Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

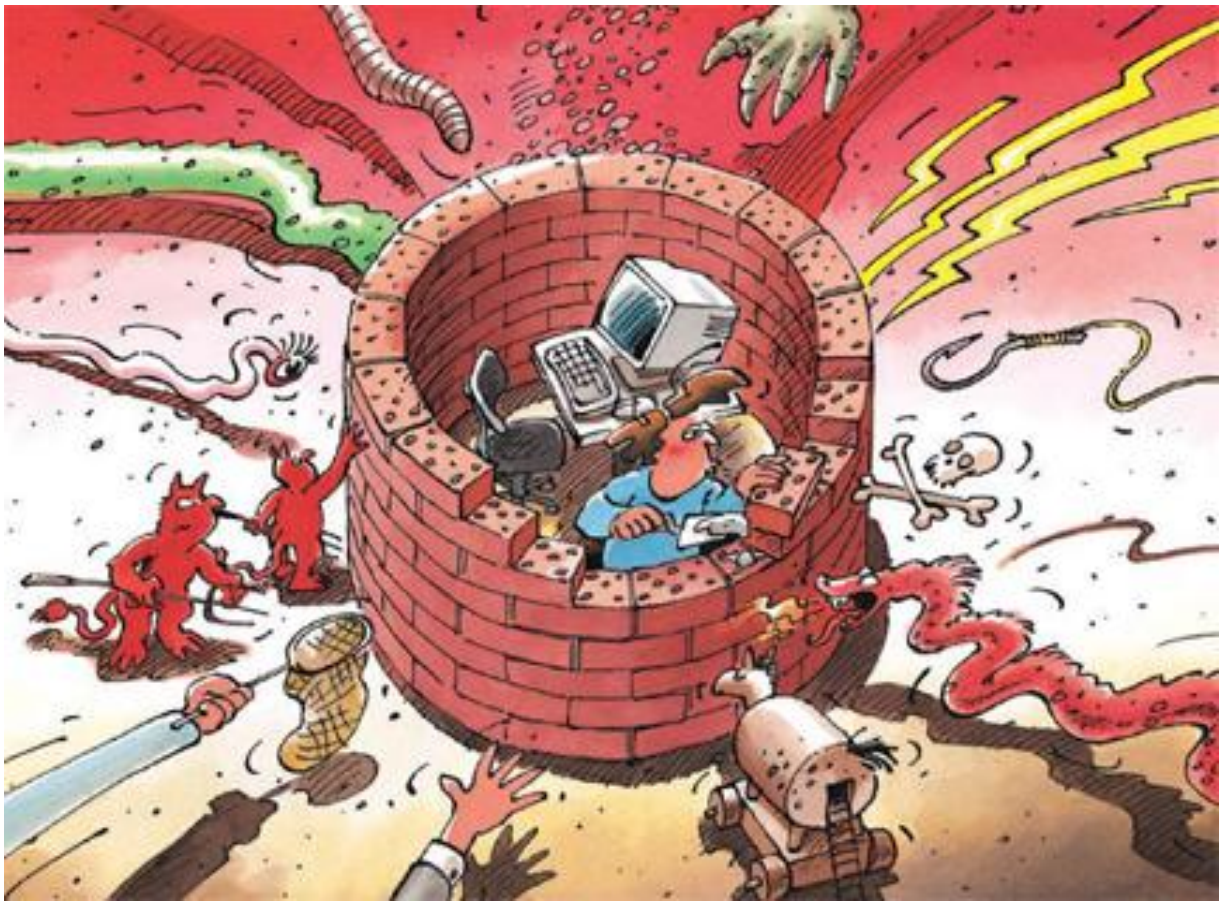
Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2010/I (Januar – Juni)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2010/I

Spionage mit IT Mitteln – Wachsende Gefahr

Im letzten Halbjahr wurden wieder einige Spionagevorfälle bekannt, so beispielsweise gegen Google, Adobe und auch gegen das Büro des Dalai Lama. Der deutsche Innenminister Thomas de Maizière warnte dann auch im jüngsten deutschen Verfassungsschutzbericht vor der Gefahr der wachsenden Wirtschaftsspionage. Besonders gefährdet seien Wirtschaftsunternehmen und öffentliche Stellen. Die bekannt gewordenen Spionagefälle sind nicht als unabhängige Einzelfälle zu betrachten, vielmehr muss auf Gemeinsamkeiten beispielsweise bei der Infrastruktur geachtet werden. Es braucht deshalb eine gesamtheitliche Analyse der Fälle.

► Aktuelle Themen International: Kapitel 4.1

► Tendenzen /Ausblick: Kapitel 5.1

Komplizierte Datenschutzbestimmungen und -einstellungen bei Internetdiensten

Anbieter von Internet-unterstützten Geräten, Sozialen Netzwerken und anderen Internet-Kommunikations-Diensten erleichtern das Leben und bieten den Vorteil, dass sich Ihre Kunden untereinander einfacher Verbinden und Austauschen können. Durch Erhebung von statistischen Daten über die Nutzung können Dienstleistungen verbessert und durch immer gezieltere Werbung (Gratis-)Angebote finanziert werden. Deshalb wollen die Anbieter solcher Applikationen an möglichst viele Informationen ihrer Nutzer herankommen. Wer seine Privatsphäre schützen will, muss sich oft durch seitenlange unübersichtliche Datenschutzeinstellungen kämpfen und versteht oft nicht, mit welchen Konsequenzen er bei welcher Konfiguration rechnen muss.

► Tendenzen/Ausblick: Kapitel 5.3

Infizierte Systeme und Webseiten – Die Möglichkeiten der MELANI

Im Februar wurden E-Mails mit Schadsoftware beobachtet, die gezielt an Personen im öffentlichen Sektor sowie in Bildungsinstituten gesendet wurden. MELANI konnte die Command- & Control Server des Botnetzes identifizieren und den zuständigen Stellen im Ausland weiterleiten. In der Schweiz war der Angriff nicht erfolgreich.

► Aktuelle Themen Schweiz: Kapitel 3.4

Um Missbrauch von Schweizer Internetadressen zu bekämpfen und akute Gefahren für Internetbenutzer abzuwehren, wurde bei der Revision der Verordnung über die Adressierungselemente im Fernmeldebereich eine neue Bestimmung eingeführt, laut welcher unter gewissen Bedingungen „.ch“-Domain-Namen blockiert werden können.

► Aktuelle Themen Schweiz: Kapitel 3.5

Die Melde- und Analysestelle Informationssicherung MELANI betreibt seit April dieses Jahres ein Checktool, welches CH-Webseiten auf allfällige Webseiteninfektionen überprüft. Eine erste Bilanz der Monate Juni – August 2010 zeigt, dass so insgesamt 148 Websites mit Infektionen gefunden werden konnten, was 0.6 Promille der untersuchten CH-Domänen entspricht

► Aktuelle Themen Schweiz: Kapitel 3.3

2 Einleitung

Der elfte Halbjahresbericht (Januar – Juli 2010) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (Wörter in kursiv) sind im **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

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

Kapitel 3 und 4 befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der zweiten Hälfte des Jahres 2009 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

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

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Kommunikation von Sicherheitslücken

Einige *Sicherheitslücken* haben in der Vergangenheit für mediale Aufmerksamkeit gesorgt, so beispielsweise die Lücke im Internet Explorer vom Januar 2010. Aber auch Lücken in Adobe Acrobat und iPhone machten von sich reden. Solche Sicherheitslücken sind vor allem dann gravierend, wenn Gegenmassnahmen nicht einfach zu ergreifen sind. Als Reaktion auf die Sicherheitslücke in mehreren Versionen des Internet Explorer vom Januar 2010 hat das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) deshalb empfohlen, den Microsoft-*Browser* vorerst nicht zu nutzen, sondern bis zum Vorliegen eines *Patches* auf einen alternativen Browser umzusteigen. Der Grund der Warnung war, dass das Ausführen des Internet Explorers im «*geschützten Modus»* sowie das Abschalten von *Active Scripting* mögliche Angriffe erschwerte, sie jedoch nicht vollständig verhindern konnte. Im BSI ist das Aussprechen von öffentlichen Warnungen gesetzlich geregelt und es herrscht die politische Erwartungshaltung, Bürger über Sicherheitslücken zu informieren.

Ob in Deutschland oder in der Schweiz steht eine Bundesstelle unter besonderer Beobachtung, welche Massnahmen sie im Falle einer Sicherheitslücke empfiehlt. Die mediale Aufmerksamkeit nach der BSI-Empfehlung, den Internet Explorer nicht mehr zu benutzen, war folgedessen enorm und beschäftigte auch die Schweizer Medien. Die Schwierigkeit einer Empfehlung besteht jeweils darin, eine sichere, aber auch eine machbare Variante als Alternative vorzuschlagen. Es ist selbstverständlich, dass Firmen nicht sofort auf eine andere Browserapplikation wechseln können. Ein solcher Wechsel muss von langer Hand geplant werden. Andernfalls sind überlastete Hotlines sowie verunsicherte und eventuell genervten Mitarbeitende garantiert. Bei der LNK-Lücke vom Juli 2010, welche einen Fehler in der Windows Shell bei der Auswertung von Parametern von LNK- und PIF-Dateien ausnutzte, stellte sich beispielsweise für viele Firmen die Frage, ob der angegebene *Workaround*, die *Verknüpfungssymbole* zu entfernen[1], ein praktikabler Weg ist. Durch diese Notlösung konnte zwar mögliche Schadsoftware keinen Schaden mehr anrichten, es musste aber in Betracht gezogen werden, dass das Verschwinden der gewohnten Symbole zu einer grossen Verunsicherung der Mitarbeitenden führen wird. Es muss immer abgewogen werden, wie gross das Schadenspotential und die Ausbreitung der spezifischen Schadsoftware sind und wie diese im Verhältnis zum Aufwand für empfohlene Massnahmen stehen. Jede Firma ist letztlich für diese Entscheidung selbst verantwortlich. MELANI versucht in solchen Fällen die Betreiber von kritischen Infrastrukturen mit Hintergrundinformationen zu versorgen, welche solche Entscheidungen erleichtern. Jedoch ist, bei der Durchsetzung eines Workarounds, zusammen mit einer Verstärkung des Supports, eine gute Kommunikation immer enorm wichtig.

Mit öffentlichen Warnungen über Sicherheitslücken hält sich MELANI prinzipiell zurück. Aufgrund der zahlreichen Sicherheitslücken in den verschiedensten Programmen, wäre eine Abstumpfung der Sensibilität der Benutzer zur Folge. Auch zeigt die Erfahrung, dass angegebene Empfehlungen nur von einer geringen Zahl Benutzer umgesetzt werden, da diese entweder zu kompliziert oder aber mit grossen Einschränkungen verbunden sind. Jeder Internetbenutzer muss sich deshalb bewusst sein, dass alle Programme kritische Schwachstellen besitzen – auch solche, die noch nicht öffentlich bekannt sind, aber bereits ausgenutzt werden. Letztere werden meist für Spionagezwecke verwendet und können bei

[1] In der Folge wären die Verknüpfungen zwar noch vorhanden gewesen, hätten aber alle gleich ausgesehen und wären nicht mehr durch unterschiedliche Symbole auseinanderzuhalten gewesen.

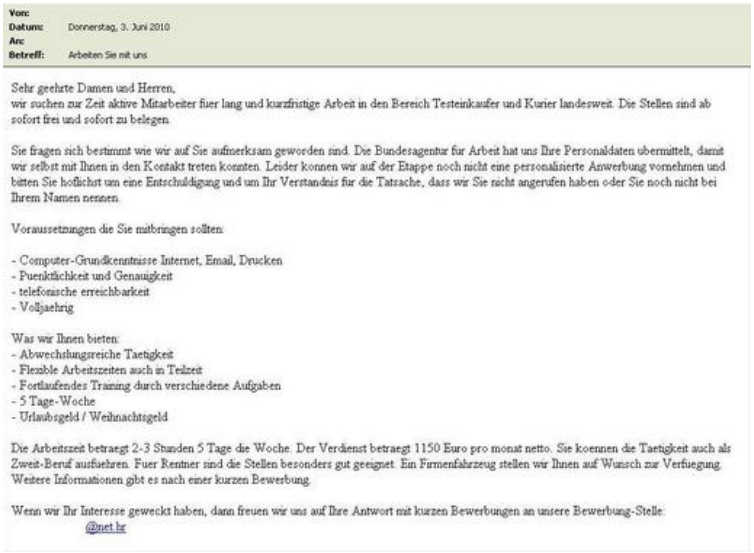
Firmen und Regierungen grossen Schaden anrichten. Ein gut ausgebauter ständiger Grundschutz ist deshalb zwingend.

Zudem gibt es Programme, welche aus dem produktiven Arbeitsalltag nicht wegzudenken sind und auf welche nicht oder nur schwerlich verzichtet werden kann. Ist ein solches Programm von einer Sicherheitslücke betroffen, kann man den Sicherheitsrisiken höchstens mit flankierenden Massnahmen entgegenwirken, indem man beispielsweise Mitarbeiter schult oder bekannte Schadsoftware-Server oder -E-Mails sperrt. Hierbei ist ein Informationsaustausch zwischen den Firmen aber auch den Providern wichtig. Zwischen Betreibern von *kritischen Infrastrukturen* ist ein solcher Informationsaustausch auf der Basis der Melde- und Analysestelle Informationssicherung MELANI möglich. Ähnliche Informationsportale für KMUs sind erst vereinzelt im Teststadium.

3.2 Finanzagenten zwecks Geldwäscherei gesucht

Es gibt weiterhin Menschen, welche sich verleiten lassen, sich von Kriminellen als sogenannte «Finanzagenten» einspannen zu lassen, vor allem dann, wenn der Aufwand gering ist und keine besonderen Qualifikationen verlangt werden: Finanzagenten sollen jeden Tag ein bisschen Zeit übrig haben, sich Geld auf ihr Konto überweisen zu lassen, um es von dort aus an Dritte weiterzuleiten. Ein gewisser Prozentsatz des überwiesenen Betrags darf als Provision behalten werden. Finanzagenten, also Geldkuriere, die sich für das Reinwaschen von Geldern aus Online-Betrügereien benutzen lassen, sind für Kriminelle begehrt. Finanzagenten sind rar und können nur für eine Transaktion verwendet werden, da sie danach in der Regel auffliegen und den zuständigen Behörden gemeldet werden.

Seit Juni 2010 tauchen in der Schweiz wieder vermehrt E-Mails auf, die für solche Geldkurier-Stellen werben und attraktive Konditionen versprechen. Wer auf ein solches Angebot reagiert, erhält in der Regel innerhalb kurzer Zeit einen Geldbetrag auf sein Konto überwiesen, der dann, meist über die Geldtransfer-Firma «Western-Union», ins Ausland überwiesen werden soll. Wer an solchen «Geschäften» und Transaktionen mitwirkt, riskiert ein Strafverfahren wegen Gehilfenschaft zu Geldwäscherei (Art. 305bis StGB).



Von:
Datum: Donnerstag, 3. Juni 2010
An:
Betreff: Arbeiten Sie mit uns

Sehr geehrte Damen und Herren,
wir suchen zur Zeit aktive Mitarbeiter fuer lang und kurzfristige Arbeit in den Bereich Testeinkaufer und Kurier landesweit. Die Stellen sind ab sofort frei und sofort zu belegen.

Sie fragen sich bestimmt wie wir auf Sie aufmerksam geworden sind. Die Bundesagentur fur Arbeit hat uns Ihre Personaldaten ubermittelt, damit wir selbst mit Ihnen in den Kontakt treten konnten. Leider konnen wir auf der Etappe noch nicht eine personalisierte Anwerbung vornehmen und bitten Sie hoflichst um eine Entschuldigung und um Ihr Verstandnis fur die Tatsache, dass wir Sie nicht angerufen haben oder Sie noch nicht bei Ihrem Namen nennen.

Voraussetzungen die Sie mitbringen sollten:

- Computer-Grundkenntnisse Internet, Email, Drucken
- Puenktlichkeit und Genauigkeit
- telefonische erreichbarkeit
- Volljaehrig

Was wir Ihnen bieten:
- Abwechslungsreiche Taetigkeit
- Flexible Arbeitszeiten auch in Teilzeit
- Fortlaufendes Training durch verschiedene Aufgaben
- 5 Tage-Woche
- Urlaubsgeld / Weihnachtsgeld

Die Arbeitszeit betraegt 2-3 Stunden 5 Tage die Woche. Der Verdienst betraegt 1150 Euro pro monat netto. Sie koennen die Taetigkeit auch als Zweit-Beruf ausfuehren. Fuer Rentner sind die Stellen besonders gut geeignet. Ein Firmenfahrzeug stellen wir Ihnen auf Wunsch zur Verfuegung. Weitere Informationen gibt es nach einer kurzen Bewerbung.

Wenn wir Ihr Interesse geweckt haben, dann freuen wir uns auf Ihre Antwort mit kurzen Bewerbungen an unsere Bewerbung-Stelle:
@net.hr

Beispiel eines Finanzagenten E-Mails

Solche Angebote werden nicht nur mittels E-Mail verteilt, 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, welche Aussicht auf grosse Gewinne machen, mit Vorsicht zu geniessen. Auch im Internet gilt grundsätzlich die Regel, dass ohne entsprechende Arbeit auch legalerweise kein grosses Geld zu verdienen ist. Eigene Bankkonten sollten nie Dritten zur Verfügung gestellt werden.

Dass aber nicht nur Privatpersonen auf solche Jobangebote hereinfallen, zeigt ein Fall bei dem ein Mitarbeiter einer Sozialverwaltung einem Arbeitslosen einen solchen Finanzagentenjob weitervermittelt hat. Gerade im Bereich Sozialhilfe/Arbeitsvermittlung ist eine besondere Sensibilität auf diese Thematik nötig, da andernfalls Personen, die schon in einer schwierigen Situation stecken, mit noch mehr Unannehmlichkeiten rechnen müssen.

3.3 MELANI überprüft CH-Webseiten auf Infektionen

Die Melde- und Analysestelle Informationssicherung MELANI betreibt seit April dieses Jahres ein Checktool, welches Schweizer Webseiten auf allfällige *Webseiteninfektionen* überprüft. Hierbei wird zum einen der *Quellcode* der Webseite auf bekannte Signaturen überprüft, zum anderen wird die Seite regelmässig und automatisiert angesurft und anschliessend analysiert, welche Aktionen auf dem Computer ausgelöst werden. Eine Liste definiert erlaubte und verbotene Aktionen und schlägt je nachdem Alarm.

Eine erste Bilanz der Monate Juni – August 2010 zeigt, dass so insgesamt 148 Domänen mit Infektionen gefunden werden konnten, was 0.6 Promille der untersuchten CH-Domänen entspricht:

Gefundene CH-Domänen mit Webseiteninfektionen	148
- gesäubert	116
- weiterhin oder wieder infiziert	32
Total untersuchte CH-Domänen	237’421

Nach dem Erkennen einer Webseiteninfektion wird jeweils direkt durch die Melde- und Analysestelle Informationssicherung MELANI der Webseitenbesitzer oder der Provider informiert, damit dieser die notwendigen Schritte zur Säuberung einleiten kann. Seit Juli 2010 hat MELANI auch die Möglichkeit, die Sperrung einer CH-Domäne bei SWITCH zu veranlassen (siehe Kapitel 3.4). Von dieser Möglichkeit wurde bis jetzt noch nicht Gebrauch gemacht und MELANI wird sich ihrer auch in Zukunft nur bedienen, wenn alle anderen, weniger einschneidenden Massnahmen erfolglos bleiben. Da die betroffenen Webseiten praktisch allesamt gehackt sind und der Besitzer meistens keine Ahnung von dem zusätzlichen schadhaften Code auf seiner Seite hat, lässt sich eine solche Infektion auch auf dem bilateralen Weg beheben.

Es gibt verschiedene Möglichkeiten, manipulierte Webseiten auf einen Webserver zu laden. Bei der Variante, welche am häufigsten verwendet wird, wird mit gestohlenen FTP-Zugangsdaten, auf den Webserver zugegriffen. Hierbei besitzt der Angreifer beispielsweise eine Liste mit FTP-Logindaten. Anschliessend wird automatisch mit diesen Daten in das Konto eingeloggt, eine Webseite (meist die *Index-Seite* oder eine vorhandene Javascript-Datei .js) heruntergeladen, der schadhafte Code eingeschleust und die Seite anschliessend

wieder hinaufgeladen. Andere Möglichkeiten sind das Ausnützen von Schwachstellen im *Content Management System (CMS)* oder auf der Webseite installierte Webapplikationen und das *Cross-Site Scripting* in Gästebüchern oder Foren. Das Ausnutzen von Schwachstellen in sogenannten Ad-Servern, also von Servern, die für das Einblenden von Werbebanner zuständig sind, ist eine weitere Möglichkeit und nimmt momentan zu.

Vorgehen für Webadministratoren nach dem Erkennen einer Webseiteninfektion

Allgemein: Durch das alleinige Ansurfen dieser Seite wird versucht, den Computer des Besuchers zu infizieren. Wir empfehlen deshalb, direkt den Quelltext auf dem Server zu untersuchen und die Seite bis zur Behebung der Infektion nicht oder nur mit den entsprechenden Sicherheitsmassnahmen zu besuchen. (Abgeschaltetes Javascript und ActiveScripting, abgeschaltete IFrame-Funktion, usw.)

- Falls *kein CMS vorhanden ist und die Daten via FTP auf den Server geladen werden,* ist der einfachste Lösungsweg, die lokal gespeicherte Webseite einfach wieder auf den Server zu laden. Einen Hinweis, welche Seiten kompromittiert wurden, kann übrigens das Datum geben, wann die Seite das letzte Mal verändert wurde. Dieses Änderungsdatum ist in den FTP-Programmen jeweils ersichtlich. Wenn in der letzten Zeit keine Änderungen gemacht wurden, das Änderungsdatum aber auf eine kürzliche Änderung schliessen lässt, ist dies ein Hinweis auf eine Kompromittierung der entsprechenden Seite.
  Es ist wichtig, anschliessend das Passwort zu ändern und zu überprüfen ob der Computer, mit dem die Webseite administriert wird, einen Trojaner enthält.
- *Geschieht die Webseitenadministration über ein CMS,* muss herausgefunden werden, wo der Schadcode eingeschleust wurde. Meist geschieht dies in wiederkehrenden Elementen wie Kopf- oder Fusszeilen. Der Schadcode kann aber durchaus auch fest im CMS programmiert sein. Falls die Stelle mit dem Schadcode nicht gefunden und entfernt werden kann, empfiehlt es sich, den Hosting Provider um Unterstützung zu bitten
  Wichtig: Das CMS unbedingt regelmässig auf den neuesten Stand bringen und auch hier die Zugangsdaten ändern.
- Neuerdings sind auch öfters *Werbeeinblendungen* von Webseiteninfektionen betroffen. Diese haben dann eine besonders grosse Reichweite, da sie auf verschiedenen Webseiten eingeblendet werden. Hierbei ist in letzter Zeit besonders das Ad-Programm OpenX von Angriffen betroffen.
  Ad-Server müssen unbedingt immer auf dem neuesten Stand gehalten werden.

3.4 MELANI entdeckt Botnetz und initiiert Takedown

In der dritten Februarwoche erhielt MELANI Informationen im Zusammenhang mit einem gezielten Hackerangriff, der durch den Versand infizierter E-Mails erfolgte. Diese wurden an Vertreter des öffentlichen Sektors und Ausbildungsinstituten versandt.

Die auf Englisch verfassten E-Mails enthielten ein Dokument zu einer NATO-Konferenz, die unter der Bezeichnung “C4I cooperation in South-Eastern Europe (SEE) – the new look” am 24./25. Februar 2010 stattfinden sollte. Beim Öffnen der Datei wurde der Computer infiziert und zu einem *Botnetzwerk* hinzugefügt. Der Code hatte insbesondere die Funktion, Login-Daten für E-Mails und soziale Netzwerke abzufangen.

Durch die Analyse des schadhaften Dokumentes konnte MELANI den Kommando-Server (*Command- & Control Server*) sowie eine umfassende Liste infizierter Systeme bestimmen.

Diese Daten wurden anschliessend den verantwortlichen Stellen zugestellt, um das Botnetzwerk zu deaktivieren. In der Schweiz wurden keine Opfer festgestellt.

Im beschriebenen Fall[2] wurden die E-Mails gezielt an Personen im öffentlichen Sektor und bestimmten Ausbildungsinstituten gesandt. Somit stellt sich die Frage, warum sich der Angriff gerade gegen diese Personen wandte. Möglich sind zwei Erklärungen: Die erste geht davon aus, dass es sich wirklich um einen gezielten (Spionage-)Angriff gehandelt hat und genau diese Personen auch im Visier waren. Hierbei wird im Vorfeld mittels *Social Engineering* versucht, Adressen und andere Informationen der Personen, die man ausspionieren will, zu sammeln. Eine zweite Erklärung beruht darauf, dass es sich nicht um einen gezielten Angriff gehandelt hat, sondern dass Kriminelle unter dem Radar der Antiviren-Hersteller bleiben und nur eine geringe Anzahl Personen infizieren wollten. Die E-Mail-Adressen werden hierbei von anderen Kriminellen gekauft. Die Angreifer haben mittlerweile begriffen, dass breit angelegte Angriffe oft weniger nützen, da sie für einen grossen Wirbel sorgen und infolgedessen bei den Antiviren-Herstellern, Forschern, Sicherheitsexperten usw. zu einer grösseren Reaktion führen. Angriffe im Stillen sind effizienter, auch wenn sie weniger Personen erreichen.

3.5 Blockierung von «.ch»-Domain-Namen bei Missbrauchsverdacht

Um Missbrauch von Schweizer Internetadressen zu bekämpfen und akute Gefahren für Internetbenutzer abzuwehren, wurde bei der Revision der Verordnung über die Adressierungselemente im Fernmeldebereich (AEFV, SR 784.104) eine neue Bestimmung eingeführt. Laut dieser muss die Registerbetreiberin von «.ch»-Domains (SWITCH) unter gewissen Bedingungen solche Domain-Namen blockieren und die entsprechende Zuweisung zu einem *Namenserver* aufheben.

Gemäss dem am 1. Januar 2010 neu in Kraft gesetzten Artikel 14*f*^{bis} AEFV[3] kann ein «.ch»-Domain-Name blockiert und die entsprechende Zuweisung zu einem Namenserver aufgehoben werden. Dies ist der Fall, wenn der begründete Verdacht besteht, dass dieser Domain-Name benutzt wird, um entweder mit unrechtmässigen Methoden an schützenswerte Daten zu gelangen (so genanntes *Phishing*) oder über diese Domain schädliche Software (so genannte Malware) verbreitet wird. Zudem muss eine in der Bekämpfung der Cyberkriminalität vom Bundesamt für Kommunikation (BAKOM) anerkannte Stelle dies beantragen. SWITCH kann für die Dauer von höchstens fünf Werktagen auch selbständig entsprechende Massnahmen ergreifen, muss diese aber wieder aufheben, wenn sie nicht von einer antragsberechtigten Stelle bestätigt wurden.

Bei der Blockierung eines Domain-Namens unterscheidet man folgende Vorgehensweisen: Entweder wird verhindert, dass der Eintrag in der administrativen Infrastruktur der Domain-Zuteilung geändert werden kann («einfrieren» des Domain-Record – die Website bleibt aber erreichbar) oder die Zuweisung zu einem Namenserver wird aufgehoben mit der Folge, dass nach der Aktualisierung im *Domain Name System* (DNS) die Website nicht mehr durch das

[2] Im Laufe des ersten Semesters 2010 stellten andere Betriebe weitere ähnliche Fälle fest. Dazu gehörte beispielsweise die E-Mail, die unter der Bezeichnung „Military operation of the EU NAVFOR Somalia“ im Namen der Europäischen Union versandt wurde (http://contagiodump.blogspot.com/2010/08/cve-2010-1240-with-zeus-trojan.html), oder diejenige, die als „2020 Project“ im Namen des „National Intelligence Council“ die Runde machte (http://krebsonsecurity.com/2010/02/zeus-attack-spoofs-nsa-targets-gov-and-mil/).

[3] http://www.admin.ch/ch/d/sr/784_104/a14bist.html (Stand: 27. August 2010)

Eingeben des Domain-Namens aufgerufen werden kann. Mit letzterer Massnahme wird lediglich verhindert, dass Internetnutzer durch Aufrufen dieser Schweizer Adresse geschädigt werden. Die Inhalte auf den Webservern werden nicht gelöscht und die Täterschaft kann jederzeit einen anderen Domain-Namen verwenden, um auf diese Inhalte zu verweisen. Es handelt sich insofern um eine kleine Massnahme, die der Verbesserung der Möglichkeiten zur Gefahrenabwehr im Schweizer Adressraum des Internet und zum Schutzes der Internetnutzer beim surfen auf „.ch"-Webseiten dient.

Seit dem 15. Juni 2010 ist die Melde- und Analysestelle Informationssicherung (MELANI) vom Bundesamt für Kommunikation (BAKOM) als kompetente Stelle in diesem Bereich anerkannt. MELANI kann nun bei SWITCH die Blockierung und Aufhebung der betreffenden Zuweisung zu einem Namenserver von «.ch»-Domain-Namen bei begründetem Verdacht auf Phishing oder Verbreitung von Malware beantragen.

MELANI wird sich dieser Möglichkeit nur sehr zurückhaltend bedienen und als letztes Mittel einsetzen, wenn die Gefahr nicht anderweitig gebannt werden kann. Wie bereits im letzten Halbjahresbericht erwähnt, wird Malware aktuell oft über gehackte Webseiten verbreitet. In solchen Fällen kann durch Kontaktaufnahme mit den legitimen Betreibern der Seite oder dem Hosting-Provider das Problem meistens behoben werden. Mit dieser informellen Vorgehensweise hat MELANI schon vor der Revision der AEFV viele Erfolge erzielt.

Auf Grund einer Änderung des Domain-Namen-Registrierungsvertrages von SWITCH, gemäss welcher ein Domain-Name erst nach erfolgter Zahlung der Gebühren genutzt werden kann, sind seit dem 1. März 2009 missbräuchliche Registrierungen von «.ch»-Domain-Namen vor allem im Bereich Phishing beinahe verschwunden und im Bereich Malware stark reduziert.

3.6 Der Bundesrat legt Botschaft zur Ratifizierung der Cybercrime Convention vor[4]

Das Übereinkommen des Europarates vom 23. November 2001 über die Cyberkriminalität[5] ist die erste und bisher einzige internationale Konvention, die sich mit Computer- und Netzwerkkriminalität befasst. Die Vertragsstaaten werden verpflichtet, ihre Gesetzgebung den Herausforderungen neuer Informationstechnologien anzupassen und es wird eine Harmonisierung des Computerstrafrechts angestrebt. Weiter werden Regelungen für das Strafverfahren getroffen (insbesondere Beweiserhebung und Beweissicherung elektronischer Daten) und das Zusammenwirken zwischen den verschiedenen Vertragsparteien soll in seinem Ablauf schnell und effizient gestaltet werden. Die Schweiz erfüllt die Anforderungen des Übereinkommens bereits weitgehend.[6]

Anpassungsbedarf ergibt sich bezüglich des Straftatbestandes des unbefugten Eindringens in ein Datenverarbeitungssystem (Art. 143bis StGB, sog. «Hacking»-Tatbestand). Hier wird

---

[4] Dossier beim Bundesamt für Justiz: http://www.bj.admin.ch/bj/de/home/themen/kriminalitaet/gesetzgebung/cybercrime__europarat.html (Stand: 27. August 2010)

[5] Convention on Cybercrime, ETS 185: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/ConventionOtherLg_en.asp (Stand: 27. August 2010)

[6] http://www.bj.admin.ch/bj/de/home/dokumentation/medieninformationen/2010/ref_2010-06-181.html (Stand: 27. August 2010)

eine Vorverlagerung der Strafbarkeit ähnlich der Strafnorm gegen *Computerviren* (Art. 144bis Ziff. 2 StGB[7]) vorgesehen: Strafbar macht sich bereits, wer Programme, Passwörter oder andere Daten zugänglich macht und weiss oder annehmen muss, dass diese in der Folge für das illegale Eindringen in ein Computersystem verwendet werden.[8]

Laut Botschaft des Bundesrates[9] soll der Vertrieb von *«Dual Use»*-Vorrichtungen und -Daten unter gewissen Voraussetzungen und getroffenen Vorkehrungen jedoch nach wie vor zulässig sein. Sicherheitstests an Computersystemen, sogenannte «Vulnerability Assessments», durchgeführt durch den Betreiber oder einen beauftragten Dritten, sowie die Entwicklung neuer Software zu diesen Zwecken gelten als durch den Befugten durchgeführte oder veranlasste Handlungen und bleiben straffrei. Massnahmen zur Qualitätssicherung bezüglich eigener Systeme und im Auftrag von Dritten werden ebenfalls nicht als strafbar erklärt und die Ausbildung von IKT-Sicherheitsfachpersonen, wo der Einsatz von «Hacking-Tools» thematisiert und durchgeführt wird, bleibt legal.

Als strafbar erklärt wird hingegen das (bezüglich der Tathandlung sowie der weiteren Verwendung der Daten) vorsätzliche Verbreiten von Programmen und anderen Daten sowie das unverantwortliche Verbreiten von Datensätzen, deren sensitiver Inhalt, der Adressatenkreis oder andere Umstände den deliktischen Einsatz der Tools als naheliegend erscheinen lässt. Ein verantwortungsloses Streuen von Hacking-Werkzeugen in einem deliktsbereiten Umfeld[10] soll nicht straffrei bleiben. Insofern wird „*Reasonable Disclosure*“ bei Sicherheitslücken weiterhin möglich sein – öffentliche „*Full Disclosure*“ ist demgegenüber zukünftig verboten.

Der Ratifizierungsentwurf des Bundesrates wurde an das Parlament überwiesen und muss nun von beiden Räten genehmigt werden. Zudem unterliegt die Ratifizierung dem fakultativen Staatsvertragsreferendum.

3.7 Missbrauchsgefahr bei verpasster Erneuerung der Domänen Registrierung

Am 10. Juni 2010 waren Webseiten des Kabelnetzbetreibers Cablecom für kurze Zeit nur eingeschränkt erreichbar. Der Grund dafür war die verpasste Erneuerung der Domäne cablecom.net, welche als Nameserver für Cablecom-Dienste verwendet wird. Nach der Entdeckung des Versäumnisses wurde die Domäne sofort für 10 weitere Jahre registriert.

Was in diesem Fall keine grossen Auswirkungen hatte und höchstens zu einem kleinen Schmunzeln führt, ist ein Problem, welches nicht zu unterschätzen ist und sich durch alle Firmengruppen zieht, aber auch Privatpersonen betrifft, welche eine Webseite unterhalten. Es gibt einen regelrechten Markt für abgelaufene Domainnamen, unabhängig davon, ob die Erneuerung der Registrierung verpasst wurde oder die Domäne auch tatsächlich nicht mehr verwendet wird. Besonders gravierend sind beispielsweise Schulwebseiten, welche nach dem Freiwerden für das *Hosten* von anzüglichen Seiten verwendet werden.

In einem anderen Schweizer Fall wurde nach dem Freiwerden der Domäne die Original-Website kopiert und unter der gleichen Domäne wieder ins Netz gestellt. Allerdings wurde

---

7 http://www.admin.ch/ch/d/sr/311_0/a144bis.html (Stand: 27. August 2010)

8 Formulierung gemäss Entwurf: http://www.admin.ch/ch/d/ff/2010/4747.pdf (BBl 2010 4749) (Stand: 27. August 2010)

9 http://www.admin.ch/ch/d/ff/2010/4697.pdf (Stand: 27. August 2010)

10 Der öffentliche Bereich des Internet muss hier sicherlich mit eingeschlossen werden.

die neue alte Webseite mit verschiedenen Zusätzen wie beispielsweise Klickwerbung ausgestattet – auch Schadsoftware wurde darauf beobachtet. Der Vorteil dieses Domain-Missbrauchs (Squatter) liegt auf der Hand: Da die Domäne schon bekannt ist, wird sie allenfalls von einer grossen Zahl Besucher aufgerufen und viele Links gehen schon (respektive noch) auf die besagte Website. Der Schaden für die Firma ist Reputationsverlust, Aufwendung von Zeit und Geld, um die Domäne zurückzubekommen sowie den Verlust von potentiellen Kunden.

Vergessen wird dabei häufig, dass auch sämtliche E-Mails, die an die ehemalige Domäne gesendet werden, von dem neuen Domänen-Besitzer einfach gelesen werden können. Dabei muss er nicht einmal die genaue E-Mail Adresse kennen. Mit der Funktion «Catch-All» werden sämtliche E-Mails, welche an eine Domäne gesendet werden, abgefangen und an eine zentrale Adresse weitergeleitet.

Für alle Domänenbesitzer gilt darauf bedacht zu sein, die einzelnen Domänen rechtzeitig zu erneuern und auch zu bezahlen.[11] Auch wenn eine Domäne absichtlich aufgegeben wird, muss man sich bewusst sein, dass irgendeine Person mit irgendeinem Geschäftsmodell – sei es noch so dubios – unter dieser Adresse anschliessend Geschäfte machen kann.

3.8 Hacking und seine physischen Auswirkungen - Beispiel Auto

3.8.1 Störsender in Arbon

Wer sein Auto im letzten Jahr im südlichen Altstadtbereich von Aarbon geparkt hatte, sah sich öfters mit dem Problem konfrontiert, sein elektronisch verschliessbares Auto nicht mehr öffnen zu können. Im Februar dieses Jahres konnten dann Spezialisten des Bundesamtes für Kommunikation (BAKOM) das Problem eruieren. Ein älterer Funklautsprecher hatte auf der Frequenz gesendet, welche auch für Autoschlüssel verwendet wird. Funkautoschlüssel funktionieren im Frequenzbereich zwischen 433.0-434.79 MHz, welches auch *Industrial, Scientific and Medical Band (ISM Band)*[12][13] genannt wird. In diesem Frequenzbereich sind jedoch auch noch andere drahtlose Anwendungen zugelassen, wie etwa Funk-Wetterstationen, drahtlose Lautsprecher- oder Kopfhöreranlagen. Ebenfalls in diesem Bereich dürfen auch die Funkamateure senden – mit bedeutend mehr Leistung, als es die Funkautoschlüssel tun. All diese Funkanwendungen können dazu führen, dass der Empfänger im Auto, der auf das Signal des Schlüssels wartet, gestört wird und nicht mehr funktioniert.

---

[11] Verschiedene Registrierungsdienste behalten sich ausdrücklich vor, bei Nicht-Bezahlung von Gebühren einfach die Domäne wieder freizugeben. Sie sparen sich so ein aufwändiges und kostenintensives Mahnwesen.

[12] http://www.bakom.admin.ch/themen/frequenzen/00652/00653/index.html?lang=de (Stand: 27. August 2010)

[13] http://de.wikipedia.org/wiki/ISM-Band: Als ISM-Bänder (Industrial, Scientific and Medical Band) werden Frequenzbereiche bezeichnet, die durch Hochfrequenz-Geräte in Industrie, Wissenschaft, Medizin, in häuslichen und ähnlichen Bereichen genutzt werden können. Entsprechende ISM-Geräte wie Mikrowellenherde und medizinische Geräte zur Kurzwellenbestrahlung benötigen dabei nur eine allgemeine Zulassung. Einige ISM-Bänder werden auch z. B. für Audio- und Videoübertragungen oder Datenübertragungen wie WLAN oder Bluetooth verwendet, ohne dass es für diese Nutzung einer Einzel-Frequenzzuweisung bedarf. Diese sind allerdings keine ISM-Anwendungen und unterliegen eigenen Bestimmungen. Durch die gemeinsame Nutzung kann es in den besonders häufig genutzten Bändern, wie etwa dem 433-MHz- und 2,4-GHz-Band, leicht zu Störungen zwischen verschiedenen Geräten kommen. (Stand: 27. August 2010)

In diesem Fall war die Interferenz ungewollt. Kriminelle machen sich aber genau diese Möglichkeit der Störung zu Nutze, um in Autos einzubrechen. Wird genau in dem Moment, in dem man das Auto abschliessen will, ein Störsignal gesendet und der Autobesitzer kontrolliert nicht, ob das Fahrzeug auch wirklich geschlossen ist, stehen die Autotüren für die Kriminellen offen und sie können sich in Ruhe im Innern des Wagens nach Wertgegenständen umsehen.

3.8.2 100 Autos per Funk abgeschaltet

Über eine per Mobilfunk gesteuerte Wegfahrsperre lässt sich bei Diebstahl das Auto blockieren. Dieses System kann ebenfalls bei mobilen Computern eingesetzt werden, so dass sich Laptops nach einem Diebstahl aus der Ferne sperren oder sogar Daten löschen und die Festplatte formatieren lassen. Über die Funktion MobileMe kann schon heute das iPhone oder iPad von einem beliebigen Computer aus der Ferne gelöscht werden.[14]

Das solche Systeme auch vor Manipulationen nicht gefeit sind, liegt auf der Hand. In den USA ist genau dies im letzten Halbjahr geschehen. Hier hat ein ehemaliger Mitarbeiter eines Autohauses mehr als 100 Fahrzeuge von Kunden über das Internet lahm gelegt. Über das in diesem Fall eingesetzte System «Webtech-Plus», können Autohändler die Kunden, welche die Finanzierungs- oder Leasingraten nicht pünktlich begleichen, am Starten des Fahrzeugs hindern.

Solche Dienstleistungen, wie das zentrale Verwalten von Wegfahrsperren oder Zugangsperren von Mobilcomputern oder Mobiltelefonen werden in Zukunft vermehrt angeboten. Obschon diese Services eigentlich eine gute Sache sind und einen Sicherheitsgewinn bedeuten, bergen sie auch gewisse Gefahren, da solche Tools zentral gesteuert werden. Manipulationen, die grosse Auswirkungen haben, sind so möglich. Dies muss, wie obiges Beispiel zeigt, nicht unbedingt ein Hacken des Systems sein, es kann auch durchaus ein Mitarbeiter respektive Ex-Mitarbeiter sein, der das System bewusst oder durch ein Fehlverhalten manipuliert.

3.8.3 Manipulation moderner Autos

In modernen Autos ist immer mehr Elektronik integriert. Fast die ganze Steuerung wird vom Bordsystem überwacht. Es erstaunt deshalb nicht, dass auch ein Auto anfällig gegen Hacker-Angriffe werden kann. Momentan ist dies noch Utopie. Trotzdem zeigten im letzten Halbjahr Forscher von US Universitäten, wie man in das Bordsystem eines fahrenden Autos eindringt und die Kontrolle dieses Autos übernimmt. Dabei wurde dem Fahrer beispielsweise die Kontrolle der Bremsen entzogen, respektive der Motor an- und abgeschaltet. Das Einzige, was nicht übernommen werden konnte, war die Steuerung, da diese in diesem Fall noch mechanisch funktionierte.

Da heutige Autos in der Regel noch keine Funkanbindung des Bordsystems haben, war bei diesem Versuch noch eine Kabelverbindung mit dem Auto notwendig, das heisst, dass der Manipulierende entweder im Auto selber sitzen oder eine solche Funkverbindung zuerst manuell installiert werden muss. Falls in Zukunft aber Bordsysteme mit dem Internet verbunden werden, sind hier Manipulationen Tür und Tor geöffnet.

[14] http://www.apple.com/mobileme/features/find-my-iphone.html (Stand: 27. August 2010)

3.9 Die Schweiz hat nun digitale Identitäten (SuisseID)

Mit dem «Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur» (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03)[15] wurde in der Schweiz die Rechtsgrundlage geschaffen, um Zertifizierungsdienste im Bereich der *elektronischen Signatur* anzubieten und staatlich anzuerkennen. Weil ZertES-konforme *Zertifikate* ausschliesslich für qualifizierte elektronische Signaturen eingesetzt werden können, werden diese Zertifikate im Rahmen einer SuisseID zusammen mit einem Zertifikat ausgegeben, das auch zur Authentifizierung und damit als standardisierter elektronischer Identitätsnachweis eingesetzt werden kann. Damit wird es möglich, bei einer Reihe von Anbietern Online-Dienstleistungen in Anspruch zu nehmen, und gegenüber dem Anbieter zweifelsfrei nachzuweisen, dass man die Person ist, für die man sich ausgibt.
Neben einigen privaten Anbietern akzeptieren momentan folgende Bundesämter den Einsatz von SuisseIDs: Das Bundesamt für Justiz (Strafregister-Portal), die Eidg. Alkoholverwaltung (Einholen von Brennbewilligungen und Anmelden von Produktions- und Verkaufsmengen für die Veranlagung), die Eidg. Steuerverwaltung (verschiedene Dienste der Mehrwertsteuer) und die Eidg. Zollverwaltung (Rückerstattungen und Betriebsprüfungen).
Der Bund subventioniert bis Ende 2010 (resp. so lange Vorrat) den privaten Kauf einer SuisseID (Smartcard oder USB-Stick) mit Fr. 65.00 und will damit die Verbreitung der SuisseIDs fördern.

Studien zu allfälligen Sicherheitsrisiken bezüglich SuisseID liegen bis zum heutigen Zeitpunkt nicht vor. Die verwendete Technologie entspricht jedoch allgemein anerkannten zeitgemässen Standards. Es können sich aber Risiken aus dem Umstand ergeben, dass die SuisseID die Authentisierung und die qualifizierte elektronische Signatur auf einem Chip vereint. Beispielsweise dann, wenn der Inhaber der SuisseID aus Gründen der Bequemlichkeit sowohl für die Authentisierung als auch für das Erstellen einer rechtsgültigen Unterschrift den gleichen *PIN-Code* verwendet. Das Nutzerverhalten muss wie bei jeder Sicherheitstechnologie in eine Gesamtbetrachtung einbezogen werden.
Trotz fortgeschrittener Gesetzgebungen haben es qualifizierte elektronische Signaturen bis heute weder auf nationaler Ebene noch auf internationaler Ebene geschafft, sich in der Praxis durchzusetzen bzw. zu etablieren. Ob mit der SuisseID diesbezüglich die richtigen Impulse gesetzt werden können, bleibt abzuwarten.

3.10 Identifikation von mobilen Internetnutzern soll besser werden

Durch den rasanten Anstieg von Smart-Phones und mobilem Internetzugang ist die Zahl der Internetanschlüsse stark angestiegen. Damit nicht für jedes Gerät eine eigene *IP-Adresse* benötigt wird, setzen die Mobilfunkanbieter Network-Address-Port-Translation (NAPT) ein. So verwenden mehrere tausend Kunden die gleiche IP-Adresse, aber unterschiedliche *Ports*. Für die Identifizierung eines Anschlusses und dessen Nutzer werden typischerweise IP-Adresse, Datum und Uhrzeit benötigt. Diese Daten werden auch regelmässig in Log-Dateien von Webdiensten gespeichert. Um einen mobilen Nutzer zu identifizieren, müsste nun auch die verwendete Port-Nummer bekannt sein. Diese Angabe wird aber nur selten aufgezeichnet. Unter diesem Gesichtspunkt ist auch die vom Parlament geforderte Registrierungspflicht für *Wireless*-Prepaid-Karten zu betrachten.[16] Die ausserdem angestrebte Pflicht, eine Teilnehmeridentifikation auch innerhalb von privaten Netzwerken

[15] http://www.admin.ch/ch/d/sr/c943_03.html (Stand: 27. August 2010)

[16] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20073627 (Stand: 27. August 2010)

(also hinter einer einzigen IP-Adresse) zu gewährleisten, ist wohl zu begrüssen – es darf aber nicht ausser Acht gelassen werden, dass unter Umständen mehr Daten zur Identifikation nötig sind, als normalerweise zur Verfügung stehen. Diesem Umstand muss bei der aktuellen Revision[17] des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)[18] sowie bei der Ausgestaltung der betreffenden Ausführungsbestimmungen Rechnung getragen werden.

3.11 Hacker treiben Unfug mit der SVP und der Europäischen Union

Ende 2009/ Anfang 2010 wurde die Webseite der SVP Stadt Zürich mehrmals verunstaltet. Es erschien der Schriftzug «26C3 - Here be Dragons». Auch wurde ein YouTube-Video mit Bezug auf die Minarettbauverbotsinitiative aufgeschaltet. Das Video lehnt sich an die Werbung eines Schweizer Kräuterbonbonherstellers, welcher mit dem Werbespruch «Wer hat's erfunden» bekannt ist. «Here be Dragons» war der Slogan des 26. Kongresses des Chaos Computerclubs (CCC) in Berlin. Dieser findet jeweils zwischen Weihnachten und Neujahr statt und zieht bis zu 3000 interessierte Hacker, Geeks, Netzkünstler, Datenschützer usw. an. Nach dem Säubern wurde die Homepage ein weiteres Mal verunstaltet, dieses Mal mit einem Jux-Video unter dem Titel «300 – SVP must die» in Anlehnung an den Film «300». Bei dieser Webseitenverunstaltung dürfte eine Lücke im Content Management System ausgenutzt worden sein.

Screenshot der kompromittierten SVP-Seite.[19]

Schon direkt nach der Minarettverbotsinitiative wurden über 5000 Seiten gehackt, darunter auch Seiten von SVP-Ortsparteien und der Jungen SVP. Hinter diesen Angriffen wurde aber eine Täterschaft mehrheitlich aus dem türkischen Raum vermutet. In diesem Fall dürfte der Angreifer aus dem deutschen oder deutsch-schweizerischen Raum stammen und Teilnehmer des CCC-Kongresses gewesen sein. Die Webseite wurde jedenfalls vom CCC als Ziel aufgelistet. Wer genau dahintersteckt, ist jedoch unbekannt. Strafanzeige wurde keine erstattet.

---

17 http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (Stand: 27. August 2010)

18 http://www.admin.ch/ch/d/sr/c780_1.html (Stand: 27. August 2010)

19 Quelle: http://yfrog.com/j5svpp (Stand: 27. August 2010)

Ein anderer Fall sorgte im Januar 2010 für Schlagzeilen. Eine *Cross-Site-Scripting Schwachstelle* im Webauftritt der Spanischen EU-Präsidentschaft «www.eu2010.es» erlaubte es, über einen präparierten Link das Bild von Präsident Zapatero auf der Frontseite der Website durch ein Bild des Komikers Rowan Atkinson (alias Mr. Bean) auszutauschen[20]. Dieser Script-Inject, der das Bean-Bild von einem anderen Server nachgeladen hat, wurde anscheinend über die Suchfunktion der Webseite eingeschleust. Der so präparierte Link wurde über verschiedene Kanäle verteilt. Aufgrund der hohen Resonanz brach die Seite zeitweilig unter dem grossen Ansturm an Neugierigen zusammen.

Screenshot nach Aufruf des präparierten Links.

Bei einem Cross Site Scripting (XSS) Angriff wird der Webserver im eigentlichen Sinne nicht angegriffen. Dieser wird nur missbraucht, um beim Browser des Nutzers Fremdinhalt in eine Webseite einzuschleusen. Die eigentliche Webseite wird dabei nicht verändert. Meist wird diese Methode benutzt um an Login-, respektive Kreditkartendaten zu gelangen, indem unter einer Vertrauenswürdigen Webadresse eine Phishingseite eingeblendet wird. Diese Fehlfunktion wird durch schlechtes oder fehlendes Überprüfen von Eingabefeldern verursacht. Wird bei einem interaktiven Feld beispielsweise in der Suchfunktion einer Webseite der *HTML-Code* nicht herausgefiltert, wird dieser bei der Resultateseite durch den Browser interpretiert. So können beispielsweise Bilder, aber auch ganze Formulare eingeschleust werden. XSS gehört zu den häufigsten Angriffsverfahren im Web.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Ausgewählte Spionagefälle im Halbjahr 1/2010

Im letzten Halbjahr wurden wieder einige Spionagevorfälle bekannt, so beispielsweise gegen Google, Adobe und auch gegen das Büro des Dalai Lama. Der deutsche Innenminister Thomas de Maizière warnte dann auch im jüngsten deutschen Verfassungsschutzbericht vor der Gefahr der wachsenden Wirtschaftsspionage. Besonders gefährdet seien Wirtschaftsunternehmen und öffentliche Stellen. Das deutsche Bundesamt für Verfassungsschutz hat die Gefahr von Industriespionage in Deutschland von Seiten

[20] http://www.la-moncloa.es/IDIOMAS/9/ActualidadHome/2009-2/04012010_AttackOnSpanishEuPresidencyWebsite_Communique.htm (Stand: 27. August 2010)

Russlands und Chinas als sehr ernst eingestuft.[21] Die bekannt gewordenen Spionagefälle sind nicht als unabhängige Einzelfälle zu betrachten, vielmehr muss auf Gemeinsamkeiten beispielsweise bei der Infrastruktur geachtet werden. Dies wird in Kapitel 5.1 weiter erläutert.

4.1.1 Google meldet Cyberangriffe

Google hat am Anfang des Jahres bekannt gegeben, dass sie Opfer von gezielten Hacking-Angriffen geworden waren. Anscheinend waren im gleichen Fall auch Firmen im Bereich Internet, Finanz und militärisches Umfeld betroffen. Laut Google haben die Angriffe im Zeitraum Dezember 09 respektive Januar 10 stattgefunden und wurden gegen Google und mindestens zwanzig weitere Unternehmen durchgeführt. Diese Hacker-Angriffe seien hochentwickelt und gezielt gewesen. Im Falle von Google seien Ziel des Angriffs vor allem Konten von Google-Mail gewesen. Im Fokus hätten Accounts chinesischer Menschenrechts-Aktivisten gestanden. Den Hackern sei es aber nicht gelungen, an sensible Daten zu gelangen. In zwei Fällen, so die Recherchen von Google, haben es die Hacker zumindest geschafft, den Posteingang anzuzeigen. Die Inhalte der E-Mails hätten sie aber nicht aufrufen können. Darüber hinaus sei aufgefallen, dass einige Google-Mail-Accounts von amerikanischen, europäischen und chinesischen Menschenrechts-Aktivisten seit Längerem ausgespäht werden. Der Zugang zu diesen sei aber nicht mit Hilfe von Schadsoftware, sondern via *Phishing* gegen die Account-Inhaber erlangt worden.

E-Mails werden zudem häufig mit präparierten *PDF-Dateien* an Firmen und öffentliche Stellen versendet. Beispielsweise hat eine Schweizer Firma gezielt versendete und mit Schadcode versehene PDF-Dokumente erhalten. In diesem Fall sollte eine Sicherheitslücke ausgenutzt werden, welche bereits am 15. Dezember 2009 publiziert, aber erst Anfang Januar 2010 geschlossen worden ist. Es wird festgestellt, dass im Gegensatz zu früher als bei gezielten Hacker-Angriffen häufig Office-Dokumente als Infektionsvektoren verwendet wurden, heute meistens PDF-Dateien eingesetzt werden.

Angriffe dieser Art sind seit Langem bekannt und vielfach dokumentiert: Verwiesen sei hier beispielsweise auf «Tracking Ghostnet» vom März 2009[22] oder die Northrop-Studie für die US-China Economic and Security Review Commission vom Oktober 2009 («Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation»)[23]. Der Angriff, welcher von Google vermeldet wurde, ist dabei technisch zwar ausgereift, kann aber von seiner technischen Komplexität nicht mit anderen, wie beispielsweise dem Angriff auf das EDA verglichen werden.

4.1.2 «Shadows in the Cloud»: Chinesisches Spionagenetzwerk

Am 6. April 2010 haben die Gruppen «Information Warfare Monitor» und «Shadowserver Foundation» einen Bericht mit dem Namen «Shadows in the Cloud» veröffentlicht.[24] Der Bericht handelt von Spionageaktivitäten gegen tibetische NGOs und das Büro des Dalai Lama, welche mit Hilfe von IKT-Mitteln ausgeübt worden sind. Dies ist nach «Tracking Ghostnet – Investigating a Cyber Espionnage Network» der zweite Bericht dieser Autoren zu möglichen chinesischen Spionageaktivitäten gegen entsprechende Ziele.

---

[21] Deutscher Verfassungsschutzbericht 2009: http://www.verfassungsschutz.de/de/publikationen/verfassungsschutzbericht/vsbericht_2009/ (Stand: 27. August 2010)

[22] Tracking Ghostnet: http://www.tracking-ghost.net (Stand: 27. August 2010)

[23] Northrop-Studie - http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf (Stand: 27. August 2010)

[24] Shadows in the Cloud - http://shadows-in-the-cloud.net/ (Stand: 27. August 2010)

Schon 2005 veröffentlichte die New York Times einen Bericht zu einer FBI-Operation namens «Titan Rain». In diesem Fall ging es um infizierte Computersysteme der US-Behörden, bei denen Dokumente und Informationen über längere Zeit abgesogen wurden. Als möglicher Täter wurde dabei China genannt. Auch in der Schweiz haben sich seitdem solche Angriffe gegen die Rüstungsindustrie und gegen Regierungsstellen ereignet. In diesen Fällen sendeten die Angreifer präparierte Dokumente mit gefälschtem Absender an Schlüsselpersonen der betreffenden Unternehmen. Die Nachrichten waren auf die Empfänger zugeschnitten, was auf vorgängige nachrichtendienstliche Informationsbeschaffung hinweisen kann.

Dieser Bericht ist ein Folgebericht auf Grund der Ermittlungen im Fall «GhostNet». Die Wissenschaftler haben entdeckt, dass auf einigen der dort infizierten Computer noch andere Malware installiert worden ist. Dies hat zur Entdeckung eines weiteren Spionagenetzwerkes geführt. Es konnten Opfer in über 36 Ländern identifiziert werden; eine Mehrheit der Betroffenen befinde sich in Indien. Gemäss dem Bericht wurden 115 betroffene Systeme in der Schweiz eruiert. Grössere Unternehmen und Betreiber von kritischen Informationsinfrastrukturen waren dabei nicht betroffen.

4.1.3 Die schöne Facebook-Freundin der Elitesoldaten

Soziale Netzwerke entpuppen sich für Armeen in vielen Ländern als Sicherheitsrisiko. Soldaten teilen via Internet verschiedenste Informationen mit und geben dadurch nicht selten auch nützliche Hinweise für ihre Gegner bekannt. Sensibilisierungskampagnen können diese Problematik nur bedingt entschärfen und Verbote sind manchmal kontraproduktiv.[25]
Anfang Jahr kündigte ein israelischer Soldat auf Facebook den letzten Einsatz seiner Einheit vor dem Heimurlaub an, und erwähnte dabei den Tag und das betroffene Dorf im Westjordanland. Dies hatte zur Folge, dass die geplante Aktion abgesagt werden musste und der fehlbare Soldat sich vor Gericht zu verantworten hatte.[26]
Kurz darauf wurde bekannt, dass eine bezaubernde junge Frau sich auf Facebook mit israelischen Militärs angefreundet und ihnen Geheimnisse entlockt habe. Laut einem Pressebericht tappten 200 Elitesoldaten in diese Falle.[27] Hinter dem falschen Profil stecke vermutlich die libanesische Schiitenmiliz Hisbollah.

Ob diese Geschichte wahr oder nur Teil der grossangelegten Sensibilisierungskampagne[28] der Armee ist, bleibt zu spekulieren. Auf der anderen Seite wird Israel nachgesagt, selber mit Hilfe von Internet und Sozialen Netzwerken Informanten aus den Reihen ihrer Feinde zu gewinnen.[29]

---

[25] http://news.bbc.co.uk/2/hi/8540236.stm;
http://www.scmagazineus.com/army-ends-ban-on-facebook-flickr-other-social-media-sites/article/138392/;
http://www.computerworld.com/s/article/9136255/Marines_solidify_ban_on_Facebook_Twitter;
http://www.marinecorpstimes.com/news/2010/02/military_socialmedia_update_022610w/ (Stand: 27. August 2010)

[26] http://computer.t-online.de/israel-facebook-eintrag-verhindert-militaeraktion/id_40993294/index;
http://www.sueddeutsche.de/digital/israel-dank-facebook-nachricht-im-militaergefaengnis-1.15999;
http://news.bbc.co.uk/2/hi/middle_east/8549099.stm (Stand: 27. August 2010)

[27] http://www.blick.ch/news/ausland/soldaten-ueber-facebook-ausspioniert-147053;
http://www.spiegel.de/politik/ausland/0,1518,694582,00.html (Stand: 27. August 2010)

[28] http://www.independent.co.uk/news/world/middle-east/israel-warns-of-facebook-spies-1687139.html;
http://news.bbc.co.uk/2/hi/7343238.stm (Stand: 27. August 2010)

[29] http://www.theregister.co.uk/2010/04/07/facebook_spying_gaza/; http://news.bbc.co.uk/2/hi/middle_east/8585775.stm (Stand: 27. August 2010)

4.2 Deutsche Innenministerkonferenz plant Massnahmen gegen Internetkriminalität

Am 27. und 28. Mai 2010 ist die Deutsche Ständige Konferenz der Innenminister und –senatoren der Länder (IMK) zu ihrer Frühjahrstagung zusammengekommen. Im Vorfeld hat der Vorsitzende Hamburger Innensenator Ahlhaus in der Presse angekündigt, dass die IMK ein umfangreiches Massnahmenpaket schnüren wolle, um der wachsenden Bedrohung durch Kriminelle im Netz zu begegnen. Hierzu sei eine Internet-Zentralstelle vorgesehen, in welcher alle Erkenntnisse von Bund und Ländern zusammenlaufen. Neben Spezialisten der Sicherheitsbehörden sollten dort auch Experten aus der Internet-Branche vertreten sein. In einem zweiten Schritt soll dann eine entsprechende internationale Anlaufstelle geschaffen werden. Zudem wäre auf EU-Ebene eine Meldepflicht für Hackerangriffe, neuartige Viren und Betrugsserien im Netz anzustreben. Ausserdem planen die Innenminister als präventiven Ansatz eine breit angelegte Aufklärungskampagne über Risiken des Internets. In Hamburg wurde eine entsprechende Aktion bereits Ende April gestartet.
Die IMK nahm den von ihrem zuständigen Arbeitskreis gefassten Beschluss zum Bericht «Strategie zur Bekämpfung der Informations- und Kommunikations-Kriminalität» sowie die durch den Arbeitskreis eingeleiteten Schritte zur Umsetzung der in dem Bericht enthaltenen Handlungsempfehlungen zur Prüfung und gegebenenfalls zur Umsetzung auf.

Die vom Phänomen Internetkriminalität ausgehende Bedrohung stellt derzeit eine der wesentlichen Herausforderungen im Bereich Verbrechensbekämpfung und Prävention dar. Da der bisher meist propagierte Ansatz einer Verbesserung der Zusammenarbeit der einzelnen regionalen und nationalen Polizeikräfte nicht die gewünschten Erfolge erzielt hat, werden nun verschiedentlich auch alternative Wege geprüft. Die Internetkriminalität macht nicht an Staatsgrenzen Halt und auch Opfer einer Tat befinden sich häufig an mehreren Orten. Umfangreiche Kenntnisse über die aktuelle Lage, eine Gesamtschau der konkreten Vorkommnisse, sowie eine Koordination der vorhandenen Ressourcen sind für eine effiziente Strafverfolgung unabdingbar. In diese Richtung stösst auch die EU-Kommission, welche die Schaffung einer europaweit operierenden Polizeieinheit gegen Internetkriminalität erwägt.
Strafverfolgungsbehörden müssen in Public-Private-Partnerships mit der Privatwirtschaft, Internet-Nutzern, und Opferverbänden zusammenarbeiten, um möglichst präzise Lagedarstellungen zu verfassen, Nutzer zu schützen und Kriminelle verfolgen zu können. Herkömmliche polizeiliche Ermittlungs- und Beweissicherungsmethoden sind im Bereich der Internetkriminalität nur bedingt anwendbar. Eine erfolgreiche Bekämpfung verlangt auch Prävention durch Sensibilisierung und Information von Bürgern, Institutionen und Organisationen.

4.3 EC-Karten Problem oder der 2010 Bug

Zehn Jahre ist es her, als die ganze Welt gespannt gewartet hat, ob Computer den Jahrhundertwechsel unbeschadet überstehen. Das Jahr 2000 Problem hielt einige Soft- und Hardwarehersteller in Atem und am Schluss ist doch nichts passiert, alles ging ohne Probleme über die Bühne. Zehn Jahre später hat ein Datumsproblem dennoch völlig unverhofft zugeschlagen: Deutsche Geldautomaten und Einzelhandelsterminals hatten ab dem 1. Januar 2010 Probleme bei der Verarbeitung des sogenannten *EMV-Chips*. Durch einen Programmierfehler konnte die Jahreszahl 2010 nicht richtig verarbeitet werden. Betroffen waren laut einer Schätzung rund 30 Millionen Karten. Der französische Hersteller Gemalto hatte den Fehler eingestanden. Damit die Karten kurzfristig wieder funktionierten hat man die Geldautomaten und Zahlungsterminals dahingehend umprogrammiert, dass beim Auslesen der Karten wieder ausschliesslich auf die hinterlegten Daten des Magnetstreifens zurückgegriffen wurde. Da im Ausland diese Umprogrammierung nicht

umgesetzt wurde, kamen findige Kreditkartennutzer auf die Idee, den Chip mit Klebestreifen abzukleben um damit einen Fallback auf den Magnetstreifen zu erzwingen. Diese Methode hatte aber auch Potential, das Lesegerät zu zerstören.

Um den kostspieligen Umtausch der Karten zu verhindern, wurde an Geldautomaten respektive an speziellen Kartenlesegeräten die Chipsoftware umprogrammiert und repariert. Hierzu muss die Software auf der Karte mittels eines geheimen Schlüssels zuerst freigeschaltet werden. Dieser Schlüssel wird über einen gesicherten Kanal an den Geldautomaten übertragen. Im Gegensatz zum Magnetstreifen kann ein Chip wirksam gegen eine Duplizierung geschützt werden und verhindert damit sogenanntes Skimming.

Bemängelt beim Vorgehen wurde allerdings, dass beim Lösen der Panne weder das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch die Finanzmarktaufsicht (BaFin) hinzugezogen worden war.[30]

Ein wesentliches Merkmal der Chipkarten ist die Tatsache, dass nach dem Aufspielen der Software eigentlich keine nachträglichen Änderungen mehr möglich sein sollten. Die Chipkarten lassen sich zwar verändern, dies aber nur mit grossem Aufwand. Vorgesehen ist hierfür ein Schlüssel für die Umprogrammierung. Dies stellt natürlich nicht nur die Frage nach einer angemessenen Verschlüsselung und Sicherung zwischen Bank und Endkunde, sondern allgemein die Frage, wer alles diesen Schlüssel besitzt und was alles mit der Kreditkarte angestellt werden kann, wenn man diesen Schlüssel hat.

4.4 Mariposa

2009/2010 entdeckte die Gruppe Defence Intelligence[31] ein Botnetz, welches zu den umfassendsten Netzen gehörte, die je gefunden wurden. Ein zwischen Dezember 2009 und Februar 2010 durchgeführtes *Sinkholing* ermöglichte es, 11 Millionen einzigartige IP-Adressen zu detektieren. Das Netz wurde „Mariposa“ („Schmetterling“ auf Spanisch) getauft, da für die Schaffung des Botnetzes das Malware Kit Butterfly verwendet wurde. Der spanische Name geht auf den Umstand zurück, dass es sich bei den Botnetzbetreibern um Spanier gehandelt hat.

Das Botnetzwerk diente hauptsächlich dazu, sensible Daten von den infizierten Computern zu stehlen. Dazu gehören Informationen über Konten, Namen von Usern, Passwörter und Details zu Online-Bankkonten. Auf einem Teil der infizierten Computer wurde zusätzlich eine Malware heruntergeladen, um *DDoS- (Distribute Denial of Service)* Angriffe durchzuführen. Diesem Netz fielen Kunden der vierzig weltweit grössten Banken sowie Computer von mindestens der Hälfte aller „Fortune-1'000“-Unternehmen zum Opfer. Die Opfer stammen aus 190 Ländern.

Das Malware Kit Butterfly stammt von einem Hacker namens Iserdo. Der 23-Jährige wurde kürzlich im slowenischen Maribor[32] verhaftet. Die Botnetzbetreiber hingegen wurden Anfang des Jahres in Spanien festgenommen. Die von der Guardia Civil[33] durchgeführte Aktion führte zur Verhaftung von drei spanischen Bürgern. Diese wurden aufgrund der von ihnen im

---

[30] http://www.faz.net/s/Rub645F7F43865344D198A672E313F3D2C3/Doc~EB6DD9EEC40AA4E1FB4EB70152FD024D2~ATpl~Ecommon~Sspezial.html (Stand: 27. August 2010)

[31] http://defintel.com (Stand: 27. August 2010)

[32] http://www.theregister.co.uk/2010/07/28/mariposa_vxer_ciffed/ (Stand: 27. August 2010)

[33] Nebst den Ordnungskräften bildete sich die “Mariposa Working Group”. Diese bestand aus der Defence Intelligence, Panda Security, Neustar, Directi, dem Georgia Tech Information Security Center und anderen Forschern.

Netz verwendeten Pseudonyme sowie ihres Alters identifiziert. Es handelte sich dabei um Netkairo, 31, Johnny Loleante, 30, und Ostiator, 25.

Nichtsdestotrotz musste sich die spanische Justiz an das Strafgesetzbuch des eigenen Landes halten. Gemäss den Aussagen von Hauptmann Cesar Lorenzana[34], stellvertretender Leiter der Abteilung technologische Verbrechen der Guardia Civil, stellt es in Spanien kein Verbrechen dar, ein Botnetz zu betreiben oder einen schädlichen Code zu verteilen. Als einzig möglicher Anklagegrund gilt somit der Datendiebstahl.

Als kleine Randnotiz ist zu erwähnen, dass zwei Monate nach ihrer Verhaftung zwei Betreiber von Mariposa es mit einem Bewerbungsgespräch, bei Panda Security, einem Mitglied der Mariposa Working Group, versucht haben. Bei dieser Gelegenheit mussten sie feststellen, dass eine Visitenkarte als Betreiber eines Botnetzwerkes nicht unbedingt die beste Voraussetzung ist, um einen Arbeitsplatz zu erhalten.

4.5 Google sammelt versehentlich WLAN-Nutzdaten

Google hat während den Kamerafahrten für Google Street View nebenher auch *WLAN*-Daten aufgezeichnet. Hierzu beschränkte sich Google nicht nur auf *MAC-Adresse* und *SSID* des WLAN-Routers, sondern schnitt auch die im WLAN übertragenen Nutzdaten mit. Unter Nutzdaten versteht man den allgemeinen Internetverkehr, der von und an einen Wireless-Router gesendet wird, allerdings muss dazu der Datenverkehr unverschlüsselt sein. Ist dies der Fall, können beispielsweise Passwörter im Klartext ausgelesen werden.

Ein Softwareentwickler von Google hatte das Mitschneiden von Nutzdaten in die Aufnahmesoftware von Street View integriert. Dies war ein Verstoss gegen die internen Datenschutzregeln des Unternehmens. Dem Entwickler drohen nun Konsequenzen. Zudem hat die Hamburger Staatsanwaltschaft am 19. Mai 2010 wegen der Datensammlungen ein Ermittlungsverfahren gegen Google eingeleitet.

Es steht ausser Frage: Wer ein WLAN-Router betreibt, muss diesen auch ausreichend verschlüsseln, ansonsten läuft er Gefahr, dass irgendeine fremde Person die Daten mitschneiden oder aber den Router für kriminelle Zwecke missbrauchen kann. Dass in diesem Falle Nutzdaten systematisch gesammelt wurden, macht keinen Unterschied. Aber gerade ein Unternehmen, das mit öffentlichen und persönlichen Information Geld verdient, hat hier eine besondere Verantwortung. Insbesondere bedarf es einer offenen Kommunikation und klaren Richtlinien für die Mitarbeitenden, was den Umgang mit Daten angeht.

Aber auch bei klaren Richtlinien wird man sich in Zukunft vermehrt die Frage stellen müssen, was öffentlich zugänglich ist und was privat ist. Dieser Übergang ist zunehmend fliessend und hört nicht mehr am Gartenzaun auf. Diese Diskussion wird geführt werden und dies nicht erst seit Google Street View – auch Facebook, Twitter und Co. steuern hier ihren Teil bei. Bei all diesen Diensten wird den Benutzern eine hohe Informationskompetenz abverlangt, die sie aber teilweise (noch) nicht besitzen.

[34] http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/ (Stand: 27. August 2010)

4.6 Einzelne Bande war für zwei Drittel aller Phishing-Angriffe verantwortlich

Gemäss dem neuesten Trimesterbericht[35] der Anti Phishing Working Group (APWG) sind 66% aller Phishing-Angriffe in den letzten sechs Monaten auf das Botnetz „Avalanche“ zurückzuführen. Hinter diesem Namen verbirgt sich eine der grössten kriminellen Gruppe, die im Phishing-Bereich tätig ist. Über dieses Botnetz wurden zwei Drittel der Phishing-Seiten, die im zweiten Semester 2009 registriert wurden, verwaltet (84'250 von 126'697).

Verschiedene Sicherheitsexperten glauben, dass hinter dem Botnetz „Avalanche“ die kriminelle Bande „Rock Phish“ steckt. Beide Botnetze verwenden dieselbe Technik wie beispielsweise die regelmässige Registrierung von Domain-Namen, die Verwendung von *Fast-Flux* und das Einfügen von sechs Webseiten pro Domain-Name. Entdeckt wurde „Avalanche“ erstmals Ende 2008, als „Rock Pish“ gerade von der Bühne verschwunden war. Gemäss dem Bericht der APWG verwendet „Avalanche“ die gleiche Technik wie „Rock Pish“, hat diese aber verbessert und verfeinert.

4.7 Ausfall der «.de»-Domain

Am 12. Mai 2010 hatte eine *DNS-Panne* bei der deutschen Registrierungsstelle DENIC auf Stufe Top-Level Domäne zur Folge, dass «.de»-Webseiten partiell nicht mehr erreichbar waren. DENIC verwaltet als zentrale Registrierungsstelle mehr als 13 Millionen Domänen.[36] Top-Level-Domänen anderer Länder sowie Domänen wie «.com» oder «.net» waren davon nicht betroffen, wobei es durch Abhängigkeiten der verschiedenen Dienste durchaus auch zu Ausfällen ausserhalb von Deutschland kommen konnte. Dies ist beispielsweise dann der Fall, wenn «.com»-Seiten über «.de»-DNS-Server aufgelöst werden. Spekulationen zu Folge könnte der Ausfall mit dem Umzug des Registrierungsdienstes von Amsterdam nach Frankfurt zusammenhängen. Bei einem Ausfall eines DNS-Dienstes ist allerdings nicht nur das Surfen im World Wide Web betroffen, viel gravierender dürfte der Ausfall der E-Mail Infrastruktur sein, da die E-Mails das Ziel nicht mehr erreichen.

DNS-Servern kommt eine wichtige, wenn nicht die wichtigste Rolle im Internet zu. Sie bilden das Bindeglied zwischen den IP-Adressen, welches die Computer verstehen und den Domänennamen, welche sich der Mensch einfach merken kann. Dies haben auch Kriminelle gemerkt, weshalb sie effiziente DDoS-Attacken direkt auf Nameserver richten und damit alle Webseiten, die durch diesen DNS-Server aufgelöst werden, unerreichbar machen. Gegen solche Angriffe gibt es derzeit keine Abwehrmöglichkeit. Ein anderes Szenario ist die Manipulation von DNS-Anfragen. Hierbei wird ein Opfer bei korrekter Eingabe der Webadresse beispielsweise auf einen manipulierten Server geleitet, so genanntes DNS-Spoofing.

4.8 Eingeführte Vorratsdatenspeicherung verstößt gegen Deutsches Grundgesetz

Anbieter von Telekommunikationsdiensten waren in Deutschland gemäss jüngster

[35] http://www.apwg.org/reports/apwg_report_Q4_2009.pdf (Stand: 27. August 2010)

[36] http://www.heise.de/netze/meldung/DNS-Fehler-legen-Domain-de-lahm-3-Update-999068.html (Stand: 27. August 2010)

Gesetzgebung verpflichtet, alle Angaben zu speichern, welche erforderlich sind, um zu rekonstruieren, wer, wann, wie lange, mit wem, von wo aus kommuniziert hat oder zu kommunizieren versucht hat. Nicht gespeichert werden durfte demgegenüber der Inhalt der Kommunikation sowie welche Internetseiten von den Nutzern aufgerufen werden. Das Deutsche Bundesverfassungsgericht (BVerfG) hat mit dem Urteil vom 2. März 2010 (1 BvR 256/08)[37] entschieden, dass die umstrittenen Bestimmungen zur *Vorratsdatenspeicherung*[38] in der eingeführten Form gegen das Grundgesetz (wie die deutsche Verfassung heisst) verstossen und somit nichtig seien.
Die Vorratsdatenspeicherung ist gemäss BVerfG nicht prinzipiell verfassungswidrig – sie muss jedoch nach dem Verhältnismässigkeitsgrundsatz ausgestaltet werden: Es müsse eine hinreichende Begrenzung der Verwendungszwecke der Daten vorgenommen werden und die Datensicherheit beim speichernden Unternehmen muss gewährleistet sein. Zudem brauche es normenklare Regelungen bezüglich Transparenz der Datenübermittlung und zum Rechtsschutz. Das Gericht hat also nicht die Vorratsdatenspeicherung an sich abgelehnt, sondern deren Umsetzung bemängelt.
Die anlassunabhängige Speicherung von Daten, welche die Zuordnung einer IP-Adresse zu einem Internetanschluss-Inhaber ermöglicht, kann durchaus verfassungsmässig sein. Jedoch dürfen auch diese Daten nicht uneingeschränkt verwendet werden. Der Gesetzgeber hat die behördlichen Auskunftsansprüche zu regeln. Jetzt muss die deutsche Bundesregierung nachbessern und grundgesetzkonforme Bestimmungen einführen.

In der Schweiz sind die Normen betreffend Datenspeicherung und -herausgabe durch Anbieter von Fernmeldediensten im Fernmeldegesetz[39], in der Fernmeldedienstverordnung[40] sowie im Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs[41] und in der zugehörigen Verordnung[42] zu finden. Die Gesetzgebung betreffend Überwachung des Post- und Fernmeldeverkehrs wird zurzeit revidiert.[43]

4.9 Hackerangriff auf Emissionshandel / Zugangsdaten von Unternehmen erbeutet

Der Handel mit sogenannten Emissionszertifikaten ist ein wichtiges Instrument bei der Reduzierung von Schadstoffemissionen. Über marktwirtschaftliche Regularien sollen Volkswirtschaften und Einzelunternehmen dazu gebracht werden, nach und nach weniger Emissionen etwa durch Verbrennung fossiler Energieträger zu verursachen: Überzählige Emissionszertifikate, die nicht durch Firmen verbraucht werden, können in eigens eingerichteten Handelssystemen an Firmen verkauft werden, welche die Umwelt stärker belasten als ihnen zusteht.

Am 2. Februar 2010 gelang es Angreifern mittels eines simplen Phishingangriffs an die Zugangsdaten von Benutzern von Emissionshandelsstellen zu gelangen. Das Phishing-Email wurde als Mitteilung (Warnung vor Hacker-Attacken!) der Deutschen

---

37 http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (Stand: 27. August 2010)

38 §§ 113a und 113b TKG (Telekommunikationsgesetz) und § 100g StPO (Strafprozessordnung).

39 FMG, SR 784.10: http://www.admin.ch/ch/d/sr/c784_10.html (Stand: 27. August 2010)

40 FDV, SR 784.101.1: http://www.admin.ch/ch/d/sr/c784_101_1.html (Stand: 27. August 2010)

41 BÜPF, SR 780.1: http://www.admin.ch/ch/d/sr/c780_1.html (Stand: 27. August 2010)

42 VÜPF, SR 780.11: http://www.admin.ch/ch/d/sr/c780_11.html (Stand: 27. August 2010)

43 http://www.bj.admin.ch/bj/de/home/themen/sicherheit/gesetzgebung/fernmeldeueberwachung.html (Stand: 27. August 2010)

Emissionshandelsstelle (DEHSt) getarnt und die Empfänger wurden aufgefordert, auf einen Link zu klicken und dort Benutzerangaben/Passwort erneut zu registrieren.

Die Betrüger verkauften die gestohlenen Verschmutzungsrechte weiter; in der Folge war das amtliche Register für den Emissionshandel in weiten Teilen Europas lahmgelegt. Das Schweizer Emissionshandelsregister des Bundesamtes für Umwelt (BAFU) hat ihre Kunden auf ihrer Webseite mit einer entsprechenden Warnung sensibilisiert.

Bemerkenswert an diesem Angriff ist weniger die technische Vorgehensweise, sondern das gewählte Ziel. Phishing-Angriffe gegen Finanzdienstleister sind in der Schweiz praktisch ausgestorben. Trotzdem erfreut sich diese Methode einer grossen Beliebtheit bei den Angreifern, welche mehrheitlich aus dem Nordafrikanischen Raum operieren. Den Angriffszielen sind keine Grenzen gesetzt, sofern diese nur mit Login und Passwort geschützt sind und sich damit Geld verdienen lässt. Betroffen sind vor allem Kreditkartenbetreiber, E-Mail Provider und Auktionsplattformen.

4.10 Microsoft kündigt Meldestelle für gestohlene Zugangsdaten an

Im Laufe des ersten Semesters 2010 kündigte der Softwarehersteller Microsoft die Schaffung einer Meldestelle für Identitäts- und Datendiebstahl an. Dank dem Internet Fraud Alert Center[44] unter der Leitung von Microsoft, das von der National Cyber-Forensics & Training Alliance[45] betrieben wird, sollen potenzielle Opfer von Daten- oder Identitätsdiebstahl wie Finanz- und E-Commerce-Institute mit Forschern und Regierungsagenturen zusammengebracht werden. Dies soll es ermöglichen, Informationen bezüglich solcher Delikte auszutauschen, um rasch und effizient handeln zu können. Findet ein Internetspezialist beispielsweise auf einem Drop Server eines Botnetzwerkes gestohlene Kreditkartennummern, könnte er diese dem Internet Fraud Alert Center zukommen lassen. Die Meldestelle würde die Informationen anschliessend an die beteiligten Betriebe weiterleiten.

4.11 DNS-Server gehackt: Pornos und Adware hinter Regierungs-Domains

Wie Sunbelt[46] berichtet, haben es Mitglieder der Webseite FLVDirect geschafft, die Domain Name Server einiger Webseiten der amerikanischen Regierung (.gov) so zu manipulieren, dass deren Besucher[47] auf die Webseite von Adware FLVDirect sowie die pornographische Webseite XXXBlackBook.com umgeleitet wurden. Die Kriminellen legten unter anderem neue *Subdomänen* wie tubes-1911.empria-kansas.gov an und nutzten auch diese, um die User umzuleiten.

---

44 https://www.ifraudalert.org/default.aspx (Stand: 27. August 2010)

45 http://www.ncfta.net/main/home/ (Stand: 27. August 2010)

46 http://sunbeltblog.blogspot.com/2010/07/flvdirect-affiliates-hacking-government.html (Stand: 27. August 2010)

47 Zu diesen Websites gehören: yaceycountync.gov, uppersiouxcommunity-nsn.gov, woodfin-nc.gov, dumontnj.gov, emporia-kansas.gov

5 Tendenzen / Ausblick

5.1 Spionage und Datendiebstahl IKT-Style

Seit dem Erscheinen des ersten MELANI Halbjahresberichtes 2005, ist der Diebstahl von Daten ein immer wiederkehrendes Thema. Unbefugte Datenbeschaffung wird aus rein finanziellen, kriminellen Interessen oder aber im Rahmen staatlich gestützter Spionage betrieben. Das Thema selber erfuhr einen zweiten medialen Frühling mit den Angriffen auf Google und andere IKT-Unternehmen, die unter dem Namen «Operation Aurora» Ende 2009 und Anfang 2010 in der Presse und in Fachgremien ausführlich diskutiert wurden. Dabei wurde diese Art gezielter, Malware gestützter Angriffe in Kreisen der IKT-Sicherheits-Community einem *Branding* unterzogen, welches im Begriff «Advanced Persistent Threat (APT)» gipfelte. Dies ging auch einher mit mehreren technischen Kommentaren, die dazu aufriefen, sich langfristig auf eben solche Angriffe zwecks Informations- und Datenbeschaffung einzustellen. Diese Erkenntnis, die sich Ende 2009 auch bei IKT-Sicherheitsunternehmen durchsetzte, ist verdankenswert, ändert aber nichts an der Tatsache, dass solche Spionagetätigkeiten bereits seit Jahren an der Tagesordnung sind.

Schon 2005 veröffentlichte die New York Times einen Bericht zu einer FBI-Operation namens «Titan Rain». In diesem Fall ging es um infizierte Computersysteme der US-Behörden, bei denen Dokumente und Informationen über längere Zeit abgesogen wurden. Als möglicher Täter wurde dabei China genannt. Ob diese Einschätzung zutrifft oder nicht, ist in einer ersten Beschauung unwichtig. Es gilt vielmehr, sich klar zu machen, dass die Täterschaft dahinter sich nicht mit einem Angriff zufrieden gibt und geben wird. Spionage ist ein langwieriger Prozess, der davon lebt, Quellen aufzubauen, abzuschöpfen und ständig neue zu platzieren, nicht zuletzt für den Fall, dass bereits vorhandene Informationslieferanten entdeckt oder ausgewechselt werden. Diese grundlegende Methodik der Spionage hat auch in der Welt der IKT seine Gültigkeit.

Eine Organisation, respektive ein Staat, der es sich zum Ziel gesetzt hat, an klassifizierte Informationen eines anderen Staates oder einer bestimmten Organisation zu gelangen, wird dafür in der einen oder anderen Form eine Infrastruktur, eine Operationsbasis aufbauen müssen. Dabei sind die Quellen steuernden Personen nur ein Teil des Ganzen. Die abgeschöpften Dokumente müssen gesichtet, ausgewertet und den Quellen muss darauf mitgeteilt werden, welche Art von Informationen weiter benötigt werden und welche weiteren Organisationen oder Behörden von Interesse sind. Eine solche Maschinerie hat allerdings auch den Nachteil, dass sie gewisse Prozesse, Vorgehensweisen und Mittel nur schwerfällig ändern kann und daher bei ihren Aktionen häufig ein ähnliches grundlegendes Muster zu erkennen ist. Seien es in der realen Welt die Art und Weise der Akquirierung von Quellen, die Art wie diese gesteuert werden oder aber die physischen Fronteinrichtungen vor Ort. Auch in der Welt der IKT, in der per se keine menschliche Quelle akquiriert werden muss und in der die Technik gewisse, schnelle Anpassungen und Kreativität erlaubt, sind dennoch sich gleichbleibende Stücke in der Gesamtinfrastruktur und der Vorgehensweise erkennbar.

Was in der klassischen Spionageabwehr eines jeden Landes und Unternehmens zum Standard gehört, nämlich das Verknüpfen einzelner Vorfälle, um die Gemeinsamkeiten zu erkennen und damit diese Vorfälle einem Gesamtkomplex zuordnen zu können, ist gerade in der Welt des Internets und der IKT eher eine Seltenheit. Dies mag in der klassischen Herangehensweise der IKT-Sicherheit liegen, bei der in erster Linie ein infiziertes System, ein einzelner Vorfall (ein so genannter Incident) gelöst werden muss, um die weitere Operabilität möglichst schnell zu gewährleisten. Eine Verknüpfung solcher Incidents über eine längere Zeitlinie zu einem Event findet selten bis gar nie statt. Auch im Sinne einer schnellen Berichterstattung werden zwar solche Einzelvorfälle wie Aurora, GhostNet, Titan

Rain, der EDA-Vorfall und dergleichen in die Medien gehoben, aber meist nur als für sich stehende, einzelne Vorfälle von IKT gestützter Spionage präsentiert. Dabei liessen sich bei genauerer Betrachtung viele dieser Vorfälle in wenige grössere Fallkomplexe verordnen, welche Aufschluss darüber geben, wer, wie und wo genau IKT zum Zwecke der Spionage und des Datendiebstahls einsetzt. Dies erlaubt auch eine genauere und abgewogene Beobachtung dieser Täterkreise und damit einen informierten Einsatz von präventiven Mitteln, da die grundsätzliche Bedrohungslage besser eingeschätzt werden kann. Die Unterscheidung von ungezielten kriminellen Massenangriffen und spezifisch angepassten, individuellen Attacken gestaltet sich für ungeübte Analysten häufig schwierig.

Auf Stufe Bund und zuhanden der Kritischen Infrastrukturen der Schweiz, ist es einer der Aufträge der Melde- und Analysestelle Informationssicherung MELANI, eine solche Auswertung einzelner Vorfälle vorzunehmen und wo möglich ein Gesamtbild eines solcher Fallkomplexes zu erstellen. Auch in anderen Ländern geht der Trend Richtung Verknüpfung solcher IKT-Vorfälle, um die Organisationen und Strukturen dahinter genauer definieren und erkennen zu können. Gerade im Umfeld privater Unternehmen, die der latenten Spionagebedrohung ausgesetzt sind, ist daher der Aufbau von Kapazitäten empfehlenswert, welche über ein klassisches Incident-handling im IT-Bereich hinausgehen. Sie erlauben es, Entscheidungsgrundlagen auf strategischer Ebene zur Verfügung zu stellen, die sich nicht nur auf den IKT-Bereich, sondern auf die Sicherung von Informationen und Daten im Allgemeinen beziehen.

5.2 Auslaufen vom Windows XP - Update-Service

Microsoft hat im ersten Halbjahr das Ende des Supportes von Windows XP SP2[48] (13. Juli 2010) und Windows Vista (13. April 2010) ohne Service Pack angekündigt. Windows XP ist seit Oktober 2001 auf dem Markt und immer noch die meist verbreitete Windows Version[49]. Laut dem Statistikunternehmen StatCounter sollen immer noch 53 Prozent mit WindowsXP arbeiten, während Windows 7 und Windows Vista mit 20% Marktanteil in etwa gleichauf liegen. Von nun an gibt es bei XP nur noch Support, wenn das Service Pack 3 installiert ist. Microsoft plant, den Support für Windows XP im April 2014 ganz zu beenden. Laut Gartner[50] ist bereits für Ende 2012 zu erwarten, dass neue Versionen vieler Anwendungen XP nicht mehr unterstützen werden.

Wie bei der Hardware gibt es auch bei Software nur eine beschränkte Garantiezeit und auch die Ersatzteile sind nicht bis in alle Ewigkeit lieferbar. Windows XP hat sich bei Firmen aber auch bei Privatpersonen so stark etabliert, dass an eine totale und globale Ablösung im Moment noch nicht zu denken ist. Wenn man bedenkt, wie schnell die Entwicklung im IKT-Bereich in den letzten Jahren stattgefunden hat, ist dies erstaunlich. Das Ende von XP wird aber unweigerlich kommen und da gerade bei Firmen ein Softwarewechsel von langer Hand geplant werden muss und nicht von heute auf morgen geschehen kann, ist hier Voraussicht gefragt, damit genügend Zeit zum Planen und Testen bleibt. Trotzdem wird es gerade bei Steuergeräten, wie sie beispielsweise in der industriellen Produktion, an Universitäten oder in Spitälern vorkommen, teilweise nicht oder nur schwer möglich sein, zeitnah auf ein

[48] There is no Service Pack 3 for the 64-bit version of Windows XP. If you are running the 64-bit version of Windows XP with Service Pack 2, you are on the latest service pack and will continue to be eligible for support and receive updates until April 8, 2014. Quelle: http://windows.microsoft.com/en-us/windows/help/learn-how-to-install-windows-xp-service-pack-3-sp3 (Stand: 27. August 2010)

[49] http://support.microsoft.com/gp/lifesupsps (Stand: 27. August 2010)

[50] http://www.cio.de/knowledgecenter/pc-support/2236656/index1.html (Stand: 27. August 2010)

anderes Betriebssystem zu migrieren, da Software und Steuerkarten auf das jeweilige Betriebssystem abgestimmt und teilweise auch zertifiziert sind.

Neben den Firmen muss aber auch die Situation der Privaten beachtet werden. Hier wird in der Regel ein Betriebssystem nicht gewechselt, sondern man ersetzt den alten mit einem neuen Computer, auf welchem jeweils ein (neues) Betriebssystem installiert ist. Hauptsache ist hier ein funktionierendes System. Warum sollte man auch einen funktionsfähigen Computer entsorgen. Das Problem, das sich hier ergibt, ist, dass nach dem End-of-Life Cycle die kritischen Sicherheitupdates wegfallen. Das heisst, dass neu bekannt werdende Sicherheitslücken nicht mehr geflickt werden. Sollte bis 2014 Windows XP immer noch einen überdurchschnittlichen Marktanteil haben, könnte dies zu einem grosses Problem werden.

Eine Übersicht über die Lebensdauer der einzelnen Windows-Produkte finden Sie hier:

http://support.microsoft.com/gp/lifeselect

5.3 Goliath und Davids Daten

Internet-unterstützte Geräte (*Smartphones, eBook-Reader*, etc.), Soziale Netzwerke und andere Internet-Kommunikations-Dienste erleichtern das Leben und bieten den Vorteil, dass sich ihre Benutzer untereinander einfacher verbinden und austauschen können. Durch Erhebung von statistischen Daten über die Nutzung können die Dienstleistungen laufend verbessert und durch immer gezieltere Werbung (Gratis-)Angebote finanziert werden. Deshalb wollen die Anbieter solcher Applikationen an möglichst viele Informationen ihrer Nutzer herankommen. Wer seine Privatsphäre schützen will, muss sich oft durch seitenlange unübersichtliche Datenschutzeinstellungen kämpfen und versteht oft nicht, mit welchen Konsequenzen er bei welcher Konfiguration rechnen muss. Zudem werden konstant neue Verknüpfungs- und Auswertungsmöglichkeiten von Datensammlungen entwickelt. Auch wenn man ganz bewusst entscheidet, was für Daten man Internetdienstanbietern preisgibt, verliert man häufig die Kontrolle darüber, was mit diesen passiert. Die Datenerhebung, -verarbeitung und -nutzung ist in den seltensten Fällen transparent. Ein heute für einen bestimmten Zweck erfasster Datensatz kann morgen durch Verknüpfung mit neuen Daten ganz andere, unerwartete Aussagen ermöglichen. Da in der Schweiz die Vertragsfreiheit gilt, können Anbieter und Käufer/Nutzer im Rahmen der Rechtsordnung grundsätzlich alles vereinbaren, denn es ist niemand gezwungen, ein entsprechendes Produkt zu kaufen oder eine Dienstleistung in Anspruch zu nehmen. Änderungen der Nutzungsbedingungen (Terms & Conditons) oder der Datenschutzbestimmungen (Privacy Policy) können aber typischerweise vom Anbieter einseitig, ohne Berücksichtigung der Kunden beschlossen werden. Wer mit den neuen Bestimmungen nicht einverstanden ist, hat meist nur die Möglichkeit, sich vom entsprechenden Dienst abzumelden oder das Produkt nicht mehr zu verwenden. Es scheint aber fraglich, ob jemand, der seine Kontakte mittlerweile fast ausschliesslich über ein Soziales Netzwerk pflegt, sich von diesem Dienst verabschieden kann und will, sowie ob SmartPhone-Nutzer ihr liebgewonnenes Gadget wieder zurückgeben, weil der Anbieter sich weitreichende Datenerhebungs-, -bearbeitungs- und -weitergaberechte ausbedingt. Viele Leute mühen sich erst gar nicht mit den seitenlangen, kompliziert geschriebenen Bedingungen ab. Typischerweise möchte man ja ein Produkt oder einen Dienst nutzen und sich nicht stundenlang mit dem Lesen langweiliger Texte und exzessiver Konfiguration beschäftigen und denkt sich:
«Was in den Allgemeinen Bestimmungen steht, wird wohl schon seine Ordnung haben und die Grundkonfiguration ist sicher auch nicht schlecht.»Nutzerinnen und Nutzer müssen aber ihre Selbstverantwortung wahrnehmen und sich auf dem Laufenden halten. Das bedeutet vor allem auch, das Kleingedruckte zu lesen und sich zu vergewissern, ob man eine bestimmte Information freigeben will. Die Nutzer müssen im Bewusstsein handeln, dass mit ihren Daten sehr weitgehende Persönlichkeitsprofile erstellt werden können – sie «bezahlen» (Gratis-

)Angebote mit ihren persönlichen Daten, die sie im Gegenzug preisgeben. Und die Anbieter solcher Dienste generieren ihre Einnahmen über die Werbung. Diese steigen, je mehr Personen solche Dienste in Anspruch nehmen und je gezielter die Bedürfnisse der Nutzerinnen und Nutzer analysiert werden können. Die Geschäftsmodelle basieren auf der Überlegung, dass die Nutzer bereit sind, Informationen zur Verfügung zu stellen, wenn sie dafür ein nützliches Produkt erhalten, das ihnen das Leben erleichtert: Auf einfache Weise mit Freunden in Kontakt zu sein, das richtige Rezept für das Abendessen oder das passende Restaurant in der Umgebung zu finden, oder auf dem Stadtbummel interessante Angebote von Geschäften zu erhalten. Auf der Suche nach möglichst vielen Benutzern und Werbemöglichkeiten stellen die Anbieter laufend neue Applikationen zur Verfügung.

Es gilt weiter zu bedenken, dass man häufig auch Daten von Drittpersonen verbreitet: Im Online-Adressbuch finden sich detaillierte Kontaktangaben und auch in nicht-öffentlichen Alben werden Fotos von Freunden und Bekannten dem Anbieter zur Verfügung gestellt. In diesem Zusammenhang sei darauf hingewiesen, dass Gesichtserkennungsprogramme immer besser werden und mehrere Smartphones mit *GPS-Funktion* jedes gemachte Foto mit einem so genannten Geotag versehen, welches die genauen Koordinaten des Erstellungsortes angibt. Dadurch eröffnen sich Möglichkeiten, die man sich wohl noch vor kurzer Zeit beim Upload von Fotos nicht hat vorstellen können. Auch ortsbasierte Dienste, welche ermöglichen, Freunden den aktuellen Aufenthaltsort mitzuteilen,[51] bergen neben ihrem unbestrittenen Nutzen auch Gefahren, bei deren Verwirklichung man im besten Fall nur leichte Unannehmlichkeiten zu gewärtigen hat – in einem schlechteren Fall hingegen zu Hause eingebrochen wird (wo man sich ja offensichtlich nicht befindet).[52]

Die heute wichtigsten Anbieter von Sozialen Netzwerken und ähnlichen Diensten stammen mehrheitlich aus dem amerikanischen Umfeld, wo allgemein gültige Datenschutzregeln meist fehlen. In der Regel werden die in europäischen Staaten generell strengeren Datenschutzauflagen ignoriert, zum Nachteil der Rechte der Bürgerinnen und Bürger und der Wettbewerbsfähigkeit hier ansässiger Unternehmen mit vergleichbaren Dienstleistungen. Es bleibt zu hoffen, dass mit zunehmender Sensibilisierung der Kundinnen und Kunden für den Umgang mit Personendaten der Markt zu Gunsten von datenschutzfreundlichen Produkten und Angeboten spielen wird.

5.4 Webdienste - Grundprobleme des Gesetzgebers

Durch die technologischen und gesellschaftlichen Entwicklungen werden laufend neue Möglichkeiten und neue Risiken geschaffen. Wenn in Folge dieser Veränderungen Probleme auftreten, werden häufig neue Gesetze gefordert. Politiker und Private erliegen der Illusion, sie könnten über die Gesetzgebung Street View verbieten, Facebook kontrollieren oder missliebige Inhalte im Internet unzugänglich machen. Auch wenn solche Massnahmen grundsätzlich vorstellbar sind, stellt sich im Zusammenhang mit der Um- und Durchsetzung von neuem Recht die Frage der Verhältnismässigkeit. Durch Überregulierung kann die Wirtschaft gehemmt und legitime Möglichkeiten von Benutzern eingeschränkt werden. Ein mit Strafe bewehrtes Verbot ist nur dann wirksam, wenn es auch durchgesetzt werden kann und wird.

Gesetze sollten technologieneutral und generell-abstrakt formuliert werden. Auch bei Massnahmen eines Regulators muss bedacht werden, dass eine zu enge Formulierung

---

[51] Beispielsweise GPS-basierte Dienste wie Foursquare, Gowalla, Facebook Places oder Google Latitude – aber auch per Twitter-Meldung oder Facebook-Status werden regelmässig Aufenthaltsorte preisgegeben.

[52] http://pleaserobme.com/ (Stand: 27. August 2010)

mögliche zukünftige Entwicklungen nicht erfasst,[53] demgegenüber zu allgemein gehaltene Regeln einen grossen Spielraum ermöglichen und allenfalls zu wenig Rechtssicherheit bieten. Es ist problematisch, wenn man spezifische Angebote oder Dienste besonders behandelt und Gesetze wegen konkreten Anwendungen erlässt: Google Street View ist nicht der einzige Dienst, welcher Bilder von Strassenzügen anbietet und Facebook ist nicht das einzige Soziale Netzwerk. Weder ein Street View Gesetz noch eine Facebook-Regulierung würden alle entsprechenden Dienste abdecken – von der Durchsetzbarkeit ganz zu schweigen.

Das Recht folgt grundsätzlich dem Territorialitätsprinzip. Schweizer Regeln sind nicht zwangsläufig auf Sachverhalte im Internet anwendbar. Sobald zum Beispiel eine ausländische Firma beteiligt ist, muss zuerst abgeklärt werden, ob Schweizer Recht Anwendung findet, eine Schweizer Behörde zuständig ist und wie allfällige Entscheide durchgesetzt werden können. Wenn beispielsweise ein amerikanisches Soziales Netzwerk grobe Datenschutzverletzungen nach Schweizer Recht begehen würde, Amerikanisches Recht dabei aber nicht verletzt, bliebe dem Schweizer Konsument wohl keine Möglichkeit, sich zu wehren.

Die Legislative kann Anbietern von legaler Infrastruktur[54] und erlaubter Dienstleistungen[55] wohl gesetzlich auferlegen, dass sie alle Inhalte kontrollieren und filtern, und jegliche Kunden vor Aufnahme von Geschäftsbeziehungen auf Herz und Nieren prüfen müssen, um Schweizer Konsumenten präventiv zu schützen. Jedoch müsste hierzu ein Zensurapparat wie in einem totalitären Staat aufgebaut und sämtliche Massnahmen über höhere Preise bezahlt werden, nur um festzustellen, dass schliesslich der Wirtschaftsstandort Schweiz enorm an Attraktivität eingebüsst hat und der angestrebte Schutz des entmündigten Konsumenten immer noch mangelhaft ist. Weitaus effizienter wären klare Prozesse, wie einem festgestellten Missbrauch entgegnet werden kann und welche Mittel dafür einzusetzen sind.[56]

In diesem Zusammenhang sei auf den parlamentarischen Vorstoss[57] hingewiesen, welcher darauf abzielt, kommerzielle pornografische Angebote auf Mobiltelefonen (gemäss Motionstitel – im Text wird dann allgemein «Fernmeldeeinrichtungen» verwendet[58]) aus Jugendschutzüberlegungen grundsätzlich zu verbieten. Als Variante wurde in der Motion beantragt, «Anbieter von Diensten der Grundversorgung zu verpflichten, alle Verbindungen zu kommerziellen Mehrwertdiensten mit erotischen oder pornografischen Inhalten für Personen unter 16 Jahren zu sperren sowie Mehrwertdienstleister zu verpflichten, keine erotische oder pornografische Inhalte an Personen unter 16 Jahren zu überlassen.». Dies obwohl nach geltender Rechtslage[59] das Anbieten, Zeigen, Überlassen und Zugänglich-Machen von Pornografie an Personen unter 16 Jahren bereits strafbar ist – unabhängig davon, ob gewinnorientiert oder gratis, ob on- oder offline. Gerade im Spezialfall der

---

[53] So geschehen bei der Verordnung vom 31. Oktober 2001 über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF, SR 780.11: http://www.admin.ch/ch/d/sr/c780_11.html), gemäss welcher nur Access-Provider die E-Mail-Box ihrer Kunden überwachen können müssen – reine E-Mail-Dienstanbieter sind scheinbar nicht erfasst. Dies mag auf dem Umstand gründen, dass zu jener Zeit vornehmlich die Access-Provider E-Mail-Konten angeboten haben und reine E-Mail-Dienstleister in der Schweiz kaum bekannt waren.

[54] Zum Beispiel Access-Provider.

[55] Zum Beispiel Unternehmen, welche SMS-Kurznummern halten und darüber Dienste vermitteln.

[56] Wie die Sperrung von SMS-Kurznummern oder die Blockierung von Domain-Namen, siehe Kapitel 3.5.

[57] http://www.parlament.ch/D/Suche/Seiten/geschaefte.aspx?gesch_id=20063884 (Stand: 27. August 2010)

[58] Diese Formulierung schliesst auch das Internet mit ein. – Es dürfte aber kaum im Sinne des Motionärs sein, im Internet nur noch (aber immerhin) Gratis-Pornografie zu erlauben.

[59] Art. 197 Abs. 1 Strafgesetzbuch (StGB, SR 311.0): http://www.admin.ch/ch/d/sr/311_0/a197.html (Stand: 27. August 2010)

Pornografie dürfte hier ein Unternehmen ab dem Moment strafbar sein, ab welchem es vom Sachverhalt Kenntnis erhält und den Zugang nicht unterbindet. Bei anderen Tatbeständen bleiben Vermittlerunternehmen aber unter Umständen straflos. Man müsste also die Frage klären, ab welchem Zeitpunkt und was für eine Art von Verantwortung einem reinen Vermittlerunternehmen[60] zugesprochen werden soll, welchem typischerweise primär keine Kenntnis des ver- und übermittelten Inhaltes unterstellt werden kann.

Auch die Vorratsdatenspeicherung, welche in letzter Zeit in Deutschland heftig diskutiert wird, ist ein interessantes Anschauungsbeispiel für Probleme der Legislative: Aus Bürgerrechtskreisen wird Datenschutz und Generalverdacht ins Feld geführt, während Polizei und Opferverbände gegen Anonymität ein Mittel fordern und Datenschutz häufig als Täterschutz sehen. Auch hier gilt es, einen gesunden Ausgleich zwischen den verschiedenen Interessen zu schaffen und eine praktikable Lösung zu finden. Während auch gemäss der vom Bundesverfassungsgericht beanstandeten Regelung[61] das Aufzeichnen der von einem Nutzer besuchten Webseiten nicht erlaubt war, können ebendiese Daten gerade bei mobilen Internetnutzern (wo sich mehrere Personen dieselbe Adresse teilen)[62] für eine Identifizierung entscheidend sein, da mit der herkömmlichen Methode (IP-Adresse und Zeit) eben nicht eindeutig bestimmt werden kann, welcher Teilnehmer in einem bestimmten Chatraum sein Unwesen trieb.

Gerade im Umfeld der Informations- und Kommunikationsinfrastrukturen, ist eine Einschränkung des Täterkreises oder aber eine klare Bestimmung des Aufenthaltsortes der Täterschaft äusserst schwierig. Das Internet als Tatmittel zum Zweck ist inhärent global und selbst eine Unterscheidung zwischen staatlichen oder privaten Akteuren gestaltet sich teilweise unmöglich. Daher gehen in der Frage der Gesetzgebung oftmals auch die Versuche in Richtung Kontrolle oder Bestrafung von so genannten Vorbereitungshandlungen. Allerdings scheitert gerade im Bereich der IKT ein solcher Ansatz an der Tatsache, dass die eingesetzten Mittel praktisch immer Dual-Use-Mittel sind, also entweder zum Schutz oder aber zur Schädigung eingesetzt werden können. Unter dem Gesichtspunkt der Verhältnismässigkeit führen solche Ansätze unter Umständen zur Behinderung der legitimen und innovativen Nutzung neuer Technologien. Am Ende ist die Nutzung der verfügbaren Technologien überall dieselbe und nur die Absicht entscheidet über Missbrauch oder nicht. Diesem Umstand versucht das Projekt zur Ratifizierung der Cybercrime Convention gerecht zu werden.[63]

[60] Internet Access-Provider, Telekom-Unternehmen, Halterin und Vermieterin von SMS-Mehrwertnummern, Betreiberin eines Online-Bezahlsystems, etc.

[61] Siehe Kapitel 4.8

[62] Siehe Kapitel 3.10

[63] Siehe Kapitel 3.6

6 Glossar

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

Active Scripting	Eine von Microsoft entwickelte Technologie, mit welcher es möglich ist, kleine Programme – so genannte ActiveX Controls – beim Anzeigen von Webseiten auf den Rechner des Besuchers zu laden, von wo sie ausgeführt werden. Sie ermöglichen es, unterschiedliche Effekte oder Funktionen umzusetzen. Leider wird diese Technologie häufig missbraucht und stellt ein Sicherheitsrisiko dar. Beispielsweise werden viele Dialer über ActiveX auf den Rechner geladen und ausgeführt. Die ActiveX-Problematik betrifft nur den Internet Explorer, da die anderen Browser diese Technologie nicht unterstützen.
Ad-Server	Ad-Server werden zur Erfolgsmessung von Internetwerbung eingesetzt. Sowohl der physische Server selbst, auf dem eine Adserver-Software läuft, als auch diese Software können als Adserver bezeichnet werden.
Botnetzwerk	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.
Command & Control Server	Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet.
Content Management System (CMS)	Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Cross-Site-Scripting	Cross-Site Scripting (XSS) bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt

	werden, in dem sie als vertrauenswürdig eingestuft werden.
DDoS	Distributed-Denial-of-Service Attacke. Eine DoS Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
DNS	Domain Name System. Mit Hilfe von DNS lassen sich das Internet und dessen Dienste benutzerfreundlich anwenden, da die Benutzer anstelle von den aus Zahlen bestehenden IP-Adressen verständliche Namen verwenden können (z.B. www.melani.admin.ch).
Dual Use	Dual Use ist ein dem Englischen entlehnter Begriff, der überwiegend in der Exportkontrolle angewendet wird und die prinzipielle Verwendbarkeit eines Wirtschaftsgutes kennzeichnet.
eBook-Reader	Ein E-Book-Reader ist ein tragbares Gerät, mit dem man elektronisch gespeicherte Bücher (E-Books) lesen kann.
Elektronische Signatur	Unter einer elektronischen 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.
EMV-Chip	Die Abkürzung EMV bezeichnet eine Spezifikation für Zahlungskarten, die mit einem Prozessorchip ausgestattet sind. Die Buchstaben EMV stehen für die drei Gesellschaften, die den Standard entwickelten: Europay International (heute MasterCard Europe), MasterCard und VISA
Fast Flux	Fast Flux ist eine DNS-Technik, welche von Botnetzwerken verwendet wird um Phishingseiten oder Seiten, die Malware verbreiten, auf diversen Hosts zu verteilen und so zu verstecken. Fällt ein Computer aus, springt der nächste Computer in die Bresche.
Finanzagent	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.
FTP	File Transfer Protocol FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Web-Seiten auf einen Webserver zu laden.
Full Disclosure	Vollständiges Veröffentlichen von Details zu einer Sicherheitslücke.
Geschützter Modus	Der geschützte Modus beispielsweise im Internet Explorer ist ein Feature, mit dem es bösartiger Software erschwert wird, sich auf dem Computer zu installieren.

GPS	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
Host	Wurde und wird in der IKT vor allem für Rechner mit sehr grosser Rechenleistung verwendet (Bankenumfeld). Heute bezeichnet man damit aber auch kleinere Computersysteme (Computer von Privatanwendern, Webserver usw.).
HTML-Code	HyperText Markup Language In HTML werden die Webseiten erstellt. Damit lassen sich die Eigenschaften der Webseiten (z.B. der Seitenaufbau, das Layout, die Links auf andere Seiten, usw.) vorgeben. Da HTML aus ASCII-Zeichen besteht, kann eine HTML-Seite mit einem gewöhnlichen Textverarbeitungsprogramm bearbeitet werden.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
ISM-Band	Als ISM-Bänder (Industrial, Scientific and Medical Band) werden Frequenzbereiche bezeichnet, die durch Hochfrequenz-Geräte in Industrie, Wissenschaft, Medizin, in häuslichen und ähnlichen Bereichen genutzt werden können. Entsprechende ISM-Geräte wie Mikrowellenherde und medizinische Geräte zur Kurzwellenbestrahlung benötigen dabei nur eine allgemeine Zulassung.
Kritische Infrastruktur	Infrastruktur oder Teil der Wirtschaft, deren Ausfall oder Beschädigung massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt einer Nation hat. In der Schweiz sind folgende Infrastrukturen als kritisch definiert worden: Energie- und Wasserversorgung, Notfall- und Rettungswesen, Telekommunikation, Transport und Verkehr, Banken und Versicherungen, Regierung und öffentliche Verwaltungen. Im Informationszeitalter hängt ihr Funktionieren zunehmend von Informations- und Kommunikationssystemen ab. Solche Systeme nennt man kritische Informationsinfrastrukturen.
Mac-Adresse	Media Access Control. Hardware-Adresse eines Netzwerkadapters zu dessen weltweiten und eindeutigen Identifizierung. Die MAC-Adresse wird vom jeweiligen Hersteller in das ROM des Adapters geschrieben (Beispiel: 00:0d:93:ff:fe:a1:96:72).
Man-in-the-middle-/ Man-in-the-Browser Angriff	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.
Name-Server	Ein Nameserver ist ein Server, der Namensauflösung anbietet. Namensauflösung ist das Verfahren, das es ermöglicht Namen von Rechnern bzw. Diensten in eine vom Computer bearbeitbare Adresse aufzulösen siehe auch Domain Name System (DNS)

Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt. Siehe auch Hotfix.
Pdf-Datei	Das Portable Document Format (PDF) ist ein plattformunabhängiges Dateiformat für Dokumente, das vom Unternehmen Adobe Systems entwickelt und 1993 veröffentlicht wurde.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z.B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
PIN-Code	Eine Persönliche Identifikationsnummer (PIN) oder Geheimzahl ist eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber einer Maschine authentisieren können.
Port	Ein Port ist ein Teil einer Adresse, der Datensegmente einem Netzwerkprotokoll zuordnet. Dieses Konzept ist beispielsweise in TCP, UDP und SCTP vorgesehen, um Protokolle auf den höheren Schichten des OSI-Modells zu adressieren.
Quellcode	Der Begriff Quelltext, auch Quellcode (engl. source code) genannt, bezeichnet in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes.
Reasonable Disclosure	Vernünftiges Veröffentlichen von Details einer Sicherheitslücke. Im Idealfall so, dass es dem Nutzer hilft, Sicherheitsmassnahmen zu ergreifen, aber dem Kriminellen nicht gelingt die Lücke auszunutzen.
Sicherheitslücke	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Sinkhole	Methode, um Botnetze zu einem bestimmten Command & Control Server umzuleiten auf den Zugriff besteht, um möglichst viele Informationen über die infizierten Systeme zu erhalten.
Smartphone	Ein Smartphone ist ein leistungsfähiges Mobiltelefon, das den Funktionsumfang eines Mobiltelefons um den eines Personal Digital Assistants (PDA) erweitert.
Social Engineering	Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.

Soziale Netzwerke	Webseiten, auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen. Oft werden persönliche Daten wie Namen, Geburtstage, Bilder, Berufliche Interessen sowie Freizeitaktivitäten bekanntgegeben.
SSID	Service Set Identifier Identifiziert den Netzwerknamen des WLAN. Sämtliche Access Points und Endgeräte des WLAN müssen den selben SSID verwenden, um miteinander kommunizieren zu können.
Subdomain	Als Subdomain bezeichnet man eine Domain, welche in der Hierarchie unterhalb einer anderen liegt.
Token	Hardware-Komponente, die einen Authentifikationsfaktor (siehe Zwei-Faktor-Authentifizierung) ausgibt (z.B. SmartCard, USB-Token, SecureID etc.).
Verknüpfungssymbole	Verknüpfungssymbole sind kleine Grafiken, welche beim Anklicken das gewünschte Programm öffnen.
Virus	Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt.
Vorratsdatenspeicherung	Speicherung von Angaben über einen bestimmten Zeitraum, welche erforderlich sind, um zu rekonstruieren, wer, wann, wie lange, mit wem, von wo aus kommuniziert hat oder zu kommunizieren versucht hat.
Webseiteninfektion	Infektion eines Computers mit Malware allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken.
Wireless (WLAN)	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Workaround	Unter einem Workaround versteht man die Umgehung eines bekannten Problems innerhalb eines technischen Systems durch eine Hilfskonstruktion. Es ist eine provisorische Lösung, die die eigentliche Fehlerursache nicht behebt.
Digitales Zertifikat	Ein Digitales Zertifikat sind strukturierte Daten, die den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels bestätigen.