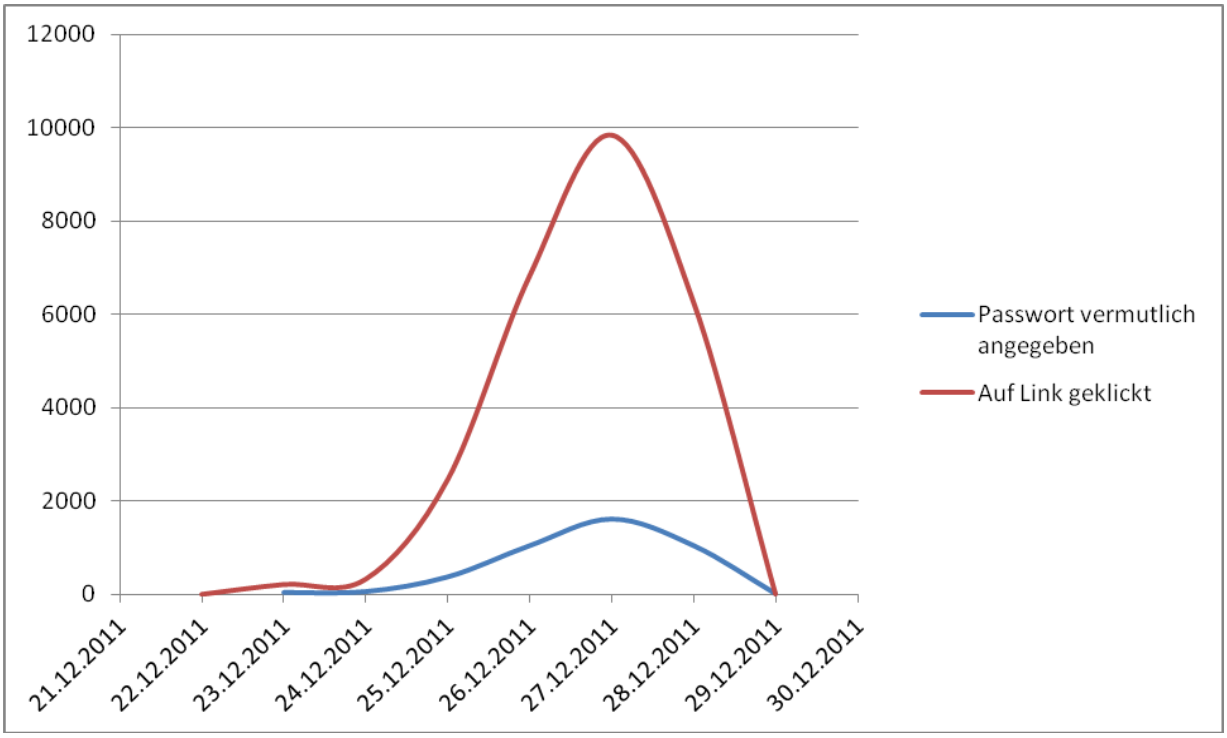
Ein Klick auf den Link öffnete im Hintergrund die Originalseite von Swisspostcard. Im Vordergrund wurde allerdings ein Formular eingeblendet, auf dem das Opfer Login und Passwort seines E-Mail-Kontos angeben musste, um seine persönliche Weihnachtskarte herunterladen zu können. Die eingegebenen Zugangsdaten wurden direkt den Betrügern weitergeleitet, welche damit umgehend auf das E-Mail-Konto zugriffen. Sofort wurden an alle Kontakte im Adressbuch weitere *Phishing*-E-Mails des gleichen Typs gesendet, um damit einen Schneeballeffekt zu erzielen.



Figur 3: Phishingseite, die im Hintergrund die Seite von Swisspostcard lädt und im Vordergrund die E-Mail Zugangsdaten verlangt.

Ein Woche später versuchten die Angreifer die gleiche Masche noch einmal. Diesmal wurde die *Phishing* E-Mail aber nicht im Namen von Swisspostcard, sondern im Namen von Fleurop versendet.

Im ersten Fall war es möglich eine Statistik der Anzahl Zugriffe zu erstellen. Insgesamt haben demnach 25‘939 Personen auf den Link geklickt, davon haben 4‘148 Personen die Seite mehrfach aufgerufen, was einen Hinweis darauf geben kann, dass diese zumindest versucht haben, Login und Passwort anzugeben. Dies entspricht etwa 16 Prozent. Ob diese Personen dann auch tatsächlich Login und Passwort angegeben haben, entzieht sich allerdings unserer Kenntnis.



Figur 4: Zugriffe auf die Phishingseite «unsereweihnachtskarten.com». Die rote Linie beschreibt die Anzahl Klicks auf die Seite. Die blaue Linie beschreibt diejenigen Benutzer, die mehrfach die Seite aufgerufen haben und demnach Login und Passwort angegeben haben könnten.

Nachdem vom 22. bis 24. Dezember 2011 nur vereinzelte Zugriffe stattgefunden haben, was sicherlich auf Weihnachten zurückzuführen ist, schnellte die Zahl am 25. Dezember hoch und erreichte am 27. Dezember 2011 das Maximum. Am 29. Dezember konnte die Seite dann vom Netz genommen werden.

Es gilt nicht mehr nur bei E-Mails von unbekannten Personen kritisch zu sein, sondern auch bei bekannten Absendern Vorsicht walten zu lassen. Insbesondere sollte man immer aufmerksam sein, wenn auf einer Webseite ein Passwort abgefragt wird.

3.4 Phishing Angriffe: Technisch optimiert

Staatliche Stellen, private Organisationen und Hosting Provider befassen sich mit der Bekämpfung von *Phishing*-Angriffen. Das Abschalten von Phishing-Seiten ist meist eingespielt. So kann mittlerweile praktisch jede Phishingseite innerhalb nützlicher Frist abgeschaltet werden, wobei «nützliche Frist» eine Zeitdauer von einigen Minuten bis zu einem Tag definiert. Kriminelle versuchen deshalb neue Methoden, um den entsprechenden Stellen das Abschalten von Phishingseiten möglichst schwer zu machen.

So wurde beispielsweise beim *Phishing*-Versuch, der in Kapitel 3.3 beschrieben wird, der Link für jedes Opfer speziell generiert und war nur einmal gültig. Konkret wurde in jedem Link die E-Mail-Adresse mit *base64* encodiert. Wurde der Initial-Link das zweite Mal angeklickt, erschien eine Fehlermeldung. Auch auf der Startseite wurde nichts anderes als eine Fehlermeldung eingeblendet. Dies erschwerte das Abschalten der Domäne, da die zuständige Stelle ohne aktiven Beweis Dritter nicht reagierte. Dies im guten Glauben, es befinde sich gar keine Phishing-Seite unter dieser Domain. Die nachfolgende Antwort eines Registrars zeigt dies deutlich:

Hello Sir,

Thank you for your email today and attention to this matter. After review we see that the subdomain you provided is not currently resolving to a phishing site at this time. If you have any further evidence of this domain being in breach of our registration agreement, please respond with it and we are happy to provide you with further assistance.

Thank you,

[redacted] Abuse Team

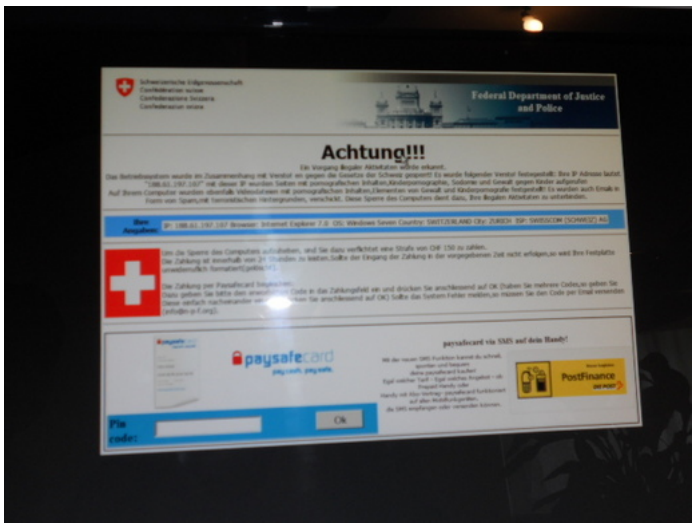
Figur 5: Antwort des Registrars nach der Anfrage von MELANI, die Domäne der Phishingseite zu sperren

Eine weitere Variante, die eingesetzt werden kann, ist die Implementation von IP-Filterung (z.B. Georestriktionen). Eine Phishingseite ist danach nur noch von bestimmten IP-Bereichen aus erreichbar. Besuchern mit anderen IP-Adressen wird eine Fehlermeldung angezeigt. Wer die Seite mit der «falschen» IP-Adresse aufruft, erhält so den Eindruck, dass die Seite schon vom Netz entfernt worden ist.

Dazu muss man wissen, dass sich die meisten Phishingseiten hinter ganz normalen Webauftritten auf einem kompromittierten Webserver verstecken. Anders als wenn eine Domäne ausschliesslich für kriminelle Zwecke verwendet wird, hat hier sowohl der Besitzer als auch der Hosting-Provider die Möglichkeit, die Webseite zu löschen. Da die Provider die Seiten meist nur Online überprüfen und nicht in der Verzeichnisstruktur des *Servers* nach der betrügerischen Seite suchen, war bis jetzt eine Fehlermeldung *«404 Not Found*» für die Provider ein sicheres Indiz, dass die Seite durch den Besitzer schon entfernt worden ist.

3.5 Jetzt auch in der Schweiz: Schadsoftware, die den PC sperrt und Bezahlung fordert

Anfang November verbreitete sich in der Schweiz eine *Schadsoftware*, welche zu erpresserischen Zwecken Computer sperrt. Dabei erscheint ein Fenster mit einer Nachricht, welche scheinbar vom Eidgenössischen Justiz- und Polizeidepartement (EJPD) stammt. In dieser Nachricht wird der Computerbenutzer aufgefordert, 150 Franken Busse zu bezahlen, da sich auf seinem Computer kinderpornografisches und anderes illegales Material befinde. Diese Meldung stammt selbstverständlich nicht von einer Schweizer Behörde.



Figur 6: Bildschirmansicht eines mit Ransomware infizierten Computers

Bereits im März und April 2011 war eine *Schadsoftware* im Umlauf, welche auf infizierten Computern eine Meldung, scheinbar vom Bundeskriminalamt Deutschland, anzeigte. Diese verlangte die Zahlung einer Busse von 100 Euro, da auf dem infizierten Computer illegale Daten gefunden worden seien. Bei Nicht-Bezahlung werde der Computer gesperrt und die *Harddisk* formatiert. Auch in anderen Ländern wurden entsprechende - jeweils auf das Land angepasste - Versionen dieser *Ransomware* beobachtet.

MELANI empfiehlt, beim Auftauchen dieser (oder einer ähnlichen) Meldung, den Computer mit einer dem neusten Stand entsprechenden AntiVirus-*Live-CD* zu analysieren und den Schädling zu entfernen oder aber sich an ein Computer-Fachgeschäft zu wenden. Zudem sollten bei einer Infektion die mit dem betroffenen Computer verwendeten Passwörter gewechselt werden.

3.6 Politik(er) im Visier von Hackern

Im zweiten Halbjahr gab es einige Vorfälle im Internet, welche es direkt oder indirekt auf Schweizer Politiker oder Parteien abgesehen haben. Gerade Politiker stehen in der Öffentlichkeit und bieten so auch mehr Angriffsfläche.

So wurde beispielsweise während der Bundesratswahl am 14. Dezember 2011 auf Twitter eine Meldung angeblich im Namen von Nationalrat Andrea Caroni veröffentlicht, dass Eveline Widmer Schlumpf wiedergewählt worden sei - und zwar bevor das offizielle Wahlergebnis bekannt war. Obschon Andrea Caroni mit diesem Account nichts zu tun hatte, musste dieser glaubhaft darlegen, dass er nicht hinter diesem *Tweet* steckte. Daraufhin erstellte er kurzerhand selbst ein Twitter-Konto und versendete Nachrichten zu diesem Thema. Dieses Beispiel zeigt, dass im Internet jeder in eine x-beliebige Rolle schlüpfen kann und in dieser Rolle x-beliebige Aussagen machen kann.

Auch die Webseite der SVP wurde am 3. August 2011 erneut durch einen Angriff auf die Verfügbarkeit lahmgelegt. Bereits im November 2009 wurden die Webseiten der Bundesratsparteien im Vorfeld der Abstimmung über die Volksinitiative vom 29. November 2009 «Gegen den Bau von Minaretten» angegriffen und lahmgelegt. Die anderen Bundesratsparteien waren allerdings in diesem Vorfall nicht betroffen.

Mit einem ganz anderen Problem sah sich Nationalrätin Chantal Galladé konfrontiert. Weil sie ihre Domäne chantal-gallade.ch nicht rechtzeitig erneuert hatte, wurde diese von einer Drittperson erworben, welche anschliessend Werbung darauf platzierte. Jeder Versuch, mit

dem neuen Inhaber in Kontakt zu treten, sei fehlgeschlagen. Eine Antwort blieb aus.[6] Mittlerweile hat Frau Galladé eine andere Domäne registriert. Auf der alten Domäne befindet sich keine Werbung mehr - sie steht nun zum Verkauf.

Ein anderer Politiker zeigte anlässlich eines Fernsehinterviews seine Identitätskarte in die Kamera. Eine unbekannte Person machte anhand eines Screenshot dieser Aufnahme eine «Kopie» der ID und versuchte, dieses Bild als Identitätsnachweis für die Erstellung eines Profils bei einem Datingportal für Homosexuelle zu verwenden. Das Datingportal nahm daraufhin Kontakt mit dem Politiker auf, um nachzufragen, ob er wirklich ein solches Profil eröffnet habe. Nach seiner Verneinung wurde das Profil sofort gelöscht. Dank der guten und aufmerksamen Arbeit des Datingportals konnte das Problem im Keim erstickt werden.

3.7 Massenweise Webshops gehackt

MELANI hat im August 2011 eine Häufung von *Webseiteninfektionen* auf Webshops festgestellt, darunter auch zahlreiche in der Schweiz. Betroffen waren Webshops, welche die Software osCommerce eingesetzt hatten.

Die Angriffe erfolgten über eine unzureichend gesicherte *Admin-Schnittstelle*. Bei älteren Versionen wurde standardmässig keine Zugriffsbeschränkung implementiert. Statt ein Passwort zu verwenden, wurde der Ordnername des *Administrationspanels* einfach durch einen obskuren Namen ersetzt und/oder man musste das Verzeichnis durch das Anlegen einer *.htaccess* Datei sichern. htaccess (englisch: hypertext access) ist eine Konfigurationsdatei des Apache Webservers, in der verzeichnisspezifische Einstellungen vorgenommen werden können. Leider unterliessen dies viele Benutzer. In Folge dessen wurde zur Erhöhung der Sicherheit in Version 2.2RC2 eine Administrations-Zugangskontrolle eingebaut. Eine nicht korrekte Implementierung hatte allerdings zur Folge, dass diese Sicherung auf einem Apache Web-Server mittels *URL-Manipulation* relativ einfach umgangen werden konnte.[7] So war es für einen Angreifer ein Leichtes, sich in die Administration einzuloggen und dort beliebigen *Code* zu installieren. Dies wurde dann im Juli/August 2011 massiv ausgenutzt. Die gehackten Shops wurden anschliessend dazu verwendet, um *Webseiteninfektionen* zu platzieren. Gemäss einer Mitteilung auf dem IT- und Tech-Kanal, gulli.com, wurden bis zu 90‘000 Onlineshops von den Angreifern kompromittiert.[8]

Zum Schutz konnte in diesem Fall das ganze Verzeichnis admin durch das Anlegen einer Datei *.htaccess* gesichert werden. Diese Zugriffskontrolle wird vom Web-Server selbst durchgeführt und ist unabhängig vom Login-Prompt der Shop-Software. Eine ausführliche Anleitung wurde durch heise.de publiziert.[9] Generell müssen nicht nur die Serversoftware, sondern auch die installierten Applikationen, wie in diesem Falle der Webshop, auf dem neuesten Stand gehalten und alle verfügbaren Sicherheitsupdates installiert werden.

---

6 http://www.tagesanzeiger.ch/zuerich/region/Warum-Chantal-Gallad-fuer-Bikinis-wirbt/story/15004208 (Stand: 23. Februar 2012).

7 http://www.oscommerce.info/confluence/display/OSCOM23/%28A%29+%28SEC%29+Administration+Tool+Log-In+Update (Stand: 23. Februar 2012).

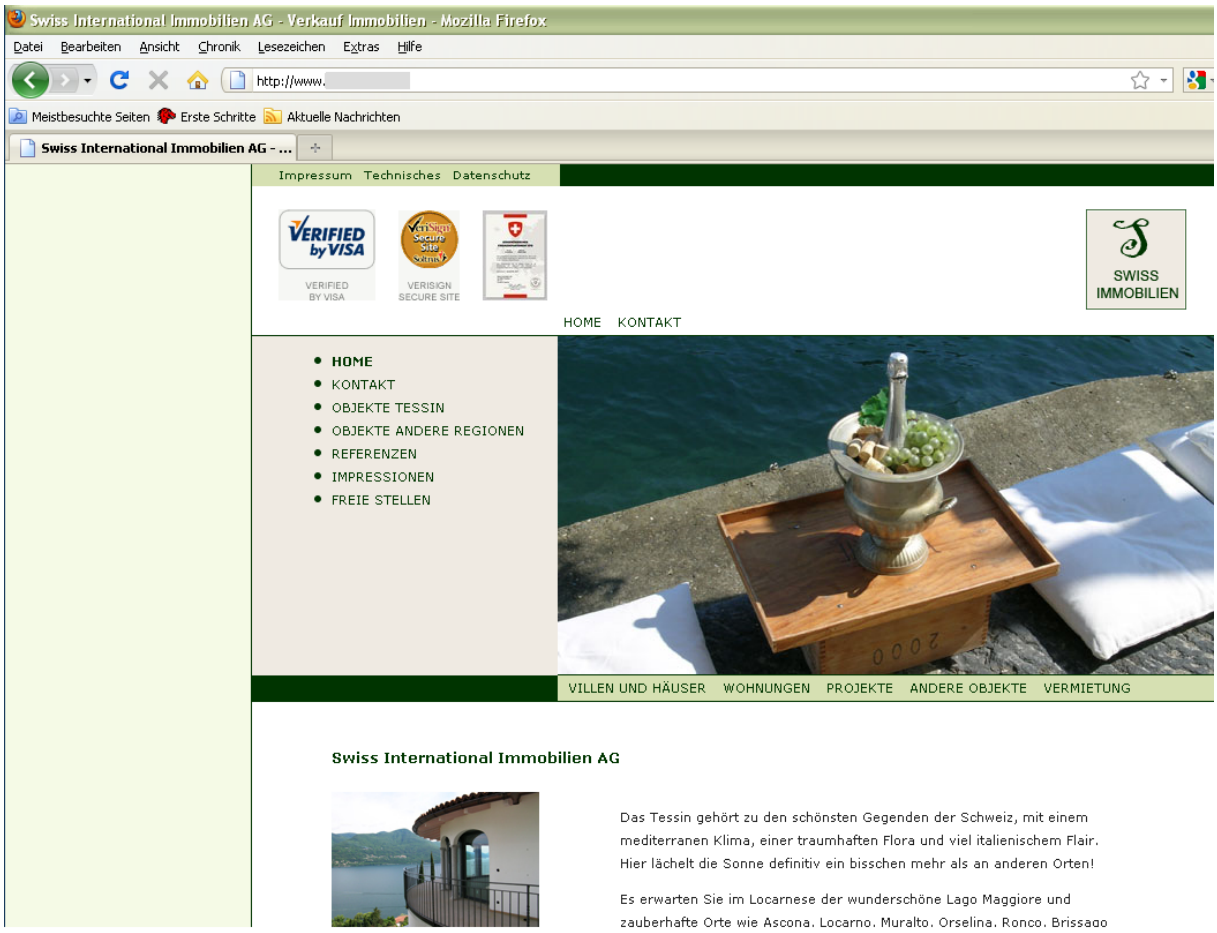
8 http://www.gulli.com/news/16740-zahlreiche-online-shopping-websites-kompromittiert-2011-08-01 (Stand: 23. Februar 2012).

9 http://www.heise.de/security/artikel/Schnellhilfe-fuer-osCommerce-Admins-1323536.html (Stand: 23. Februar 2012).

3.8 Gefälschte Webseiten von Immobilienfirmen werben mit Stelleninseraten für Finanzagenten

Nach einem E-Banking Betrug muss das erbeutete Geld «gewaschen» werden. Hierzu werden oft *Finanzagenten* angeworben, was beispielsweise über Jobbörsen geschieht. Es werden aber auch speziell Seiten ins Netz gestellt, welche vorgaukeln, Firmenwebseiten zu sein, und eine Rubrik «Freie Stellen» oder Ähnliches aufweisen. Bei diesen Jobs geht es immer um das Gleiche: Gelder aus unbekannten Quellen müssen angenommen und an bestimmte Konten weitergeleitet werden. Auf diese «Freien Stellen» wird jeweils per *Spam*-Nachricht hingewiesen.

Ein besonders dreister und hartnäckiger Fall von Finanzagentenrekrutierung wird momentan in der Schweiz beobachtet. Konkret werden die Angaben von Firmen verwendet, welche zwar im Handelsregister eingetragen sind, jedoch keine Internetpräsenz haben. Unter diesen Adressangaben geben die Webseiten vor, von Firmen zu stammen, welche mit Immobilien im Tessin handeln und diesbezüglich Regionalvertreter suchen, um Kundengelder zu transferieren. Die Seiten sehen sehr professionell aus. Sie sind meist eine 1 zu 1 Kopie der Webseite einer Drittfirma. Hier stellt sich das Problem, dass die kriminelle Motivation – im Gegensatz zu beispielsweise *Phishing*-Webseiten nicht offensichtlich ist. Normalerweise werden kriminelle Webseiten schnell von Providern deaktiviert. In diesem Fall ist es allerdings sehr schwierig, den Provider zu bewegen, diese Webseite zu deaktivieren. Gelingt dies trotzdem, dauert es nicht lange und eine identische Webseite wird unter einer anderen Domäne aufgeschaltet. Es scheint, dass sich hier eine Gruppe von Kriminellen darauf spezialisiert hat, diese Webseiten möglichst lange am Laufen zu halten und damit möglichst viele Finanzagenten anzuwerben.

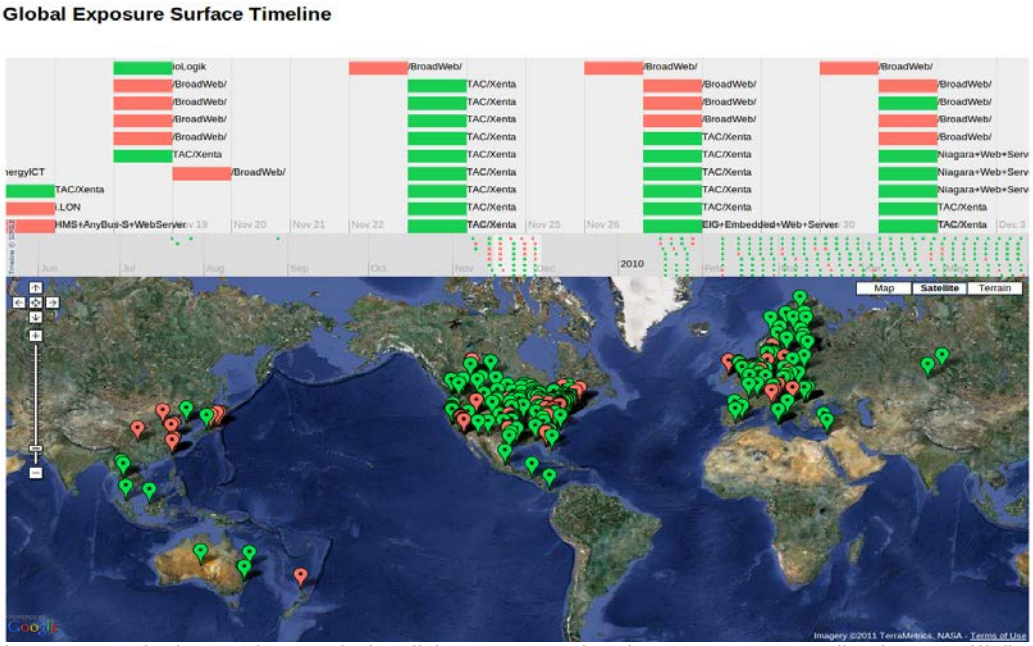


Figur 7: Beispiel einer Finanzagentenrekrutierungsseite.

Solche Angebote werden nicht nur mittels E-Mail und speziell erstellten Webseiten in Umlauf gebracht, sondern sind auch auf diversen Internetseiten mit seriösen Jobangeboten zu finden. Grundsätzlich ist Vorsicht geboten, wenn Geld, welches man zuvor (gewollt oder irrtümlich) bekommen hat, an Unbekannte via Bargeldtransfer überwiesen werden soll. In jedem Fall sind Angebote mit Vorsicht zu geniessen, die mit Aussicht auf unverhältnismässig hohe Gewinne locken. Auch im Internet gilt grundsätzlich die Regel, dass ohne entsprechende Arbeit auf legale Weise kein grosses Geld zu verdienen ist. Eigene Bankkonten sollten nie Dritten zur Verfügung gestellt werden.

3.9 Kontrollsysteme mit Internetverbindung – Besonderes Sicherheitsbewusstsein nötig

Suchmaschinen für Webseiten gehören zum Alltag jedes Internetbenutzers. Dass es auch eine Suchmaschine gibt, um *Server*, *Router*, *Firewalls*, Drucker und andere Geräte, die am Internet angeschlossen sind, zu finden, war bis vor kurzem weniger bekannt. «SHODAN» ist eine solche Suchmaschine und existiert bereits seit einigen Jahren. Sie steht aber erst seit kurzem im Blickpunkt der Öffentlichkeit. Dies nachdem Untersuchungsergebnisse zu *SCADA*-Systemen, welche mit dem Internet verbundenen sind, veröffentlicht worden waren. Die Forscher an der Universität Cambridge verfolgten mit der Untersuchung die Absicht, die leicht anfälligen industriellen *Kontrollsysteme* mit Internetverbindung quantitativ einzuschätzen. Die Forschungen[10] sollten den Mythos widerlegen, wonach industrielle Kontrollsysteme nicht mit dem Internet verbunden sind und demnach nicht zu Befürchtungen wegen der Sicherheit von heiklen Infrastrukturen Anlass geben. Die Forscher entdeckten dabei Dutzende von mit dem Internet verbundenen, anfälligen Siemens Simatic-Systemen (Ziele im Visier von Stuxnet), *SCADA*-Systeme sowie *Building Management Systeme* (BMS).

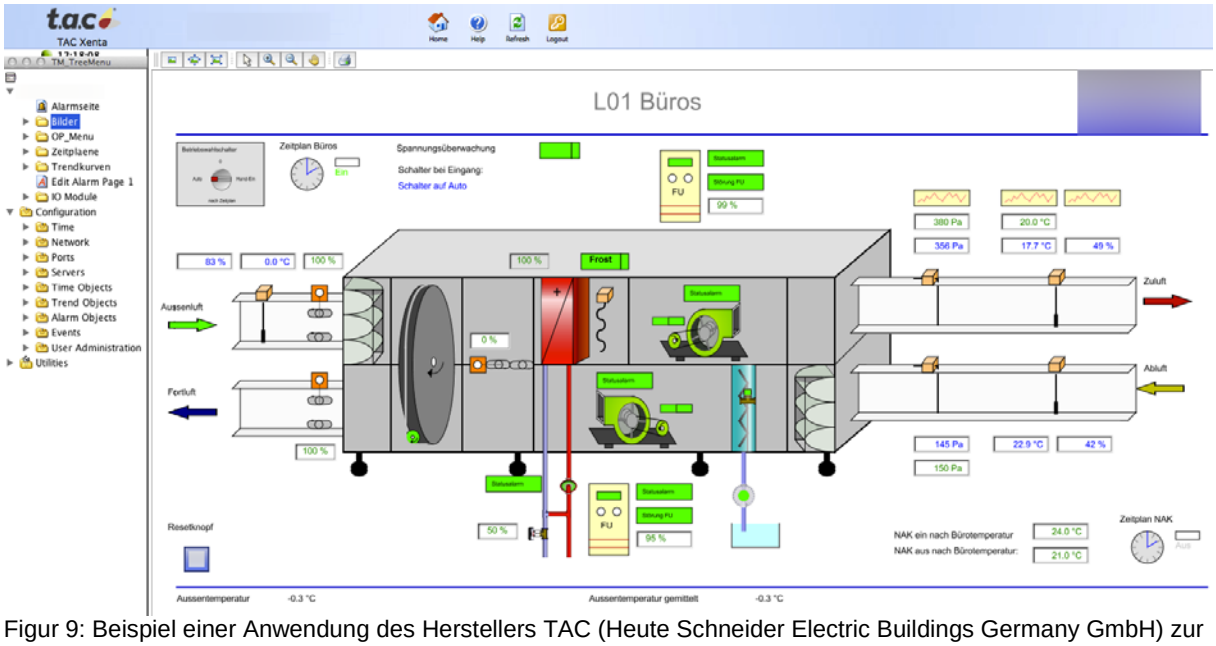


Figur 8: Quantitative Analyse und Visualisierung von Industriesteuersystemen, die eine Angriffsfläche bieten. (Quelle: Eireann Leverett)[11] Rot markiert sind die Systeme mit einem bekannten Exploit.

[10] http://www.wired.com/images_blogs/threatlevel/2012/01/2011-Leverett-industrial.pdf (Stand: 23. Februar 2012).

[11] http://cryptocomb.org/2011-Leverett-industrial.pdf (Stand: 23. Februar 2012).

In der Schweiz führten diese Nachforschungen zur Aufdeckung von 34 anfälligen Systemen. Es handelte sich mehrheitlich um Anwendungen, welche für *Building Management Systeme* verwendet werden. Es wurde bei diesen Steuerungsanlagen mit Webzugriff schlicht vergessen, die Standardpasswörter zu ändern. Somit war es möglich, Zugriff auf diese Anlagen zu erhalten und diese vollständig zu kontrollieren. MELANI stellte bei der Überprüfung der Information fest, dass die anfälligen Systeme nicht zu heiklen Infrastrukturen, sondern vor allem zu Betrieben, z.B. Hotels und Büros, gehörten.



Figur 9: Beispiel einer Anwendung des Herstellers TAC (Heute Schneider Electric Buildings Germany GmbH) zur Steuerung von Gebäuden.

Die potenziellen Ziele gelten zwar nicht als heikel, aber die Tatsache, dass bei der Installation eines *Building Management Systeme* (BMS) mit Internetverbindung das Default-Passwort nicht geändert wird, bildet einen gravierenden Verstoss gegen die grundlegenden Informatiksicherheitsvorschriften. Die Möglichkeit, z.B. auf das Heizungs- oder Klimaanlagen-Netz eines fremden Betriebs zugreifen und es zu manipulieren, könnte unter bestimmten Umständen schwerwiegende Probleme verursachen. Weiter eröffnen die teilweise Einbindung und Zugriffsmöglichkeiten auf andere betriebsinterne Verwaltungsapplikationen, wie Abrechnungssoftware und dergleichen, zusätzliches Missbrauchspotential. Grundsätzlich sollten industrielle Kontrollsysteme nicht mit dem Internet verbunden werden. Falls dies unbedingt erforderlich ist, ist bei der Vorgehensweise besondere Vorsicht geboten. Eine ausführliche Einschätzung befindet sich in Kapitel 5.1.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Angriff auf niederländische Zertifizierungsstelle

Bei einem Angriff auf DigiNotar, eine niederländische *Zertifizierungsstelle*, wurden nach aktueller Erkenntnis missbräuchlich über 530 *Zertifikate* ausgestellt. Darunter befanden sich beispielsweise *Zertifikate* für Domänen von Nachrichtendiensten: Die Angreifer konnten jeweils mehrere *Zertifikate* für www.sis.gov.uk, www.cia.gov und www.mossad.gov.il ausstellen. Auch für diverse andere Domänen wurden missbräuchlich *Zertifikate* ausgestellt, darunter windowsupdate.com, welche die Update Funktion aller Windowsprodukte von Microsoft beherbergt, und verschiedene Google-Domänen.

DigiNotar ist ein Herausgeber von *Zertifikaten* (Certificate Authority, CA), welche die Identität von Webseiten garantieren und die verschlüsselte Kommunikation sicherstellen. Werden solche *Zertifikate* gefälscht, kann es beispielsweise sein, dass man zwar denkt, auf die gewünschte Webseite zuzugreifen, in Wirklichkeit aber mit der Infrastruktur des Angreifers verbunden ist. Ein Angreifer kann so den Weg der Daten ändern, verschlüsselte Daten abfangen und auch falsche Daten zurückliefern. Bei dem Angriff auf DigiNotar sind nun gefälschte – aber von *Browsern* und Computern als vertrauenswürdig eingestufte – *Zertifikate* in Umlauf gebracht worden. So kann beispielsweise eine verschlüsselte Verbindung auf ein Webmail-Konto entschlüsselt oder ein Update von Windows gefälscht werden. Allerdings reicht ein gefälschtes *Zertifikat* alleine noch nicht aus. Die Verbindung muss auch über entsprechend eingerichtete *Server* geleitet werden. DigiNotar hat den Angriff anscheinend bereits am 19. Juli 2011 entdeckt; Google entdeckte dann Ende August *Man-in-the-Middle* Angriffe auf seine Maildienste und machte dies publik.

Microsoft hat kurz darauf für seine Betriebssysteme ab Windows XP und für Internet Explorer Updates veröffentlicht, die den *Stammzertifikaten* der kompromittierten DigiNotar-CA das Vertrauen entziehen und sie auf die Liste der nicht vertrauenswürdigen Herausgeber setzt. Auch andere *Browser*-Hersteller wie Mozilla (Firefox) und Google (Chrome) haben bei ihren Programmen die von DigiNotar herausgegebenen *Zertifikate* mittlerweile als ungültig markiert.

Gemäss einem veröffentlichten Zwischenbericht des mit der Untersuchung beauftragten Sicherheitsunternehmens[12] zeigt eine Auswertung der Daten, dass die falschen *Zertifikate* auch wirklich zum Einsatz gekommen sind. Etwa 300‘000 *IP-Adressen* haben beispielsweise das gefälschte Google-*Zertifikat* benutzt. Diese *IP-Adressen* lassen sich laut dem Bericht zu 99% iranischen Rechnern zuordnen. Um die Daten abfangen und entschlüsseln zu können, musste der Angreifer noch eine zusätzliche Interaktion direkt am Datenweg, z.B. bei den Providern vornehmen. Ein iranischer Hacker behauptet mittlerweile, der Urheber zu sein und weitere Zertifikatsherausgeber angegriffen zu haben. Ob die Angriffe tatsächlich von ihm ausgegangen sind oder ob hier allenfalls ein staatlicher Akteur mit Spionageabsicht dahinter steckt, lässt sich momentan noch nicht sagen.

Der Hackerangriff gegen DigiNotar hat die Firma in die Insolvenz getrieben. Nach Aussagen des Mutterunternehmens Vasco wird der Geschäftsbetrieb der Tochter eingestellt und die Firma liquidiert. Die niederländische Regierung hat bereits kurz nach Bekanntwerden der Vorfälle die Kontrolle über die operativen Geschäfte von DigiNotar übernommen. DigiNotar gab nämlich neben seinen eigenen auch *Zertifikate* als sub-CA für die «PKI Overheid» des niederländischen Staates aus und es gab Anzeichen, dass die dafür verwendeten Systeme ebenfalls kompromittiert worden waren. Das «PKI Overheid»-Stammzertifikat wurde jedoch nicht zurückgezogen, weil dies sonst zu Ausfällen bei der Kommunikation von Computersystemen hätte führen können, die auf verschlüsselte Verbindungen angewiesen waren. Es konnte zudem nicht nachgewiesen werden, dass über diese Infrastruktur missbräuchliche *Zertifikate* ausgestellt worden waren. Alle von DigiNotar als sub-CA ausgegebenen «PKI Overheid»-*Zertifikate* wurden aber vorsichtshalber durch neue *Zertifikate* von anderen sub-CA ersetzt.

In einem weiteren Fall behauptete ein Hacker, er sei in die Systeme des Zertifikataustellers GlobalSign eingedrungen. Der belgische Zertifikatsaussteller nahm seine *Server* daraufhin für eine Woche vom Netz und startete eine Untersuchung. Diese ergab, dass der Hacker jedoch nicht in einen *Server* eingedrungen war, der für die Zertifikatsausgabe genutzt wird, sondern in einen *Server*, der die öffentlichen Firmen-Webseiten für Nordamerika zur Verfü-

12 http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html (Stand: 23. Februar 2012).

gung stellt. Darauf sollen sich laut GlobalSign keine Webanwendungen und auch keine Kundendaten befunden haben.[13]

Der sichere Einsatz von *Kryptosystemen* mit öffentlichen Schlüsseln (sog. «Public Key»-Kryptografie) steht und fällt mit der Sicherheit der entsprechenden *Certification Service Provider* (CSP) und Public-Key-Infrastruktur (PKI)[14]. Entsprechend ist die Sicherheit von CSPs und PKIs immer schon ein Thema gewesen, mit dem sich Sicherheitstechniker befasst haben. Im Mittelpunkt des Interesses sind dabei Szenarien gestanden, bei denen entweder *Zertifikate* (über Schwachstellen in der Kollisionsresistenz der eingesetzten kryptografischen Hashfunktionen[15]) gefälscht oder Code-Signierzertifikate missbraucht werden. Im zweiten Fall erlaubt – wie der Stuxnet-Wurm gezeigt hat – ein solches *Zertifikat* z.B. das Einbringen von *Malware* in Form digital signierter *Treibersoftware* in ein Betriebssystem. Die jüngsten Angriffe auf CSPs haben nun aber gezeigt, dass auch die Kompromittierung eines CSP zwecks Ausgabe falscher *Zertifikate* eine reale Bedrohung darstellt. Dabei scheinen Hacker vermehrt auf die Quelle abzuzielen und sparen sich somit den viel mühsameren Weg über die an sich sicheren Kryptoverfahren.

4.2 SCADA – Schadsoftware, Angriffe und Schwachstellen

Supervisory Control And Data Acquisition Systeme werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung). Ursprünglich hatten diese Systeme nur wenig Ähnlichkeit mit herkömmlicher IKT; sie waren von den Computernetzwerken isoliert, benutzten proprietäre Hard- und Software und setzten zur Kommunikation mit dem Zentralrechner eigene Protokolle ein. Die breite Verfügbarkeit vergleichsweise günstiger Geräte mit eingebauter Schnittstelle zum Internet-Protokoll hat in den letzten Jahren in diesem Bereich grosse Veränderungen gebracht. Den Vorteil des Einsatzes kostengünstiger herkömmlicher IKT erkauft man sich damit, dass SCADA-Systeme nun grundsätzlich den gleichen Bedrohungen ausgesetzt sind, wie wir sie vom Internet her kennen: Malware sowie Angreifer halten Einzug.

Symantec entdeckt «Duqu», eine Schadsoftware mit Bezügen zu Stuxnet

Am 14. Oktober 2011 wurde eine *Schadsoftware* namens «Duqu» bekannt, die Computer von Unternehmen und Entwicklern von Industriesteuersystemen (*SCADA*-Systeme) ausspionieren soll. Auf diese Weise entwendete Daten können für spätere Angriffe auf Industriesteuersysteme verwendet werden. Die Grundkomponenten (Treiber) dieser neuen *Schadsoftware* basieren auf Bestandteilen der bereits bekannten *Schadsoftware* Stuxnet.[16] Im Gegensatz zu Stuxnet besitzt die neue *Schadsoftware* allerdings keine Verbreitungsroutine und keine *SCADA* Komponente, um beispielsweise Steuersysteme zu manipulieren. Um möglichst unerkannt zu bleiben, aktiviert sich die *Schadsoftware* erst 15 Minuten nach der Installation. Nach 36 Tagen entfernt sich die *Schadsoftware* vom infizierten System, was die Erkennung zusätzlich erschwert. Es wurden verschiedene Varianten von «Duqu» beobachtet.

---

13 http://www.zdnet.de/news/41558800/globalsign-comodohacker-hat-die-falschen-systeme-erwischt.htm (Stand: 23. Februar 2012).

14 In diesem Sinne stellen die CSPs bzw. PKIs eine Achillesverse der «Public Key»-Kryptografie dar.

15 Dieser Punkt wird z.B. in der «Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen» vom 4. August 2010 vertieft: http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de (Stand: 23. Februar 2012)

16 Siehe MELANI-Halbjahresbericht 2010/2, Kapitel 4.1, Link: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 23. Februar 2012).

In einem Fall wurde für die Installation ein gestohlenes *Zertifikat* einer taiwanesischen Firma verwendet; auch dies ist eine Parallele zu Stuxnet. Die anderen Varianten waren angeblich nicht digital signiert.

Die Funktionen der *Schadsoftware* umfassen das Aufzeichnen von Tastatureingaben, das Analysieren von Netzwerkinformationen und das Abspeichern des Bildschirminhaltes. Diese Informationen werden in einer unauffälligen Bilddatei versteckt an den Angreifer gesendet. Prinzipiell ist allerdings die Funktion nicht an die *Schadsoftware* gebunden und kann beliebig vom Angreifer variiert werden. «Duqu» kommuniziert verschlüsselt mit einem *Kommando-server* mit indischer *IP-Adresse*, dem der infizierte Rechner gesammelte Daten abliefert und von dem dieser neue Befehle abholt. Eine Variante soll bereits im Dezember 2010 im Umlauf gewesen sein, neuere Varianten stammen aus dem Zeitraum September/Oktober 2011. «Duqu» soll auf Computern von sieben bis acht europäischen Unternehmen gefunden worden sein, darunter auch eine *IP-Adresse* in der Schweiz.

Angebliche Angriffe auf Wasserversorgung

Ein angeblicher elektronischer Angriff auf das Wasserversorgungssystem in Springfield/Illinois in den USA Anfang November 2011 hat in Fachkreisen zu breiten Diskussionen geführt. Angeblich soll es einem Angreifer gelungen sein, in das Steuersystem der Wasserversorgung einzudringen und dort eine Wasserpumpe durch mehrmaliges Ein- und Ausschalten zu zerstören. Anscheinend gab es in der Zeit vor dem Defekt unter Anderem Zugriffe auf das Netzwerk der Anlage von einem Computer mit *IP-Adresse* in Russland, was die Gerüchteküche zusätzlich aufheizte. Ein paar Tage später bestritten das FBI sowie das Department of Homeland Security (DHS) die Berichte über den Angriff in Springfield. Es gebe keine Hinweise auf einen Cyber-Angriff. Die Behauptungen aus einem entsprechenden Bericht des Terrorismus-Lagezentrums von Illinois, der an die Öffentlichkeit gelangt war und auf dem die Spekulationen beruhten, sollen auf unbestätigten Rohdaten basiert haben. Es gebe keine Anzeichen, dass Zugangsdaten zu dem System entwendet wurden und es wurden auch keine Anzeichen eines Eindringens gefunden. Die Zugriffe aus Russland stammten von einem autorisierten Techniker, welcher gerade in Russland unterwegs war und sich via (regulären) Fernzugriff in das Netzwerk der Anlage einwählte. Die Pumpe habe schon längere Zeit Probleme bereitet und sich mehrfach an- und abgeschaltet, bevor sie ihren Dienst schliesslich ganz versagt habe.

Möglicherweise motiviert durch die Meldungen zu obigem Fall drang ein Hacker am 18. November 2011 in die Wasserversorgung von South Houston/Texas ein und veröffentlichte als Beweise *Screenshots* aus dem Steuersystem der Einrichtung. In diesem Fall bekannte sich eine Person unter dem Pseudonym «pr0f» mit einer Botschaft auf der Seite pastebin.com zu diesem Angriff: «Der Moment ist gekommen um aufzuzeigen, dass sensible Systeme nicht mit dem Internet verbunden sein dürfen. Man soll sich nicht über einen angeblichen grossen Cyberkrieg Sorgen machen, sondern man muss sich vielmehr schon vor Einzeltätern fürchten, die aus verschiedensten Motiven und ohne grosse Informatikkennisse solch sensible Systeme angreifen könnten».

US-Beobachtungssatellit in den Jahren 2007 und 2008 gehackt

Laut einem Bericht der Bloomberg Businessweek[17] wurden in den Jahren 2007 und 2008 mehrfach Angriffe auf die Steuerungssysteme von zwei US-Beobachtungssatelliten festgestellt. Diese werden zur Erd- und Klimabeobachtung sowie zur Kartierung eingesetzt. Bei den Angriffen sollen Hacker während mehrerer Minuten die Kontrolle übernommen haben.

---

17 http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html (Stand: 23. Februar 2012).

Wie der Angriff im Detail ablief, ist nicht bekannt. Denkbar ist es beispielsweise, dass Daten verfälscht wurden. Theoretisch wäre es möglich gewesen, den Satelliten zu steuern und ihn sogar zum Absturz zu bringen.

Sicherheitsbedenken beim Netzwerk des Boeing Dreamliners

Laut einem Bericht der FAA[18] gibt es Sicherheitsbedenken bei der Netzwerkverkabelung des neuen Dreamliners von Boeing. Anscheinend ist das Netzwerk für die Passagiere, welches unter anderem den Internetzugriff während des Fluges ermöglicht, physisch auch mit dem Kontroll- und Navigationsnetzwerk des Flugzeuges verbunden, welches die sicherheitsrelevanten Funktionen steuert.

Boeing selbst sagte, dass das Dokument der FAA irreführend und dass das Passagiernetzwerk nicht vollständig mit den anderen Netzwerken verbunden sei. Es handelt sich dabei um eine Kombination von physischer Trennung und Software *Firewalls*, sowie anderen Lösungen, die nicht öffentlich diskutiert werden. Es könnten zwar Daten zwischen den Netzwerken ausgetauscht werden, installierte Schutzmechanismen sollen aber unter allen Umständen verhindern, dass der Internet Service der Passagiere auf das Kontroll- und Navigationsnetzwerk zugreifen kann.

Eine physische Verbindung des Passagiernetzwerks mit dem Kontrollnetzwerk des Flugzeuges würde das Kontrollsystem anfällig für Hackerangriffe machen. Boeing selbst hat das Problem erkannt und will eine neue Lösung testen und implementieren.

Die grundsätzliche Problematik der *SCADA*-Systeme liegt insbesondere in ihrer Geschichte: Ursprünglich waren es abgeschottete, eigenständige und proprietäre Systeme, auf die von aussen höchstens zu Wartungszwecken via ein *Dial-up Modem* vom Hersteller zugegriffen werden konnte. Entsprechend weisen diese Systeme kaum Funktionen zum Schutz vor elektronischen Angriffen auf. In jüngster Zeit werden *SCADA*-Systeme jedoch zunehmend vernetzt, verwenden standardisierte Protokolle und Technologien, sind teilweise sogar über das Internet erreichbar und können mit speziellen Suchmaschinen (siehe Suchmaschine SHODAN in Kapitel 3.9) manchmal auch gefunden werden. Stuxnet hat ebenfalls gezeigt, dass ein abgeschottetes System alleine keine Sicherheit gewährleisten kann. Solange es möglich ist, Daten beispielsweise via *USB*-Stick in die abgeschotteten Systeme zu transferieren, besteht auch die Möglichkeit, *Schadsoftware* einzuschleusen. Die Medienpräsenz von Stuxnet hat bei vielen Sicherheitsexperten auch das Interesse an Industrieleittechnik und *SCADA*-Systemen geweckt. So wurden seither verschiedene Sicherheitslücken in solchen Produkten identifiziert. Es wurden unter anderem Methoden entdeckt, die es erlauben, Systeme fernzusteuern, beliebige Daten herunter- respektive hochzuladen, *Codes* einzuschleusen und zu starten sowie falsche Daten einzuspeisen, auf welche die Steuerungen dann entsprechend reagieren.

4.3 Anonymous

Am 27. Juli 2011 hat die britische Polizei auf den schottischen Shettland Inseln den mutmasslichen Sprecher der Hacker-Gruppen «Anonymous» und «LulzSec» festgenommen. Es handelt sich dabei um einen 19-jährigen Mann. In verschiedenen Staaten, darunter USA, England, Holland, Spanien, Türkei wurden bereits andere Teilnehmer der Internet-Protestbewegung festgenommen. Solche Verhaftungen führen jeweils zu Angriffen auf die

[18] Federal Aviation Administration, Bundesluftfahrtbehörde der USA, http://www.faa.gov (Stand: 23. Februar 2012).

Webseiten der entsprechenden Polizeikorps oder Regierungen. So geschehen auch nach einer koordinierten Aktion der italienischen und Tessiner Polizei Anfang Juli, bei welcher 15 mutmassliche Aktivisten in Italien verhaftet wurden. Ebenfalls wurde ein im Tessin wohnhafter 26-jähriger Italiener, der als Kopf der italienischen Zelle von Anonymous gehandelt wird, verhaftet. Das Anonymous-Kollektiv hatte unter anderem die italienischen Firmen Eni, Finmeccanica und Unicredit angegriffen. Auch Institutionen wie die italienische Post, der Senat, die Abgeordnetenkammer und die Webseite der Regierung von Ministerpräsident Berlusconi waren im Visier von Anonymous. Internetaktivisten haben als Antwort auf die Verhaftung nach eigenen Angaben zufolge Datenmaterial von den *Servern* der italienischen Cyber-Polizei CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastructure Critiche) entwendet und diese ins Internet gestellt. Die staatliche Behörde ist für den Schutz und die Aufrechterhaltung der kritischen IT-Infrastruktur in Italien zuständig. Ein Schreiben, dass es sich hier um eine Vergeltungsaktion handle, wurde zwar von der Gruppe «Anonymous» als nicht authentisch zurückgewiesen. Trotzdem dürfte ein gewisser Zusammenhang bestanden haben.

Ebenfalls im Juli 2011 gaben Internet-Aktivisten an, in einen NATO-*Server* eingedrungen zu sein und dort zahlreiche Dokumente von einem *Server* kopiert zu haben. Als Beweis wurden zwei PDF-Dokumente aus den Jahren 2007 und 2008 veröffentlicht. Der Einbruch soll mittels *SQL-Injection* durchgeführt worden sein. Eine andere Aktion war die Veröffentlichung von 25‘000 Datensätzen mit Namen, Adressen und Geburtsdaten von Polizisten in Österreich. Begründet wurde diese Aktion unter anderem mit einem Verweis auf die Einführung der Vorratsdatenspeicherung in Österreich im April 2011.

Am meisten Aufsehen hat aber sicherlich der Angriff auf Kundendaten der US-Firma Strategic Forecast (Stratfor) Ende Jahr erregt. Die Firma Stratfor ist auf internationale Sicherheitsanalysen spezialisiert und versorgt seine Kunden mit Berichten zu aktuellen geopolitischen Sicherheitsfragen wie Terrorismus, politische Umwälzungen oder Machtwechsel in einzelnen Ländern. Bei der Hackerattacke wurden unter anderem E-Mail Bestände, Benutzerdaten, Passwörter und Kreditkarteninformationen entwendet. Ein Ziel der Aktion sei es gewesen, mit den gestohlenen Kreditkartendaten Überweisungen an wohltätige Organisationen zu tätigen und so «mehr als 1 Million USD an gemeinnützige Einrichtungen umzuverteilen». Angeblich ist es auch zu nicht autorisierten Zahlungen mit gestohlenen Kreditkarten gekommen. Die Aktivisten dürften damit den Wohltätigkeitsorganisationen einen Bärendienst erwiesen haben – solche Zahlungen verursachen auf allen Seiten administrativen Aufwand. Nachdem sich zuerst Anonymous zur Aktion mit dem Namen «LulzXmas» bekannt hat, kursierte im Internet im Namen von Anonymous auch ein Dementi und anschliessend wiederum ein Dementi des Dementi. Wieder in einem anderen Beitrag wurden die wahren Gründe des Angriffs in der Offenlegung der Kontakte zu Geheimdiensten und der Rüstungsindustrie angegeben.

Unter dem Label «Anonymous» subsumieren sich Internet-Aktivisten aus aller Welt, um für ein freies Internet und gegen staatliche Kontrolle zu demonstrieren. Obwohl «Anonymous» mehrfach betont, ein Kollektiv von gleichgestellten Aktivisten zu sein, sind einige wenige Personen als treibende Kräfte der Bewegung zu sehen. Bei diesen dürfte es sich um einigermassen versierte Nutzer handeln, welche der grossen Masse Möglichkeiten eröffnen und Drall geben. Diese Positionen können aber ebenfalls von beliebigen Personen – auch kurzfristig – eingenommen werden. Eine Analyse zur Mitgliederstruktur ist in Kapitel 5.2 zu finden.

4.4 Mutmasslicher staatlicher Akteur spionierte jahrelang weltweit Computersysteme aus, darunter auch die UNO in Genf und das IOC

Die Sicherheitsfirma McAfee hat am 3. August 2011 Informationen über einen koordinierten Angriff auf verschiedene Firmen, Behörden und Organisationen veröffentlicht. Aufgrund einer Fehlkonfiguration konnte die Sicherheitsfirma auf einem Kontrollrechner der Angreifer *Log-Dateien* finden, in denen Zugriffsaktivitäten seit 2006 protokolliert wurden. Die Analyse dieser Dateien gab Rückschlüsse darauf, wen die Angreifer attackiert hatten und wie lange diese Attacken jeweils dauerten. Die Entdeckung dieses Angriffs soll nach Angaben des Sicherheitsunternehmens McAfee zu den grössten bisher bekannten Spionageangriffen gehören. Seit 2006 wurden demnach 72 Firmen, Organisationen und Regierungen systematisch ausgespäht, darunter auch der UNO Sitz in Genf und der Hauptsitz des Internationale Olympische Komitee (IOC) in Lausanne. Der grösste Teil der angegriffenen Netzwerke befindet sich jedoch in den USA. Es handelt sich dabei um Firmen von Satellitenkommunikationsgesellschaften, diverse Sicherheitsfirmen und auch eine Produktionsfirma für Solarzellen. Konkrete Firmennamen wurden nicht genannt. Daneben sollen auch Regierungsstellen der USA, Kanada, Indien, Vietnam und Taiwan betroffen sein. Über die Art der erbeuteten Informationen gibt es nur die Aussage des Sicherheitsunternehmens, dass die «erbeuteten Informationen in den falschen Händen eine massive wirtschaftliche Bedrohung darstellen kann.»[19]

Bei der Infektion nutzten die Angreifer traditionelle Infektionsmethoden wie gezielte E-Mails und präparierte Links. Die Betroffenen erhielten auf sie zugeschnittene E-Mails mit gefälschten Absender-Adressen. Sobald der Empfänger auf den Link geklickt hat, wird dann eine *Schadsoftware* geladen und installiert. Zusätzlich wird ein Kanal zum Kontrollserver geöffnet.

Ein staatlicher Akteur scheint in diesem Fall wahrscheinlich, da sich die erbeuteten Informationen von Kriminellen kaum verkaufen lassen dürften. Der Umstand, dass beispielsweise der Kontrollserver schlecht geschützt im Netz gestanden hat, zeigt entweder, dass die Angreifer im Absichern ihrer Infrastruktur ebenfalls nicht perfekt sind, oder aber, dass sie sich nicht oder nicht gross um deren Absicherung kümmern, da bereits genügend Alternativen vorhanden sind. Dieser Spionageangriff zeigt einmal mehr auf, dass es ein andauerndes Interesse an Daten und Informationen gibt, und der Druck auf sensible Daten jeden Tag zunimmt. Es ist davon auszugehen, dass weitere Spionagenetzwerke im Aufbau sind, andere bereits aufgebaut und möglicherweise aktiv sind, aber noch nicht entdeckt worden sind.

So werden auch weiterhin gezielte E-Mails versendet. Dies zeigt beispielsweise ein gezielter Angriff gegen Rüstungskonzerne im Juli 2011. Die Angreifer haben in diesem Fall professionell formulierte E-Mails an Mitarbeiter von Rüstungskonzernen gesendet, die für eine Konferenz des US-Verbands der Luft- und Raumfahrttechnik AIAA werben. Das vermeintlich als «geheim» klassifizierte Dokument hat die Empfänger dazu aufgefordert, bis zum 30. Juli Fachbeiträge für die bevorstehende Konferenz einzureichen.[20] E-Mails, die auf eine Konferenz Bezug nehmen sind besonders beliebt bei den Angreifern.

Zu bedenken ist, dass nicht nur international tätige Grosskonzerne Angriffsziel von Wirtschafsspionage sein können, sondern auch innovative kleine und mittelständische Unternehmen.

---

19 http://www.spiegel.de/netzwelt/web/0,1518,778126-8,00.html (Stand: 23. Februar 2012).

20 http://www.heise.de/security/meldung/Gezielte-Angriffe-auf-Ruestungskonzerne-dauern-an-1282837.html (Stand: 23. Februar 2012).

Immer wieder wird die Täterschaft aus China vermutet, welche hinter solchen Angriffen stehen könnte, was durch die chinesische Regierung aber stets bestritten wird. Tatsächlich ist es schwierig, die Täterschaft hinter einem Angriff eindeutig festzustellen, da die einzigen Spuren bei solchen Attacken meist *IP-Adressen* sind. Wenn eine *IP-Adresse* aus China stammt, ist dies jedoch kein Beweis, dass der Angreifer auch aus China stammt. Es ist beispielsweise relativ einfach in einem beliebigen Land *Server* zu mieten, über welche die Angriffe durchgeführt werden und die alleine dazu dienen, den Ursprungsort des Angriffs zu verschleiern. Und selbst wenn der Angriff wirklich aus China stammt, ist auch noch nicht geklärt, welche Täterschaft dahintersteckt. Laut einem Bericht im Wall Street Journal will der US-Geheimdienst 20 chinesische Hackergruppen ausgemacht haben, von denen eine Mehrzahl von Cyber-Angriffen gegen die USA ausgehen sollen.[21] Auch wenn laut Bericht 12 dieser Gruppen mit der chinesischen Volksbefreiungsarmee in Verbindung stehen, dürfte der Beweis, dass die Angriffe tatsächlich vom Staat in Auftrag gegeben werden, schwierig zu erbringen sein. Erschwerend kommt dazu, dass mehrere Staaten in der Lage sind, grössere Spionageoperationen über Netzwerke zu lancieren.

4.5 Diverse Hacking Angriffe

Auch im zweiten Halbjahr fanden diverse Hacking- und Spionageangriffe statt oder wurden publik. Nachfolgend sei eine nicht vollständige Liste an Beispielen gegeben:

Spionageangriff auf die US-Handelskammer

Wie das Wall Street Journal berichtete, sollen chinesische Hacker mindestens sechs Hintertüren im Rechnernetz der US-Handelskammer installiert haben. So konnte wahrscheinlich die Dachorganisation der US-Wirtschaft in Washington über Monate systematisch ausgeforscht werden. Die Sicherheitslücke wurde bereits im Mai 2010 entdeckt und geschlossen, der Vorfall wurde aber erst in der zweiten Jahreshälfte 2011 publik.[22]

Neuer Angriff auf Sonys Online Dienste

Nach dem Angriff auf Kundendaten von Sony im letzten Halbjahr ist es im Oktober 2011 Hackern erneut gelungen, in Nutzerkonten bei Sonys Online Diensten PlayStation Network (PSN) und Sony Entertainment Network (SEN) einzudringen. Dies sei in 93‘000 Fällen gelungen. Diese Kontodaten seien gesperrt worden und Kreditkartendaten seien diesmal nicht in Gefahr gewesen. Anders als beim ersten Fall wurde hier nicht direkt Sony angegriffen: Mit Hilfe von anderweitig beschafften Passwortinformationen wurde versucht, in die Konten zu gelangen. Die Erklärung ist simpel: Viele Computernutzer verwenden bei mehreren, wenn nicht sogar allen Diensten das gleiche Passwort. Die Inhaber der Accounts wurden per Mail benachrichtigt und mussten einen Authentifizierungsprozess durchlaufen, um ihr Konto wieder freizuschalten. Falls betrügerische Einkäufe im Sony-Netzwerk vorgenommen wurden, werde das Unternehmen das Geld erstatten, so Sony.

---

21 http://online.wsj.com/article_email/SB10001424052970204336104577094690893528130-lMyQjAxMTAxMDEwMjExNDIyWj.html; ganzer Bericht des Office of the National Counterintelligence Executive: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (Stand: 23. Februar 2012).

22 http://www.spiegel.de/netzwelt/netzpolitik/0,1518,805052,00.html (Stand: 23. Februar 2012).

Hacker greifen Südkoreanische Netzwerke an

Bei einem Hackerangriff in Südkorea sind Daten von etwa 35 Millionen Internetnutzern gestohlen worden. Wie die Behörden des Landes Ende Juli mitteilten, wurden die Übergriffe auf die Onlineplattform Nate und das Soziale Netzwerk Cyworld von Computern mit *IP-Adressen* in China aus getätigt. Zu den illegal beschafften Daten zählten den Angaben zufolge unter anderem Telefon- und Sozialversicherungsnummern sowie E-Mail-Adressen und Passwörter. Die südkoreanische Polizei erklärte, die Ermittlungen würden vermutlich mehrere Monate dauern.[23]

4.6 Deaktivierung des Botnetzwerks «DNS-Changer»

Bei einer Infektion mit der *Schadsoftware* «*DNS*-Changer» wurde das *DNS-System* auf den betroffenen Computern so manipuliert, dass der *Webbrowser* die Benutzer bei Abfrage von populären Webseiten unbemerkt auf manipulierte Seiten umleitete.

Im November 2011 wurden die kriminellen Administratoren dieses *Botnetzwerks* vom FBI verhaftet. Die manipulierten *DNS*-Server der Kriminellen wurden durch korrekt arbeitende, vom FBI betriebene *DNS*-Server ersetzt, damit keine weiteren Manipulationen mehr möglich sind.

Diese *Server* sollten am 8. März 2012 abgeschaltet werden, das FBI hat dann aber die Übergangsfrist bis zum 9. Juli 2012 verlängert. Ab diesem Datum können infizierte Computer keine Domain-Namen mehr auflösen und die betroffenen Nutzer demzufolge keine Webseiten mehr aufrufen. Je nach Einsatzart des Computers kann dies zu schwerwiegenden Problem führen.

SWITCH[24] und die deutschen Behörden haben deshalb Online-Tests bereitgestellt, bei dem sich auf einfache Weise überprüfen lässt, ob der eigene Computer von der *Schadsoftware* «*DNS*-Changer»[25] befallen ist.

Gemäss den MELANI vorliegenden Informationen soll das FBI innerhalb einer Woche 20'500 *IP-Adressen* allein aus der Schweiz identifiziert haben. Das bedeutet nicht, dass auch so viele Systeme infiziert sind, da es sich mehrheitlich um dynamische *IP-Adressen* handelt. Trotzdem sind möglicherweise mehrere Tausend PCs in der Schweiz mit der *Schadsoftware* «*DNS*-Changer» infiziert.

4.7 Strafverfolgungstrojaner

Am 8. Oktober 2011 gab der «Chaos Computer Club (CCC)»[26] bekannt, dass ihm ein Strafverfolgungstrojaner der deutschen Behörden zugespielt worden sei. Dieser Trojaner dient Ermittlern in Deutschland zur so genannten Quellen-Telekommunikationsüberwachung. Internettelefone, sogenannte *Voice-over-IP-Gespräche* (VoIP) können so schon vor ihrer Verschlüsselung beim Sender oder nach der Entschlüsselung beim Empfänger abgehört werden.

---

23 http://www.tagesanzeiger.ch/digital/internet/Hacker-greifen-suedkoreanische-Netzwerke-an/story/31054597 (Stand: 23. Februar 2012).

24 http://www.dns-check.ch (Stand: 23. Februar 2012).

25 http://www.dns-ok.de (Stand: 23. Februar 2012).

26 http://www.ccc.de (Stand: 23. Februar 2012).

In der Diskussion wurde dieser Trojaner häufig undifferenziert als «Bundestrojaner» bezeichnet und deshalb fälschlicherweise mit nachrichtendienstlichen Spionageprogrammen und dem grossen Lauschangriff gleichgesetzt. Die Rechtsgrundlagen für die unterschiedlichen Einsatzarten dürfen jedoch nicht vermischt oder verwechselt werden.

Der CCC hat den Strafverfolgungstrojaner untersucht und den Behörden vorgeworfen, dass seine Funktionen nicht darauf beschränkt sind, Gespräche aufzuzeichnen, sondern auch Möglichkeiten bietet, Daten auf dem Computer zu lesen und diese weiterzuleiten. So können beispielsweise Inhalte des *Webbrowsers* mit Hilfe von Screenshots ausgelesen werden. Eine Fernzugriffsmöglichkeit soll zudem das Nachladen beliebiger Funktionen ermöglichen. Auch die Verschlüsselung ist vom CCC kritisiert worden: Die ausgehende Kommunikation sei nur *symmetrisch verschlüsselt*, bei der eingehenden Kommunikation fehle die Verschlüsselung gänzlich. Dies spielt besonders eine Rolle, da Daten und Kommandos angeblich nicht über deutsche, sondern über ausländische *Server* abgewickelt werden. Der Trojaner soll zudem Sicherheitslücken enthalten, welche grundsätzlich durch Dritte ausgenutzt werden könnten um selbst Zugang zum überwachten Computer zu erlangen.

Auch in der Schweiz wurde nach diesem Vorfall über den Einsatz von Strafverfolgungstrojanern diskutiert. Die Bundeskriminalpolizei setzte Trojaner in der Schweiz in vier Fällen ein - dreimal in der Terrorismusbekämpfung und einmal gegen organisierte Kriminalität. Der Kanton Zürich ist mindestens ein Mal mit einem Trojaner gegen Drogenhändler vorgegangen[27]. Die Schweizer Piratenpartei hat nach Bekanntwerden dieser Trojanereinsätze bei der Bundesanwaltschaft eine Klage wegen der Verwendung von Spionage-Software im Kampf gegen Terrorismus und organisierte Kriminalität eingereicht. Die Bundesanwaltschaft verfügte indes die Nichtannahme der Klage.[28]

Bereits vor dem Internetzeitalter durften Strafverfolgungsbehörden Telefongespräche von verdächtigen Personen abhören, wenn für den konkreten Fall eine richterliche Genehmigung vorlag. Die Anbieter von Fernmeldediensten sind gesetzlich verpflichtet, den Strafverfolgungsbehörden solche Überwachungen zu ermöglichen.[29]

Mit der Verbreitung von alternativen Kommunikationstechnologien ergeben sich bei Ermittlungen der Strafverfolgungsbehörden neue Herausforderungen. Da bei der Internettelefonie (z.B. Skype) kein klassischer Telefondienstanbieter mehr die Gesprächsdurchleitung vornimmt und die Kommunikation verschlüsselt durch die Leitungen geht, ist eine Überwachung nur noch an den Endgeräten möglich. Um Überwachungen durchzuführen, dürfen im Strafverfahren technische Hilfsmittel eingesetzt werden.[30] Bei der Internettelefonie kann dies ein Programm sein, welches auf den Computer der Zielperson eingeschleust wird und in der Folge deren Kommunikation vor der Verschlüsselung abgreift und an die Strafverfolgungsbehörden sendet.

Ob die aktuellen[31] rechtlichen Grundlagen in der Schweiz für diese Art der Überwachung ausreichen, ist in der juristischen Lehre wie auch in der Politik umstritten.[32] Dabei hilft es der

---

27 http://www.nzz.ch/nachrichten/politik/schweiz/trojaner_im_fall_stauffacher_eingesetzt_1.12994241.html (Stand: 23. Februar 2012).

28 http://www.aargauerzeitung.ch/schweiz/anzeige-der-piratenpartei-zu-spionage-software-bleibt-ohne-folgen-115718001 (Stand: 23. Februar 2012).

29 Siehe Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs BÜPF und die zugehörige Verordnung VÜPF: http://www.admin.ch/ch/d/sr/c780_1.html (Stand: 23. Februar 2012) und http://www.admin.ch/ch/d/sr/c780_11.html (Stand: 23. Februar 2012).

30 Art. 280 Schweizerische Strafprozessordnung: http://www.admin.ch/ch/d/sr/312_0/a280.html

31 Die Schweizerische Strafprozessordnung ist erst seit dem 1.1.2011 in Kraft, vorher hatte jeder Kanton wie auch der Bund je ein eigenes Verfahrensrecht.

Klärung der Thematik nicht, dass in den Diskussionen regelmässig Strafverfolgung und Nachrichtendienste sowie Telefonüberwachung und Online-Durchsuchung von Computern miteinander vermischt werden. Es gilt zum Einen auf der rechtspolitischen Seite die verschiedenen Entitäten und Massnahmen einzeln zu behandeln und zum Anderen auf der Anwendungsseite den Funktionsumfang der Software auf die genehmigten Eingriffe zu beschränken sowie eine Funktionsänderung respektive einen Missbrauch der verwendeten Methoden auszuschliessen. Es geht nicht an, dass eine Abhörsoftware, welche für das Mitschneiden von VoIP-Gesprächen eingesetzt werden soll (und darf), beispielsweise auch die Erstellung von Screenshots ermöglicht oder E-Mails abgreift. Erst recht problematisch wird es, wenn nicht ausgeschlossen werden kann, dass unbefugte Dritte Kenntnis der erhobenen Daten erhalten geschweige denn Manipulationen an der im Einsatz befindlichen Software vornehmen könnten. Die Sicherheit muss beim Einsatz entsprechender Mittel höchste Priorität haben.

Abschliessend bleibt festzuhalten, dass sowohl die Hürden für eine «normale» Telefonüberwachung als auch die Hürden für eine allfällige Internet-Telefonüberwachung hoch sind: In der Schweiz kann nur nach richterlicher Genehmigung, bei bestimmten schweren Delikten, und wenn «die bisherigen Untersuchungshandlungen erfolglos geblieben sind oder die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden» eine Überwachung gerechtfertigt werden.[33] Das Prinzip der Verhältnismässigkeit muss hier wie bei jedem Eingriff in Grundrechte berücksichtigt werden.

4.8 Handel von Überwachungs- und Forensiksoftware durch Wikileaks veröffentlicht

Seit dem 1. Dezember 2011 veröffentlicht WikiLeaks zusammen mit Medienpartnern in der ganzen Welt Dokumente, die darlegen sollen, dass der Markt für IKT-Sicherheits-, Überwachungs- und *Forensik*lösungen nicht nur mit Regierungsbehörden demokratischer Staaten floriert, sondern auch Geschäfte mit so genannten Unrechtsstaaten gemacht werden. Die überwiegende Mehrheit dieser Dokumente sind Verkaufsbroschüren, öffentliche Präsentationen und Preislisten von rund 100 Unternehmen aus den Bereichen globale Sicherheitslösungen sowie IKT-Sicherheit und –Forensik, darunter DigiTask und Siemens aus Deutschland, FoxIT aus den Niederlanden, Dreamlab Technolgies AG aus der Schweiz und Hewlett Packard aus den USA.

Nach dem Fall verschiedener Regimes im arabischen Raum wurden Dokumente publik, die aufzeigen, dass zumindest Offerten existierten, in denen einige dieser Unternehmen ihre Produkte den ehemaligen Machthabern anboten. Nach dem Fall der ägyptischen Regierung wurde öffentlich, dass die Deutsch-Englische Gamma Gruppe ihre Produkte dem Mubarak-Regime anbot. Im Falle von Libyen soll die Regierung Gaddafis die IKT-Lösungen der französischen Amesys für ihr «Public Safety System and Passport Network» eingesetzt haben.[34] Auch in Syrien wird angeblich Überwachungssoftware westlicher IKT-Firmen eingesetzt. Neben einer Software der deutschen Firma Utimaco, die abgehörte Telefonleitungen mit den Rechnern in seinem Überwachungszentrum verbindet, kommt auch Software zur Mail-

---

32 Der Einsatz von Überwachungssoftware ist in der Schweiz nur bei der Strafverfolgung möglich, im Umfeld von Nachrichtendiensten ist ein solcher Einsatz in der Schweiz nicht erlaubt.

33 Art. 269 Schweizerische Strafprozessordnung: http://www.admin.ch/ch/d/sr/312_0/a269.html (Stand: 23. Februar 2012).

34 http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html (Stand: 23. Februar 2012).

Archivierung der US-Firma NetApp zum Einsatz. Von der französischen Firma Qosmos soll die Technik zur Überwachung von Kommunikationsnetzen stammen. Die Hersteller sollen jedoch niemals direkt an Syrien geliefert haben.[35]

Im jetzigen «Enthüllungsfall» wird seitens WikiLeaks und diverser Gruppierungen zur Stärkung der Informationsfreiheit ebenfalls damit argumentiert, dass diese Art von Technologietransfer zu Unrechtssystemen nicht nur moralisch und ethisch verwerflich sei, sondern die Mithilfe zur Überwachung und damit Unterdrückung der Bevölkerung in diesen Ländern auch Menschenleben forderte. Allerdings wird auch ganz generell der Verkauf solcher Produkte an westliche Strafverfolgungsbehörden, Nachrichtendienste und Militärs angeprangert. WikiLeaks macht denn auch in ihrem Editorial klar, dass der Einsatz von solchen IKT-Überwachungslösungen und der daraus resultierende Markt prinzipiell störend seien, sowie entsprechende gesetzliche Bestimmungen zur Kontrolle solcher «Datenwaffen» gänzlich fehlen. Die von WikiLeaks genannten Unternehmen sind im Bereich der IKT-Forensik, *Lawful Interception* und der so genannten *Data Retention* tätig (Siehe auch Kapitel 5.3).

Interessanterweise werden in diesen unter dem Namen «Spy Files» veröffentlichten Dokumenten nur westliche Anbieter genannt. Aufsteigende asiatische Unternehmen, welche Programme für flächendeckende Überwachung und Nachrichtendienstliche Auswertungen oder generell für die Innere Sicherheit anbieten und sich auf Nutzeridentifizierung, Zensurmassnahmen, Überwachung von Sozialen Netzwerken oder HTTPS-Verbindungen spezialisiert haben, bleiben unerwähnt. Bei diesen Newcomern auf dem Sicherheitsmarkt gibt es wenig Hemmungen, Überwachungssoftware an interessierte Staaten unabhängig von deren inneren Ordnung zu verkaufen.

4.9 Strategien und Übungen

Neue EU-Strategie für Sicherheit in den Netzen

Die Europäische Union hat eine «grosse europäische Strategie für die Sicherheit der europäischen Netze» im kommenden Jahr angekündigt. In einem Schreiben an die zuständigen Ministerien in den Mitgliedsländern werden zunächst die jeweiligen «Sicherheitskapazitäten» ermittelt. Die EU müsse politisch in diesem Bereich noch zulegen und weist der Europäischen Agentur für Netz- und Informationssicherheit ENISA[36] eine Schlüsselrolle für ihre Strategie zu.[37]

Länderübergreifende Krisenmanagement-Übung im Bereich IKT in Deutschland

Am 30. November und 1. Dezember 2011 hat das Bundesministerium des Innern insbesondere mit den Bundesländern Hamburg, Thüringen, Sachsen, Hessen und Niedersachsen erstmals die Bewältigung einer bundesweiten Krise infolge von Cyber-Attacken geübt. Im Verlauf dieser sogenannten LÜKEX-Übung (Länder Übergreifende Krisenmanagement-Übung/EXercise), die mit unterschiedlichen Themenstellungen alle zwei Jahre stattfindet, wurde das Zusammenwirken von mehreren betroffenen Ressorts auf Bundesebene mit den Krisenstäben der Länder sowie ausgewählten Unternehmen trainiert. Der diesjährigen Übung lag eine fiktive Übungsanlage zugrunde, welche die Krisenstäbe in Bund und Ländern

35 http://www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html (Stand: 23. Februar 2012).

36 http://www.enisa.europa.eu (Stand: 23. Februar 2012).

37 http://www.heise.de/security/meldung/Neue-EU-Strategie-fuer-Sicherheit-in-den-Netzen-angekuendigt-1394814.html (Stand: 23. Februar 2012).

mit einer ganzen Reihe von Schadensereignissen (u.a. massiven *Spam*-Angriffen, Schadprogrammen sowie einer mutwillig herbeigeführten Überlastung von Systemen) in den Verwaltungen sowie beteiligten Wirtschaftsunternehmen konfrontiert hat. An der Übung haben insgesamt 2.500 Beteiligte aus 12 Bundesländern teilgenommen.

Im Fokus der Übung standen die Bund-Länder-Abstimmung zur Analyse der Ursachen der IKT-Angriffe sowie Präventionsmassnahmen auf der politischen und administrativen Ebene. Geübt wurde ausserdem die Koordinierung von Maßnahmen zum Schutz der Bevölkerung sowie der Unternehmens- und Verwaltungsnetze und das Zusammenwirken von öffentlichen und nicht-öffentlichen Organisationen auf Bundes- und Landesebene. Gemeinsam mit allen Beteiligten wird die Übung in den kommenden Monaten detailliert ausgewertet. Ziel ist es, Verbesserungen in den Krisenplanungen und Managementabläufen zu erreichen.[38]

Die Schweiz und insbesondere Vertreter der Bundeskanzlei sowie der "nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken" nahmen bei der Übung LÜKEX als Beobachter teil. In der Schweiz werden ähnlich zur LÜKEX strategische Führungsübungen durchgeführt. Das Thema der nächsten Übung dieser Art wird ebenfalls ein Cyberangriff auf die Schweiz sein. Der Bundesrat möchte damit die nationale Strategie zur Abwehr eines solchen Angriffs und insbesondere das Konzept zu deren Umsetzung prüfen. Die Übung wird aus vier Teilen bestehen und von September 2012 bis Mai 2013 stattfinden. Sie richtet sich an die Krisenstäbe der Departemente und an die übrigen Organe der Bundesverwaltung, die im Ereignisfall einberufen werden.[39]

Cyber Atlantic

Figur 10: Logo Cyber-atlantic 2011

Die erste Cybersecurity Übung zwischen der EU und den USA wurde am 3. November 2011 in Brüssel durchgeführt. Die eintägige Table-Top Übung «Cyber Atlantic 2011» untersuchte, wie im Fall eines Angriffs auf kritische Informationsinfrastrukturen die Zusammenarbeit zwischen der EU und den USA funktioniert. Dabei wurden die Szenarien *Advanced Persistent Threat (APT)* und Angriff auf ein *SCADA*-System im Energiesektor simuliert. Mehr als 20 Länder waren in die Übung involviert, 16 davon nahmen an der Übung aktiv teil. Die Übung ist Teil einer EU-US Vereinbarung im Bereich Cyber Security, welche am EU-US Gipfel in Lissabon am 20. November 2010 beschlossen worden ist.[40] Die Schweiz nahm bei der Übung Cyber Atlantic 2011 als Beobachterin teil und konnte so wertvolle Erkenntnisse für die internationale Koordination bei Cybervorfällen sammeln.

---

38 Pressemitteilung des deutschen Bundesministeriums des Innern: http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/12/luekex.html?nn=109632 (Stand: 23. Februar 2012).
Eine Übersicht an vergangenen Übungen: https://www.bsi.bund.de/DE/Themen/IT-Krisenmanagement/IT-Krisenreaktionszentrum/Uebungen/Beispiele/beispiele_node.html (Stand: 23. Februar 2012).

39 http://intranet.bk.admin.ch/aktuell/media/03238/index.html?lang=de&msg-id=43517 (Stand: 23. Februar 2012).

40 http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011 (Stand: 23. Februar 2012).

5 Vertiefte Analysen und Trends

5.1 SmartGrid und Hausautomation

SCADA-Systeme (Supervisory Control and Data Acquisition) werden wie bereits in den Kapiteln 3.9 und 4.2 erwähnt vor allem bei der Steuerung von Kraftwerken oder Transportsystemen, vermehrt aber auch in Häusern, Firmengebäuden und Hotels zur Steuerung von Heizung, Klimaanlage und Storen Systeme eingesetzt. Bei modernen Anlagen kann die Steuerung sogar mittels Tablets und Smartphones und entsprechender Apps vorgenommen werden. Der Wunsch, die Steuerung nicht nur in den eigenen vier Wänden im geschützten Hausnetz zu verwenden, sondern via Internet von überall her zu bedienen, liegt auf der Hand. Besonders bei Ferienwohnungen macht eine Fernsteuerung Sinn, um beispielsweise vor Ankunft den Boiler einzuschalten, die Wohnung angenehm zu temperieren oder einfach aus der Ferne zu kontrollieren, ob der Herd sowie alle Lichter ausgeschaltet sind und die Heizung einwandfrei funktioniert.

Doch auch hier muss man sich mit der Sicherheit beschäftigen. Die Systeme sind direkt mit dem Internet verbunden und sind deshalb prinzipiell auch den gleichen Gefahren wie Computersysteme ausgesetzt. Wie in Kapitel 3.9 beschrieben, wurde bei diversen Steuerungsanlagen von Hotels und Firmen mit Webzugriff schlicht vergessen, die Standardpasswörter zu ändern. Somit war es möglich, Zugriff auf diese Anlagen zu erhalten und diese vollständig zu kontrollieren. Was auf den ersten Blick als harmlos erscheint, kann weitreichende Konsequenzen haben, beispielsweise wenn im Winter in einem leer stehenden Haus die Heizung abgestellt wird oder wenn die Alarmanlage ebenfalls durch die Hausautomation gesteuert wird und so deaktiviert werden kann.

Auch in einem anderen Bereich werden wir zukünftig mit *SCADA*-Systemen in Berührung kommen. Die Umwälzungen im Energiebereich, gerade im Hinblick auf den langfristigen Atomausstieg, zwingt die Energieversorger nach Möglichkeiten zu suchen, die Energiestabilität zu gewährleisten, auch wenn immer weniger Bandenergie von Atomkraftwerken und immer mehr ungleichmässige Energie in Form von Wind- und Solarenergie zur Verfügung steht. Bei der Lösung dieses Problems soll das *SmartGrid* helfen. In einem ersten Schritt wird zur Erhöhung der Systemstabilität der Energieverbrauch direkt beim Verbraucher detektiert. Diese Angaben werden an eine Zentrale übermittelt. Während heute der Energieverbrauch zu einem grossen Teil auf Schätzungen und Erfahrung basiert, wird es dann möglich sein, diesen viel genauer zu bestimmen und so eine verbesserte Systemstabilität zu garantieren. Kommen diese Daten aber in die falschen Hände oder wird ein solcher *SmartMeter* gehackt, kann beispielsweise anhand von Stromdaten analysiert werden, ob jemand zu Hause ist oder nicht oder man kann auch direkt die Stromrechnung manipulieren.

In einem zweiten Schritt ist es vorstellbar, dass auch Geräte wie Geschirrspülmaschine und Waschmaschine an das *SmartGrid* angeschlossen und von diesem kontrolliert werden. Durch den Endverbraucher wird dann der Zentrale signalisiert, dass dieser gerne die Waschmaschine starten möchte. Dies geschieht nicht unmittelbar, sondern die Steuerungszentrale entscheidet, wann der geeignete Zeitpunkt ist, um das entsprechende Gerät in Gang zu setzen.

Es ist klar, dass ein solches System sehr gut geschützt werden muss, da Fehlmanipulationen unter Umständen zu gravierenden Stromausfällen führen können. Im schlimmsten Fall kommt die gesamte Energieversorgung zum Erliegen.

5.2 Anonymous – die Vor- und Nachteile der offenen Struktur

«Anonymous» hat in den vergangenen Monaten mit diversen Operationen im Cyberspace für Aufregung gesorgt. Auf der Opferliste figurieren prominente Firmen wie Sony, die Bank of America, die Sicherheitsfirma Stratfor (siehe Kapitel 4.3) oder sogar kriminelle Gruppierungen wie die mexikanische Drogenmafia «Los Zetas».

In der Schweiz hat vor allem die «Operation Payback» für Aufsehen gesorgt, bei welcher unter anderem die Postfinance nach der Sperrung des Kontos des WikiLeak Gründers Julian Assange angegriffen worden ist. Doch wer steckt eigentlich hinter Anonymous und diesen Angriffen? Gemäss verschiedenster Aussagen ist Anonymous keine Organisation oder Gruppe im eigentlichen Sinn, die über Statuten verfügt und bei der man eine Mitgliedschaft beantragt und Beiträge bezahlt. Anonymous ist vielmehr eine Idee respektive Lebenseinstellung[41]. Die Unterstützung ist an keine Form gebunden. Jede und jeder «Anon» macht somit, was sie oder er kann und für richtig hält. Diese Definition hat auf der einen Seite den Vorteil, dass die Hemmschwelle sinkt, bei Anonymous mitzumachen und das Momentum eines aktuellen Unmutes gegen eine Firma und einen Staat von Initianten ausgenutzt werden kann, bevor sich Teilnehmer an Aktionen über die Konsequenzen zu sehr Gedanken machen (können). Auf der anderen Seite birgt diese Art der Struktur auch Gefahren – unter anderem für die Bewegung selbst. Da alle «Anons» selbst entscheiden, was sie für richtig halten, können mitunter auch Aktionen angekündigt oder durchgeführt werden, die nicht unbedingt der Mehrheits- geschweige denn der Gesamtmeinung von Anonymous entsprechen.

Das beste Beispiel dafür war die Ankündigung, Anonymous werde Facebook am 5. November 2011 angreifen – mit dem Ziel, dass auf Grund dieses Angriffs «möglichst viele Benutzer Facebook verlassen».[42] Dies hatte naturgemäss ein grosses Medienecho zur Folge – passiert ist am 5. November jedoch nichts. Die Ankündigung hat nicht nur in der Presse zu Diskussionen geführt, sondern auch in den Reihen von Anonymous selbst. So wurde von anderen «Anons» der geplante Angriff als Werk eines verwirrten Einzelkämpfers und die Ankündigung als «imaginär» bezeichnet, obschon es aus Sicht von Anonymous wohl durchaus Gründe gibt, eine solche Aktion durchzuführen. Der Name des Initianten wurde anschliessend offengelegt, was wohl als grösste Strafe innerhalb von Anonymous angesehen werden dürfte.[43]

Aber auch beim Angriff auf Stratfor häuften sich verschiedene Motive, Dementis und Dementis der Dementis. Nachdem sich Anonymous zuerst zur Aktion mit dem Namen «LulzXmas» bekannt hat und dazu aufgefordert hatte, mit den gestohlenen Kreditkartendaten Überweisungen an wohltätige Organisationen zu tätigen, kursierte im Internet im Namen von Anonymous auch ein Dementi, das anschliessend wieder dementiert wurde. Wieder in einem anderen Beitrag wurden die wahren Gründe des Angriffs in der Offenlegung der Kontakte zu Geheimdiensten und der Rüstungsindustrie angegeben.[44] Doch gerade der Fall Stratfor beleuchtet einen weiteren Aspekt: Unter dem Deckmantel von Anonymous könnten sich auch Kriminelle mit rein finanziellen Absichten und ohne grosse Visionen verstecken. Die Kreditkartendaten wurden nicht nur verwendet, um angeblich 1 Million Dollar an wohltätige Organisationen zu transferieren. Sie wurden zusätzlich ins Netz gestellt, wo sie für alle Kriminellen

---

41 http://www.format.at/articles/1131/524/303276_s1/format-chat-anonymous-mitglied-tvxor (Stand: 23. Februar 2012).

42 https://www.taz.de/!81221/ (Stand: 23. Februar 2012).

43 http://www.golem.de/1111/87543.html (Stand: 23. Februar 2012).

44 http://www.n-tv.de/technik/Hacker-Angriff-gibt-Raetsel-auf-article5086791.html (Stand: 23. Februar 2012).

(und den Rest der Welt) frei verfügbar waren und für beliebige Zwecke eingesetzt werden konnten.

Die lockere Anbindung bei Anonymous resultiert in einer Reihe unkoordinierter, mehr oder weniger spektakulärer 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 Angriffe ausüben oder Mitteilungen veröffentlichen. Dahingehend ist es müssig, nach einem Angriff oder nach der Veröffentlichung von Daten jeweils zu diskutieren, ob es sich nun um Anonymous oder nicht um Anonymous gehandelt haben soll. Demgemäss sind auch Bekennerschreiben und Dementi einzuordnen.

5.3 «Gute» und «Böse» Überwachung im Internet

Mit der Analyse des deutschen Strafverfolgungstrojaners (umgangssprachlich auch Bundestrojaner) durch den «Chaos Computer Club» und der Veröffentlichung des Funktionsumfanges, wurden die Diskussionen rund um deren Einsatz nicht nur in Deutschland, sondern auch in der Schweiz neu entfacht. Zudem begann WikiLeaks am 1. Dezember 2011 mit der Publikation zahlreicher Dokumente, die darlegen sollen, dass private Sicherheitsunternehmen IKT-Lösungen an Staaten mit vorwiegend autokratischen Regierungen und mangelndem Menschenrechtsbewusstsein verkaufen. Viele dieser Lösungen stammen aus dem Umfeld der so genannten *Lawful Interception* und der IKT-Forensik und erlauben es den jeweiligen Behörden, die Internet und Mobiltelefon gestützte Kommunikation ihrer Bürger abzuhören, mitzuschneiden oder aber Daten auf Computern auszuspähen.

Dieser an sich alten Diskussion, welche neu lanciert worden ist, liegt eines der fundamentalen Probleme des Internet, der vernetzten Gesellschaft und der IKT zu Grunde: Das Aufkommen immer neuer Möglichkeiten zu kommunizieren, Daten und Informationen auszutauschen und diese stets überall und jederzeit verfügbar zu haben, hat Folgen: Die Massnahmen zur Ortung und Beschaffung von Informationen und ganz generell die Arbeit der Sicherheitsbehörden eines Staates werden dadurch komplizierter. Diese Entwicklung macht beispielsweise bei einer gerichtlich angeordneten Abhörung einer Skype-Kommunikation den Einsatz von IKT-Lösungen, wie zum Beispiel Fremdprogrammen auf dem Computer des Verdächtigen nötig. Gerade jene Staaten, die eine repressive Politik gegenüber politisch Andersdenkenden verfolgen, stärken auf Grund der zunehmenden Möglichkeiten der Kommunikation im Inland, wie auch ins Ausland vermehrt die zentrale Kontrolle über die innerstaatlichen Netzwerke und deren Verbindungen ins Ausland. Dabei kommen hier zum Teil die gleichen IKT-Produkte und Lösungen zum Einsatz, wie sie in scheinbar besser funktionierenden Rechtsstaaten ebenfalls eingesetzt werden. Grund dafür ist, dass auf der technischen Ebene Internet Computer und Netzwerke überall gleich funktionieren und entsprechende IKT-Lösungen überall eingesetzt werden können, ganz egal wo sich diese IKT-Elemente befinden und welche rechtlichen Rahmenbedingungen vorherrschen.

Auf der rechtlichen Seite unterstehen IKT-Produkte, abgesehen von gewissen Restriktionen beim Handel mit Krypto-Lösungen, keiner Exportkontrolle. Diese liesse sich auch faktisch nicht umsetzen. Zum einen sind softwarebasierte IKT-Lösungen, wie sie nun von WikiLeaks angeprangert werden, praktisch immer so genannte *Dual-Use-Güter*, und zum anderen bestehen sie aus Programm*code* - sind also physisch nicht vorhanden - und können jederzeit von einem Ort zum anderen verschickt werden. Ironischerweise wäre ein solches Exportregime weltweit nur mit einer totalen Kontrolle des ganzen Internets und dessen Datenströmen durchsetzbar.

Aufgrund der Tatsache, dass sich verschiedenste Vorgänge immer mehr über das Internet abspielen, ist klar, dass seitens der Sicherheitsbehörden eines Landes eine Nachfrage nach

IKT-Lösungen in der einen oder anderen Form besteht. Nur so können sie im Rahmen der Rechtsstaatlichkeit weiterhin ihren Auftrag erfüllen. Eine scharfe Trennlinie, ab wann solche Lösungen nun im westlichen Verständnis von Staaten unrechtmässig eingesetzt werden, existiert nicht. Allerdings steht es jedem Staat frei, in dieser Sache verbindliche Regeln für seine heimische IKT-Industrie zu erlassen, was den Handel mit IKT-Lösungen betrifft, sowie gesetzlich klar zu regeln, in welchen Fällen solche Produkte von den eigenen Behörden eingesetzt werden dürfen. In der Schweiz sind diesen Arbeiten im Rahmen der Revision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs[45] (BÜPF) und weiteren Gesetzen in diesem Bereich begonnen worden oder sind bereits abgeschlossen.

5.4 Sicherheit im mobilen Zeitalter – Wie schütze ich mein Smartphone?

Wie neueste Statistiken zeigen[46], verfügt die Schweiz über rund vier Millionen Mobiltelefone, darunter 1,5 Millionen *Smartphones*[47]. Zwei Betriebssysteme sind weltweit und in der Schweiz marktbeherrschend: iOS von Apple mit rund 50 % Marktanteil bei den in der Schweiz verkauften Smartphones und Android von Google mit einem Marktanteil von rund 27 %. Auch bei den Tablets sind diese beiden Betriebssysteme am stärksten verbreitet.

In diesem Zusammenhang lässt sich eine immer grössere Konvergenz zwischen den Betriebssystemen für mobile Geräte und «klassischen» Betriebssystemen für *Desktops* feststellen. Das beweist das neue Apple Betriebssystem «Mountain Lion», das verschiedene iOS-Funktionen enthält, oder das neue «Windows 8», das in der *Desktop*- und in der Mobilversion über die gleiche graphische Oberfläche verfügen wird[48]. Diese Statistiken zeigen, dass wir uns in einer Übergangsphase befinden, die von *Desktop*-Systemen hin zu mobilen Systemen führt. Welche Bedeutung hat dies für die Sicherheit? Eine Analyse von iOS und Android soll dies näher beleuchten:

- Das Betriebssystem von Apple ist ein proprietäres System, das nur auf der Hardware dieses Unternehmens funktioniert. Solange ein Benutzer sein iOS nicht entsprechend manipuliert hat[49], kann er nur Anwendungen aus dem iTunes-Store installieren oder Anwendungen[50] «in house» ohne AppStore installieren, wenn er im «iOS Enterprise Program» mitmacht. Für das iOS-System kann jeder und jede Anwendungen entwickeln. Bevor diese auf den Markt gelangen können[51], müssen sie jedoch zuerst von Apple analysiert und akzeptiert werden. In der Folge werden die Anwendungen direkt von Apple signiert und im iTunes-Store angeboten. Dem Benutzer ist es allerdings nicht möglich, die einer Anwendung zugeteilten Rechte einzusehen.

---

45 http://www.admin.ch/ch/d/sr/c780_1.html(Stand: 23. Februar 2012).

46 http://weissbuch.ch/wb11press.html (Stand: 23. Februar 2012).

47 Ein Smartphone ist ein mobiles Telefon, welches fortgeschrittene Funktionen wie beispielsweise den Internet-Anschluss oder die Verarbeitung persönlicher Daten mit der Grundaufgabe eines Telefons vereint. Die andere Kategorie von modernen Mobiltelefonen wird «Feature Phones» genannt. Diese mobilen Telefone verfügen nur über einige Zusatzfunktionen. Sie sind somit in der Entwicklung nicht so komplex wie die Smartphones.

48 Das nächste Windows 8 Metro scheint den Start-Button, der den Microsoftbenutzern so am Herzen liegt, bereits verloren zu haben: http://arstechnica.com/microsoft/news/2012/02/discoverability-windows-8-and-the-disappearance-of-the-start-button.ars (Stand: 23. Februar 2012).

49 Diese Operation wird in der iOS-Welt als «Jailbreak» bezeichnet.

50 Dank dem Programm «iOS Developer Enterprise» kann eine Firma beispielsweise einen eigenen App Store entwickeln: https://developer.apple.com/programs/ios/enterprise/ (Stand: 23. Februar 2012).

51 https://developer.apple.com/appstore/guidelines.html (Stand: 23. Februar 2012).

- Das Android-System beruht hingegen auf einer *Open-Source*-Plattform mit Linux-Kernel und kann auf der Hardware verschiedenster Hersteller betrieben werden. Hauptvertriebspunkt der Anwendungen ist der Google Play Store (früher Android Market[52]) – mit einem einfachen Klick kann der Benutzer von jeglicher Website Anwendungen installieren[53]. Auch für Android kann jeder und jede Anwendungen entwickeln. Hier besteht hingegen kein Überprüfungsprozess, der demjenigen von Apple entspricht. Darüber hinaus *signiert* der Entwickler die Anwendungen selber. Der Endbenutzer hat hier die Möglichkeit, die Rechte der Anwendung einzusehen (allerdings nur, wenn er von der Website zum Google Play Store gelangt, da die Rechte typischerweise nicht direkt von der Anwendung des Smartphones angezeigt werden).

Vor kurzem veröffentlichte Symantec einen Bericht[54] darüber, wie die beiden Betriebssysteme versuchen, die Sicherheit des Endbenutzers zu gewährleisten. Der Bericht untersuchte die fünf folgenden Hauptpunkte:

1. **Traditionelle Zugangskontrolle:** Beispielsweise die Verwendung eines Passwortes, um Zugang zum Telefon zu erhalten, oder die Möglichkeit, dass das Gerät nach einer gewissen Zeit der Inaktivität den Zugang blockiert.
2. **Die Herkunft der Anwendungen:** Betrachtet wird hier hauptsächlich die *digitale Signatur*.
3. **Verschlüsselung:** Datenverschlüsselung bei Diebstahl oder Verlust des Gerätes.
4. ***Sandboxing*:** Der Versuch, die Anwendungen so zu isolieren, dass diese nur zu den von ihnen benötigten Prozessen Zugang erhalten
5. **Rechte der Anwendungen:** Den Anwendungen werden nur die Rechte zugeteilt, die diese unbedingt benötigen, um ihre Funktionen zu erfüllen.

Laut Bericht sind die Unterschiede zwischen den beiden Systemen offensichtlich. Kurz Zusammengefasst ist dabei der massgeblichste Faktor in der Herkunft der Anwendungen zu suchen. Diesbezüglich besteht ein offensichtlicher Gegensatz zwischen den beiden Philosophien. Apple übernimmt bezüglich der Sicherheit die Verantwortung[55] der zu installierenden Anwendungen. Auf der anderen Seite ermöglicht es der *Open-Source*-Ansatz von Android den Benutzern, beliebige Anwendungen zu installieren, allerdings ohne grosse Kontrolle und Einschränkungen bei der Funktionsweise respektive den benötigten Rechten zu haben. Man muss sich nur auf den Android Market begeben, um bereits auf der ersten Seite Spiele zu finden, die Bewilligungen erfordern, welche für den Zweck der Anwendung selber völlig unnötig sind. Dazu gehören beispielsweise das Recht zum Versenden und Erhalten von *SMS*, zum Tätigen von Anrufen und der Zugang zu auf dem Gerät gespeicherten persönlichen Daten[56].

Ein anderer Aspekt liegt darin, dass sich der Schutz vor *Schadsoftware* bei einem mobilen Gerät sehr davon unterscheidet, was man von *Desktop*-Systemen her gewohnt ist. In Zu-

---

52 Der Android Market wurde am 7. März 2012 durch den Google Play Store ersetzt

53 Dieser Vorgang wird als «Sideloading» bezeichnet.

54 http://www.symantec.com/podcasts/detail.jsp?podid=b-a-window-into-mobile-device-security (Stand: 23. Februar 2012).

55 Zumindest in einem Fall, demjenigen des amerikanischen Forschers Charlie Miller, war es möglich, die Sicherheit des App Stores auszuschalten und eine potenziell schädliche Anwendung zu veröffentlichen: http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (Stand: 23. Februar 2012).

56 Ein interessantes Beispiel ist dasjenige von Uloops, einer Anwendung, um Musikstücke zu komponieren. In der Beschreibung weisen die Entwickler darauf hin, dass die Anwendung Zugang zum Telefonstatus und zur Identität hat. Sie kann Informationen wie die interne ID des Telefons, Modell, Marke, Benutzername, Passwort und E-Mail und somit eine grosse Anzahl persönlicher Daten importieren. https://market.android.com/details?id=net.uloops.android&feature=featured-apps#?t=W251bGwsMSwxLDIwMywibmV0LnVsb29wcy5hbmRyb2lkIl0 (Stand: 23. Februar 2012).

kunft wird der Schutz von mobilen Geräten völlig neu überdacht oder die «alten» Ideen der *Desktop*-Systeme auch in die mobilen Geräte implementieren werden müssen:

- Antivirus:
  Bei den mobilen Systemen wird mit dem Betriebssystem kein Antivirenschutz vertrieben. Auf iOS kann nur Apple einen solchen Schutz anbieten, da ein Virenschutz Zugriff zu allen Anwendungen haben sollte, was installierten Anwendungen aber nicht erlaubt wird. Generell wird dies durch *Sandboxing* und durch die Rechtevergabe verhindert. Auf Android sind die einzigen wirksamen Antivirenprogramme kostenpflichtig. Trotzdem ist die kostenlose Anwendung von Creative Apps die am häufigsten vertriebene Antiviren-App. Laut einer Studie von AVTest[57] scheint diese keinen einzigen von 172 geprüften *Viren* erkannt zu haben.
- Firewall:
  Bis anhin liegen keine Studien vor, die *Firewalls* auf mobilen Geräten analysiert haben.
- Aktualisierungen des Betriebssystems und der Anwendungen:
  Für die Geräte mit unverändertem Betriebssystem (also ohne *Jailbreak* oder verändertem *ROM*), liefern nur Apple und einige Hardware-Produzenten, die Android implementieren, regelmässig Aktualisierungen. Der Grossteil der Hardware-Produzenten, die das Google-System verwenden, sind dazu allerdings nicht bereit. In der Folge existieren allfällige Sicherheitslücken so lange bis sich der Benutzer ein neues Gerät kauft.

Der Endbenutzer hat somit die schwierige Wahl: Entweder er entscheidet, sich Apple anzuvertrauen und in einem geschlossenes System[58] ohne grosse «Freiheiten» zu agieren, oder er entscheidet sich für ein *Open-Source*-System mit all seinen Vor- und Nachteilen[59], welches sich durch Offenheit und wenig Restriktionen auszeichnet.

5.5 Angriffe auf Anbieter von Zertifizierungsdiensten und deren Auswirkungen[60]

Der sichere Einsatz von *Kryptosystemen* mit *öffentlichen Schlüsseln (sog. «Public Key»-Kryptografie)* steht und fällt mit der Sicherheit der entsprechenden *Certification Service Provider (CSP)* und Public Key Infrastruktur (PKI)[61]. Entsprechend ist die Sicherheit von CSPs und PKIs immer schon ein Thema gewesen, mit dem sich Sicherheitstechniker befasst haben. Im Mittelpunkt des Interesses standen dabei Szenarien, bei denen entweder *Zertifikate* (über Schwachstellen in der Kollisionsresistenz der eingesetzten kryptografischen Hashfunktionen[62]) gefälscht oder Code-Signierzertifikate missbraucht worden sind. Im zweiten Fall

---

57 http://www.av-test.org/fileadmin/pdf/avtest_2011-11_free_android_virus_scanner_english.pdf (Stand: 23. Februar 2012).

58 Nebst den Vor- und Nachteilen der iOS-Architektur und des Marktmodells sind auch allfällige Überraschungen wie beispielsweise der Versand von GPS-Positionierungsdaten zu erwähnen. In Unkenntnis des Benutzers werden die Daten beim Backup an Apple weitergeleitet: http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking/ (Stand: 23. Februar 2012).

59 Auch in diesem Fall sind nebst der Architektur und dem Marktmodell weitere Faktoren zu berücksichtigen. Android überlässt dem Provider die Möglichkeit, das operative System zu ändern oder vor dem Telefonverkauf Anwendungen zu installieren. Dies gilt beispielsweise für die Anwendung Carrier IQ, die auf einigen Android-Geräten vorinstalliert ist. Sie zeichnet das Verhalten des Benutzers in umfassendem Mass auf und teilt dies dem eigenen Provider mit: http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ (Stand: 23. Februar 2012).

60 Auszug aus gleichnamigen Fachbericht abrufbar unter http://www.melani.admin.ch/dokumentation/00123/01132/index.html?lang=de

61 In diesem Sinne stellen die CSPs bzw. PKIs eine Achillesverse der «Public Key»-Kryptografie dar.

62 Dieser Punkt wird z.B. in der «Technologiebetrachtung: Kollisionsresistenz und Brechung kryptografischer Hashfunktionen» vom 4. August 2010 vertieft. http://www.isb.admin.ch/themen/sicherheit/00530/01276/index.html?lang=de (Stand: 23. Februar 2012).

erlaubt – wie der Stuxnet-Wurm gezeigt hat – ein solches *Zertifikat* z.B. das Einbringen von *Malware* in Form digital signierter Treibersoftware in ein Betriebssystem. Die jüngsten Angriffe auf CSPs haben nun aber gezeigt, dass auch die Kompromittierung eines CSP zwecks Ausgabe falscher *Zertifikate* eine reale Bedrohung darstellt. Mit Hilfe von falschen *SSL/TLS-Server-Zertifikaten* lassen sich grossflächige *Man-in-the-Middle* (MITM) Angriffe durchführen. Der Angreifer hat somit die volle Kontrolle über die übertragenen Daten, kann diese entschlüsseln und im Klartext aufzeichnen.

Wenn – wie in den vorliegenden Fällen – falsche *Zertifikate* ausgegeben werden, dann sind zunächst einmal zwei Punkte zu beachten:

- Einerseits versagen für solche *Zertifikate* alle im Einsatz stehenden Mechanismen auf der Basis von Sperrlisten (CRLs und/oder OCSP-Abfragen), um diese Zertifikate zurückzuziehen. Ein falsches (d.h. fälschlicherweise ausgegebenes) *Zertifikat* ist nicht zwingend gesperrt und entsprechend ist es auch nicht als solches erkennbar. Hier bräuchte es eine Unterscheidungsmöglichkeit für autorisierte (d.h. berechtigterweise ausgegebene) und nicht autorisierte *Zertifikate*.

- Andererseits hat sich gezeigt, dass das (zentralistische und hierarchische) Vertrauensmodell *ITU-T X.509* grundsätzlich problematisch ist. Wird in diesem Modell ein CSP bzw. eine als vertrauenswürdig anerkannte *Root Certificate Authority (Root CA)* kompromittiert, dann sind davon alle Entitäten betroffen, die sich auf diese CA berufen (im Extremfall können das alle Internet-Benutzer sein). Sicherheitstechnisch sitzen alle im gleichen Boot und die Wahrscheinlichkeit, dass eine Root CA kompromittiert wird, steigt mit der Länge der Liste.

Nach diesen Vorbemerkungen stellt sich die Frage, welche Vorkehrungen man treffen kann, um unter den gegebenen Umständen MITM-Angriffe bestmöglichst zu verhindern. Weil es nur wenig Lösungsansätze zur Verhinderung von MITM-Angriffen gibt, wird man versuchen müssen, MITM-Angriffe für den Angreifer möglichst schwer und aufwändig zu machen. Dabei gilt es zu unterscheiden, ob man am Vertrauensmodell Änderungen vornehmen kann oder nicht.

- Kann man am Vertrauensmodell keine Änderungen vornehmen, dann empfiehlt es sich, mit vorwiegend leeren Listen vertrauenswürdiger Root CAs bzw. mit einer selektiven Aufnahme von nur bestimmten Root CAs zu arbeiten. Google nutzt diese Möglichkeit bereits seit Chrome, Version 13, unter dem Begriff «Public Key Pinning». Will man den Ansatz auf beliebige Domänen verallgemeinern, dann bietet sich eine Verbindung zum Domain Name System (*DNS*) an.

- Kann man am Vertrauensmodell Änderungen vornehmen, dann kommen grundsätzlich neue Lösungsansätze in Frage. Hier böte sich ein Vertrauensmodell an, in dem Kompromittierungen auch nur lokale Auswirkungen haben. Ein solches Modell muss zwingend verteilt sein und dynamische Vertrauensbeziehungen unterstützen. Forscher der Carnegie Mellon Universität haben z.B. gezeigt, dass Angriffe meist lokal stattfinden, und dass man falsche *Zertifikate* deshalb im Abgleich mit geografisch verteilten Notariatsdiensten feststellen kann.

Wie jedes sozio-technische System verfügt auch ein CSP über Schwachstellen und Verwundbarkeiten, die im Rahmen von Angriffen adressiert und (mehr oder weniger gezielt) ausgenutzt werden können. Dabei beziehen sich die Schwachstellen und Verwundbarkeiten weniger auf die eingesetzten kryptografischen Verfahren und Mechanismen als auf die Schnittstellen zu den entsprechenden Zertifikatsausstell- und -ausgabeprozessen. Angriffe sind hier denkbar und – wie die jüngsten Angriffe dokumentieren – auch realisierbar. Als Analogie kann man einen Notengeldfälscher betrachten: Dieser kann entweder Notenscheine fälschen oder – was allerdings komplizierter und aufwändiger ist – in eine Notendruckzentrale einbrechen und die dort installierten Maschinen zur Ausgabe von regulären Noten-

scheinen missbrauchen. Es liegt auf der Hand, dass die zweite Möglichkeit zwar schwieriger zu realisieren dafür aber umso einträglicher ist. Ein analoger Angriff ist jetzt im PKI-Bereich gelungen und es ist möglich und wahrscheinlich, dass solche und ähnliche Angriffe in Zukunft wieder gelingen werden. Entsprechend lohnt es sich, solche Möglichkeiten in die Überlegungen zur Ausgestaltung zukünftiger PKIs mit einzubeziehen.

6 Glossar

.htaccess	.htaccess (englisch: hypertext access) ist eine Konfigurationsdatei, in der verzeichnisspezifische Einstellungen vorgenommen werden können.
«404 Not Found»	Eine Fehlerseite ist eine Webseite, die angezeigt wird, wenn man beispielsweise auf nicht mehr funktionierenden Link im Internet klickt bzw. eine nicht existente URL aufruft. Die meisten Browser zeigen dabei die vom Webserver gelieferte Standard-Seite. Fehlerseiten können vom Webmaster der Seite individuell angelegt werden.
AcceptPathInfo	Einstellung im Apache Webserver.
Admin-Schnittstelle oder Administrationspanel	Die Admin-Schnittstelle ist eine graphische Benutzeroberfläche, mit welcher ein Administrator Einstellungen tätigen kann.
Advanced Persistent Threat	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.
Apache Web-Server	Der Apache HTTP Server ist ein quelloffenes und freies Produkt der Apache Software Foundation und der meistbenutzte Webserver im Internet.
Backup	Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Base64	Base64 beschreibt ein Verfahren zur Kodierung von 8-Bit-Binärdaten (z.B. ausführbare Programme, ZIP-Dateien) in eine Zeichenfolge, die nur aus lesbaren Codepage-unabhängigen ASCII-Zeichen besteht.
Blog	Ein Blog ist ein auf einer Website geführtes und damit meist öffentlich einsehbares Tagebuch oder Journal, in dem mindestens eine Person, der Web-Logger - kurz Blogger - Aufzeichnungen führt, Sachverhalte protokolliert oder Gedanken

	niederschreibt.
Bot/ Botnetzwerke	Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen.
Browser	Computerprogramme, die vorwiegend dazu verwendet werden, verschiedene Inhalte im World Wide Web anzuzeigen. Die bekanntesten Browser sind Internet Explorer, Netscape, Opera, Firefox und Safari.
Building Management Systeme	Ein Building Management System (BMS) ist eine Software, mit der ein Gebäude, das über eine Gebäudeautomatisierung verfügt, visualisiert und gesteuert werden kann. Zu den üblichen Funktionen eines Building Management Systems gehören das Steuern von Licht- und Klimaanlagen.
Certificate Authority (CA)	Siehe Zertifizierungsstelle.
Certification Service Provider (CSP)	Siehe Zertifizierungsstelle.
Code	Programmanweisungen, die dem Computer die auszuführenden Befehle vorgeben.
Data Retention	Data Retention (deutsch: Vorratsdatenspeicherung) bezeichnet die Speicherung personenbezogener Daten durch oder für öffentliche Stellen, ohne dass die Daten aktuell benötigt werden.
Desktops	Ein Desktop-Computer, kurz «Desktop» ist ein Computer in einer Gehäuseform passend für den Einsatz als Arbeitsplatzrechner auf Schreibtischen.
Dial-up Modem	Bedeutet «Einwahl» und bezeichnet das Erstellen einer Verbindung zu einem anderen Computer über das Telefonnetz.
DNS-System	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
Dual-Use-Güter	Dual Use (engl. mit doppeltem Verwendungszweck) ist ein Begriff, der überwiegend in der Exportkontrolle angewendet wird und die prinzipielle Verwendbarkeit eines Wirtschaftsgutes (z.B. einer Maschine, aber auch Software und Technologie) sowohl zu zivilen als auch militärischen Zwecken kennzeichnet.

Event-Viewer	Programm, das Fehler- und Hinweismeldungen des Windows-Betriebssystems anzeigt.
Exploit	Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen.
Finanzagenten	Ein Finanzagent ist jemand, der sich als legaler Geldvermittler und damit auch im Finanz-Transfergeschäft betätigt. In jüngerer Zeit wird dieser Begriff in Zusammenhang mit illegalen Finanz-Transaktionen gebraucht.
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 dem jeweiligen Rechner – installiert.
Forensik	Unter dem Begriff Forensik werden die wissenschaftlichen Arbeitsgebiete zusammengefasst, in denen kriminelle Handlungen systematisch identifiziert (beziehungsweise ausgeschlossen), sowie analysiert oder rekonstruiert werden.
Georestriktionen	Einschränkungen beispielsweise beim Abrufen von Webseiten aufgrund der Länderzugehörigkeit der IP-Adresse, die man verwendet.
Harddisk	Hard Disk (deutsch: Festplattenlaufwerk) ist ein magnetisches Speichermedium der Computertechnik, welches Daten auf die Oberfläche einer rotierenden Scheibe schreibt.
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.
IP-Adressen	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
ITU-T X.509	X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate.
Jailbreak	Mit Jailbreaking (englisch: Gefängnisausbruch) wird das Überwinden der Nutzungseinschränkungen auf Apple Produkten mittels geeigneter

	Software bezeichnet.
Kommandoserver	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Kontrollsysteme	siehe SCADA
Kryptosysteme	Ein Kryptosystem ist ein System, dass zur Verschlüsselung eingesetzt wird. Kryptographie bedeutet ursprünglich die Wissenschaft der Verschlüsselung von Informationen.
Lawful Interception	Lawful Interception (deutsch: Telekommunikationsüberwachung) bezeichnet die Möglichkeit von Staaten, den Telekommunikationsverkehr von beispielsweise Sprache, Text, Bildern und Filmen überwachen zu dürfen.
Live-CD	Eine Live-CD beinhaltet ein bootfähiges Betriebssystem.
Log-Dateien	Eine Logdatei enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen von Prozessen auf einem Computersystem.
Man-in-the-Middle	Man-in-the-Middle Attacke. Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt und dadurch deren Datenaustausch mitlesen oder verändern kann.
Open-Source	Open Source ist eine Palette von Lizenzen für Software, deren Quelltext öffentlich zugänglich ist und durch die Lizenz Weiterentwicklungen fördert.
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 Absender-Adressen zustellen.
Public-Key-Infrastruktur, öffentliche Schlüssel	Public Key Infrastructure. Infrastruktur zur Verwaltung und zum Einsatz von digitalen Zertifikaten.
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 Lö-

	segeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Recovery Prozess	Recovery (deutsch: Datenwiederherstellung) bedeutet die Wiederherstellung von Originaldaten nach einem Datenverlust.
ROM	Read Only Memory Ein Speicher, bei dem Daten lediglich gelesen, nicht aber überschrieben werden können.
Root CA	Zentrale Zertifizierungsstelle
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
Sandboxing	Sandboxing ist eine Technik, die auf einem Computer eine abgeschottete Umgebung generiert, die für die Ausführung von nicht vertrauenswürdigen Programmen genutzt werden kann.
SCADA	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Schadsoftware, Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Screenshots	Unter einem Screenshot (deutsch Bildschirmkopie) versteht man in der IKT das Abspeichern des aktuellen graphischen Bildschirminhalts.
Server	Computersystem, welches den Clients bestimmte Ressourcen, wie z.B. Speicherplatz, Dienste (z.B. E-Mail, Web, FTP, usw.) oder Daten, anbietet.
Signieren/Signatur/ digitale Signatur	Unter einer digitalen Signatur versteht man mit elektronischen Informationen verknüpfte Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren und die Integrität der signierten elektronischen Informationen prüfen kann.
SmartGrid	Als SmartGrid wird ein intelligentes (Strom-) Netz bezeichnet, bei welchem Daten von verschiedenen Geräten (typischerweise den Zählern bei den Verbrauchern) aus dem Netz an die Betreiberin zurückgemeldet, und je nach Ausgestaltung auch Befehle an diese Geräte erteilt werden können.

SmartMeter	Ein SmartMeter (deutsch: intelligenter Zähler) ist ein Zähler für Energie, der dem jeweiligen Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigt, die auch an das Energieversorgungsunternehmen übertragen werden können.
Smartphones	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
SMS	Short Message Service. Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken (**S**tructured **Q**uery **L**anguage), die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder die Kontrolle über den Server zu erhalten.
SSL/TLS Serverzertifikat	SSL (Secure Socket Layer)-Serverzertifikat. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, in-dem sie diese mit ihrer eigenen digitalen Unterschrift versieht.
Stammzertifikaten	Zertifikat, welches dazu dient die Gültigkeit aller untergeordneten Zertifikate zu validieren.
Symmetrische Verschlüsselung	Bei der symmetrischen Verschlüsselung verwenden im Gegensatz zu einer asymmetrischen Verschlüsselung beide Teilnehmer den gleichen Schlüssel.
Treibersoftware	Ein Gerätetreiber, häufig kurz nur Treiber genannt, ist ein Computerprogramm oder Softwaremodul, das die Interaktion mit angeschlossenen Geräten steuert.
Tweet	Beiträge der Kommunikationsplattform Twitter.

URL-Manipulation	Mit bestimmten Manipulationen an der URL kann ein Server dazu gebracht werden, Seiten anzuzeigen, die eigentlich gesperrt sind.
USB	Universal Serial Bus. Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
Viren	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
Voice-over-IP-Gespräche	Voice over IP(VoIP). Telefonie über das Internet-Protokoll (IP). Häufig verwendete Protokolle: H.323 und SIP.
Webseiteninfektionen	Infektion eines Computers mit Malware allein durch den Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Zertifikate	Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.
Zertifizierungsstelle	Eine Zertifizierungsstelle ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermassen das Äquivalent eines Personalausweises im virtuellen Raum und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht.