Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

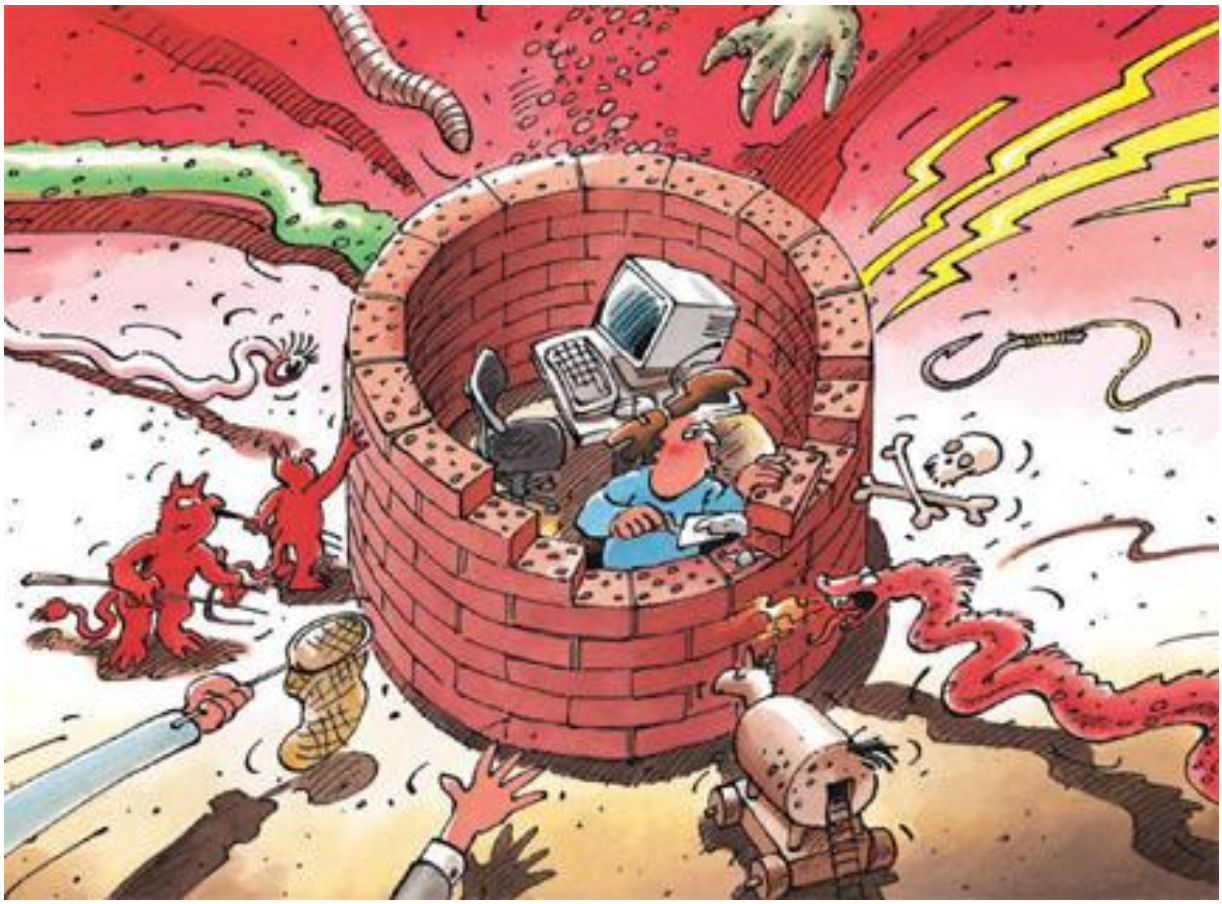
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2012/II (Juli – Dezember)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2012/II

- **Phishing auf dem Vormarsch**
  Klassisches Phishing, also das Versenden von E-Mails, welche das Opfer in irgendeiner Weise verführen wollen, persönliche Daten anzugeben, ist auf dem Vormarsch. Die Angreifer haben es dabei vor allem auf Kreditkartendaten abgesehen. Allerdings gesellte sich zu den eher einfach gestrickten zahlreichen Kreditkarten-Phishings ein neuer Modus Operandi, der im zweiten Halbjahr 2013 auch gegen Schweizer E-Banking Kunden gerichtet war.
  ► Aktuelle Lage Schweiz: Kapitel 3.1

- **DDoS – massive Angriffe gegen diverse US-Banken**
  Angriffe auf die Verfügbarkeit von Webseiten, so genannte Distributed Denial of Service (DDoS), zählen mittlerweile zu den Hauptgefahren von Netzwerken. Seit September 2012 werden zum Teil massive DDoS-Angriffe gegen diverse US-Banken gemeldet. Auch andere Angriffe auf die Verfügbarkeit sorgten für Schlagzeilen.
  ► Aktuelle Lage Schweiz: Kapitel 3.6
  ► Aktuelle Lage International: Kapitel 4.2

- **Cyberkonflikt in Nahost - Update**
  Im Rahmen der Untersuchungen zur Schadsoftware «Flame» entdeckte die russische Antiviren-Software-Herstellerin Kaspersky Lab eine weitere Schadsoftware, welche «Gauss» getauft wurde. Es handelt sich bei Gauss um den ersten bekannten Fall, in dem eine ausgeklügelte, mutmasslich staatliche Spionagesoftware typische Charakteristiken eines Onlinebanking-Trojaners aufweist. Die Mehrheit der infizierten Geräte stand im Libanon, gefolgt von Israel und den Palästinensergebieten.

  Die Bürocomputer der saudischen staatlichen Ölgesellschaft Saudi Aramco waren auf Grund von Infektionen mit einer Schadsoftware lahmgelegt. Kurz darauf musste auch der katarische Gasproduzent RasGas sein Büronetzwerk von der Aussenwelt trennen. Obwohl keine offizielle Bestätigung vorliegt, gehen verschiedene Experten davon aus, dass RasGas von der gleichen Schadsoftware heimgesucht wurde. Westliche Experten spekulierten denn auch, dass dahinter Bemühungen des Iran stehen könnten, dessen Energieexport durch die internationalen Sanktionen stark unter Druck geraten ist, um eine Erhöhung der Öl- und Gasproduktion der arabischen Staaten zu verhindern.

  ► Aktuelle Lage International: Kapitel 4.1, Kapitel 4.2

- **Abhängigkeit von der IKT im täglichen Leben – immer und überall**

  Schon seit einigen Jahren sind nicht mehr bloss Computer oder Server die Zielscheibe von Cyberangriffen. Jedes Informatiksystem kann ins Visier von Hackern geraten. Eine elektronisch gesicherte Hoteltüre zu knacken, ist nur eines von vielen Beispielen, Die Abhängigkeit der heutigen Gesellschaft von der IKT ist sehr facettenreich.
  ► Aktuelle Lage Schweiz: Kapitel 3.4
  ► Aktuelle Lage International: Kapitel 4.3, Kapitel 4.6

- **Regulierung versus Freiheit – Wie macht man das Internet sicher?**
  Bis zum heutigen Zeitpunkt wird das Internet nicht staatlich reguliert und lässt sich als freier Raum weitgehend über technische Standards und Verwaltungsrichtlinien (so genannte Policies) regeln. Es gibt auf der anderen Seite eine starke Koalition von Ländern, die sich für eine Internetregulierung einsetzen, um ihre staatliche Kontrollmacht auf den Cyber-Raum auszudehnen, und die ihre Souveränität stärken wollen.
  ► Aktuelle Lage International: Kapitel 4.9
  ► Tendenzen Ausblick: Kapitel 5.3

2 Einleitung

Der sechzehnte Halbjahresbericht (Juli – Dezember 2012) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

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

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 2012 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

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

3 Aktuelle Lage IKT-Infrastruktur national

3.1 Phishing - aktuelle Trends

Klassisches *Phishing*, also des Versenden von E-Mails, welche das Opfer in irgendeiner Weise verführen wollen, persönliche Daten anzugeben, ist auf dem Vormarsch. Die Angreifer haben es dabei meist auf Kreditkartendaten abgesehen. Allerdings gesellten sich zu den eher einfach gestrickten zahlreichen Kreditkarten-Phishings auch so genannte *Voice-Phishing* Angriffe, die im zweiten Halbjahr 2013 auch gegen Schweizer E-Banking Kunden gerichtet waren. Solche Angriffe benötigen im Gegensatz zu E-Banking *Schadsoftware* nur eine geringe technische Infrastruktur und können auch von technisch nicht versierten Personen durchgeführt werden. So genügt in den meisten Fällen ein Computer und/oder ein Telefon.

3.1.1 Kombinierte Phishing-Voice-Phishing Angriffe

Seit Herbst 2012 wird im Bereich Phishing ein neuer Modus Operandi beobachtet. Dabei werden Phishing E-Mails versendet, welche vorgeben, dass das Finanzinstitut zum Schutz des E-Banking Kontos ein neues Sicherheitssystem installiert hat. Ein Bankmitarbeiter werde sich mit dem Opfer telefonisch in Verbindung setzen, um den Prozess zu diskutieren und zu vervollständigen. Zu diesem Zweck wird das Opfer gebeten, neben persönlichen Daten auch seine Telefonnummer anzugeben.

Anschliessend werden die Opfer – und das ist neu in der Schweiz - von den Betrügern angerufen und unter dem Vorwand, die Sicherheit zu verbessern, dazu bewegt, das Passwort und das zweite Sicherheitselement anzugeben. Dabei wird das Opfer beispielsweise aufgefordert, einen Code in den Kartenleser einzugeben und dem Angreifer das Ergebnis mitzuteilen. Mit diesen Angaben kann sich der Betrüger in das E-Banking Konto einloggen und eine Zahlung auslösen. Wird für das Auslösen der Zahlung die sogenannte *Transaktionssignierung* verlangt, wird der Prozess wiederholt und auch diese in der gleichen Art und Weise vom Betrüger erfragt. Der Telefonanruf wird jeweils professionell durchgeführt und erfolgt oftmals auch in Schweizerdeutsch.

3.1.2 Phishingseiten auch mit https

Man hat lange damit gerechnet, dass die Angreifer auch Phishing-Seiten verwenden werden, die eine Verschlüsselung (https-Seiten) aufweisen. Im Herbst des Berichtsjahres wurde nun bei verschiedenen Phishing-Wellen schliesslich auf verschlüsselte Seiten verlinkt. URLs, die mit https:// *(hyper text transfer protocol secure)* beginnen, deuten darauf hin, dass die auf der entsprechenden Website eingegebenen Informationen verschlüsselt übermittelt werden.

Allerdings wurde nicht ein spezielles *Zertifikat* benutzt, sondern einfach das *Zertifikat* einer gehackten Webseite mitverwendet. Von einem eigentlichen Trend kann allerdings nicht gesprochen werden, zumal es bei einzelnen Fällen geblieben ist.

Abbildung 1: Phishingseite mit Verschlüsselung

3.1.3 Phishing E-Mails zunehmend auch ohne Phishing-Seite

Wie im letzten MELANI-Halbjahresbericht[1] bereits berichtet, versuchen Phishing-Betrüger auch ohne klassische, auf einem Webserver gespeicherte, Phishingseite an die Daten des Opfers zu gelangen. Dabei haben sich zwei Methoden etabliert: Die Erste beinhaltet das Anhängen einer Phishingseite als HTML-Formular an die E-Mail. Beim Öffnen wird die HTML-Seite lokal auf dem Computer des Empfängers aufgebaut. Werden die Formularfelder ausgefüllt und auf den Knopf «Weiter» gedrückt, werden die Daten «direkt» an den Angreifer versendet.

Die zweite Methode ist noch einfacher. Hier wird das Formular einfach in die E-Mail integriert. Es ist ausser einer für den Betrug gelösten E-Mail-Adresse nichts mehr notwendig. Die Angreifer machen sich zudem den Umstand zu Nutze, dass bei jeder E-Mail eine spezielle Rückantwortadresse definiert werden kann, die von der sichtbaren Absenderadresse abweicht. So kann als sichtbare Absenderadresse die offizielle Adresse eines Finanzinstitutes verwendet werden und erst wenn dann der «Antwort-Knopf» gedrückt wird, sieht man wohin die E-Mail wirklich gesendet wird.

[1] MELANI Halbjahresbericht 2012/1, Kapitel 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

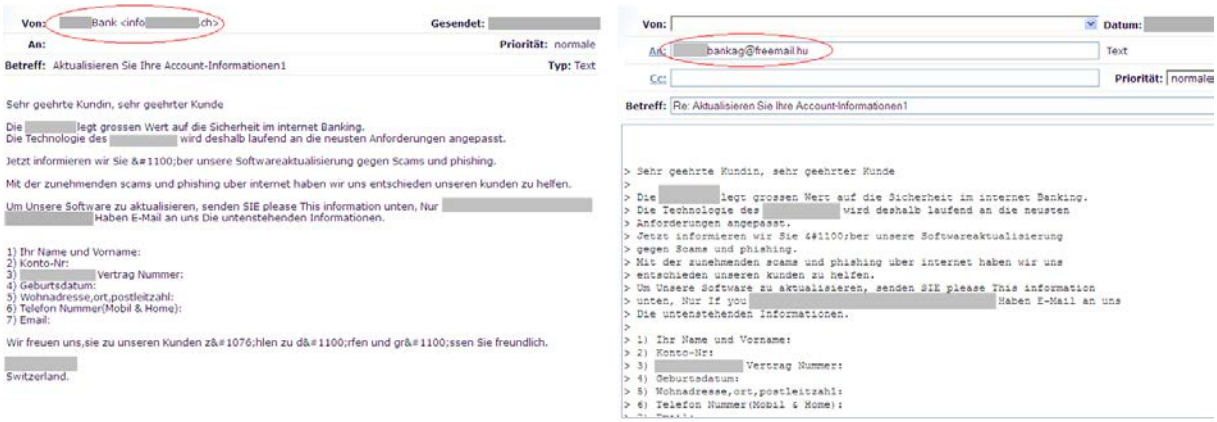


Abbildung 2: Phishing E-Mail mit präparierter Rückantwort-Adresse. Die E-Mail scheint von der info-Adresse einer Schweizer Bank zu kommen, die Antwort wird dann aber an eine Adresse bei einem Gratis-E-Maildienst in Ungarn gesendet.

Für den Angreifer haben beide Methoden den Vorteil, dass er keinen gehackten oder speziell für diese Zwecke aufgesetzten Webserver benötigt, worauf er normalerweise die Phishing-seite platziert. Diese konnten nämlich bei Bekanntwerden durch die Sicherheitsbehörden, respektive den Hosting-Provider, in relativ kurzer Zeit deaktiviert werden.

3.1.4 Erste Schweizer Domäne durch MELANI bei Switch gelöscht

Um den 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; in Kraft per 1. Januar 2010) ein neuer Artikel eingeführt. Gemäss diesem muss die «.ch»-Registerbetreiberin (SWITCH) *Domain*-Namen blockieren und die entsprechende Zuweisung zu einem Namenserver aufheben, wenn eine in der Bekämpfung der Cyberkriminalität vom Bundesamt für Kommunikation (BAKOM) anerkannte Stelle die Blockierung beantragt hat oder der begründete Verdacht besteht, dass dieser Domain-Name nicht rechtmässig benutzt wird. Dies entweder um mit unrechtmässigen Methoden an schützenswerte Daten zu gelangen (so genanntes *Phishing*) oder um über diese Domain schädliche Software (so genannte *Malware*) zu verbreiten. SWITCH kann diese Massnahme zur Gefahrenabwehr selbständig ergreifen und während 5 Tagen aufrecht erhalten. Von dieser Möglichkeit hat SWITCH bereits vielfach Gebrauch gemacht, insbesondere um Besucher von gehackten Webseiten zu schützen. Die Melde- und Analysestelle Informationssicherung (MELANI) musste nun zum ersten Mal selbst von dieser Kompetenz Gebrauch machen.

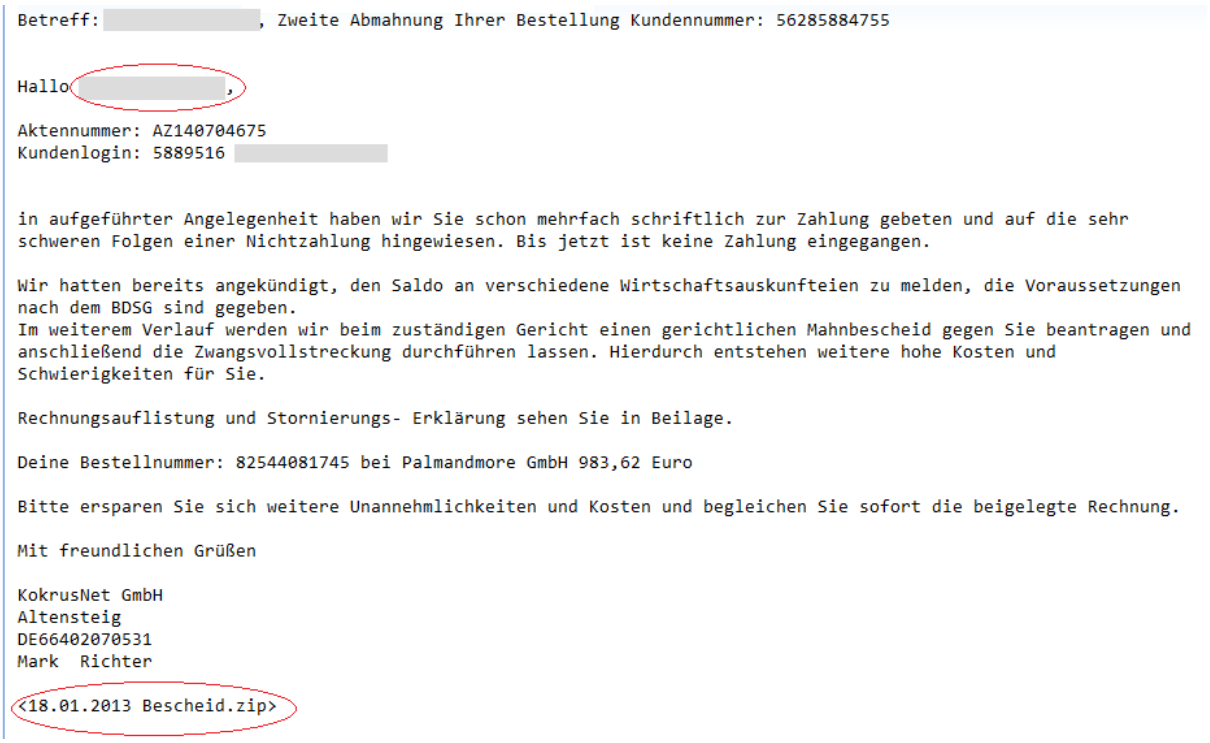
Im Dezember 2012 wurde MELANI eine Phishing-Seite mit einer Schweizer Internet-Adresse gemeldet. Der Domainname wurde ausschliesslich für den Phishing-Angriff gelöst und es handelte sich nicht – wie in vielen anderen Fällen – um eine gehackte Webseite, auf welcher die Betrüger normalerweise die Phishing-Seite in einem Unterverzeichnis platzieren. MELANI hat sich daraufhin entschlossen, die von SWITCH bereits verhängte Sperre von 5 Tagen um weitere 30 Tage zu verlängern und gleichzeitig durch SWITCH eine Halterverifikation durchzuführen zu lassen. Da diese nicht beantwortet wurde, konnte die Domäne endgültig gelöscht werden.

3.2 Falsche Rechnungen mit Schadsoftware

Seit einigen Monaten sind vermehrt E-Mails mit gefälschtem Absender im Umlauf, welche jeweils Bezug auf eine (erfundene) Bestellung, Lieferung oder Rechnung nehmen. Bei ME-

LANI treffen jede Woche mehrere solcher Meldungen ein. Die Absender versuchen dabei mit der Ankündigung von Mahnungen, den daraus folgenden Kosten und möglichen Gerichtsverfahren eine Drohkulisse aufzubauen und so die Empfänger zu verleiten, den Anhang zu öffnen, um weitere Informationen zu erhalten. Im Anhang befindet sich in diesen Fällen allerdings eine Schadsoftware, welche sich meist in einer zip-Datei befindet.

In den bei MELANI bekannten Fällen wurden diese Mails personalisiert verschickt, d.h. die Anrede enthielt den Vor- und Nachnamen des Empfängers. Die persönliche Adressierung von Betrugsmails scheint sich allmählich zu etablieren, weil dadurch ein vertrauenswürdigerer Eindruck erzeugt werden kann.



Betreff: , Zweite Abmahnung Ihrer Bestellung Kundennummer: 56285884755

Hallo ,

Aktennummer: AZ140704675
Kundenlogin: 5889516

in aufgeführter Angelegenheit haben wir Sie schon mehrfach schriftlich zur Zahlung gebeten und auf die sehr schweren Folgen einer Nichtzahlung hingewiesen. Bis jetzt ist keine Zahlung eingegangen.

Wir hatten bereits angekündigt, den Saldo an verschiedene Wirtschaftsauskunfteien zu melden, die Voraussetzungen nach dem BDSG sind gegeben.
Im weiterem Verlauf werden wir beim zuständigen Gericht einen gerichtlichen Mahnbescheid gegen Sie beantragen und anschließend die Zwangsvollstreckung durchführen lassen. Hierdurch entstehen weitere hohe Kosten und Schwierigkeiten für Sie.

Rechnungsauflistung und Stornierungs- Erklärung sehen Sie in Beilage.

Deine Bestellnummer: 82544081745 bei Palmandmore GmbH 983,62 Euro

Bitte ersparen Sie sich weitere Unannehmlichkeiten und Kosten und begleichen Sie sofort die beigelegte Rechnung.

Mit freundlichen Grüßen

KokrusNet GmbH
Altensteig
DE66402070531
Mark Richter

<18.01.2013 Bescheid.zip>

Abbildung 3: Beispiel einer falschen Rechnung mit persönlicher Anrede und Schadsoftware (Bescheid.zip) im Anhang.

3.3 Steueranlagen offen im Netz – auch in der Schweiz

Die Sicherheit von industriellen Steueranlagen wird nicht nur von Sicherheitsexperten, sondern auch von den Medien vermehrt thematisiert.[2] Dabei nehmen laut dem amerikanischen Industrial Control System *CERT* (ICS-CERT), welches Ende Oktober eine entsprechende Warnung[3] herausgegeben hat, Angriffe auf solche Systeme zu. Hintergrund der Warnung ist, dass immer mehr Werkzeuge angeboten werden, die es Angreifern ermöglichen, solche Systeme aufzuspüren und in diese Systeme einzudringen. Spezielle Kenntnisse sind dabei nicht notwendig. Das bekannteste Werkzeug ist hier sicherlich die Suchmaschine «SHODAN», welche bereits seit einigen Jahren existiert, das Internet nach *SCADA* Systemen durchsucht

[2] http://www.br.de/fernsehen/das-erste/sendungen/report-muenchen/report-februar-102.html (Stand: 28. Februar 2013).

[3] http://ics-cert.us-cert.gov/index.html (Stand: 28. Februar 2013).

und schon in einem früheren Halbjahresbericht thematisiert worden ist[4] Mittels dieser Suchmaschine war es dem ICS-CERT möglich, über 500‘000 Systeme aufzufinden. Neben SHODAN existiert beispielsweise auch das Every Routable IP Project (ERIPP).

Demgegenüber steht eine Vielzahl von Betreibern von industriellen Steueranlagen, die den Fokus bislang primär auf die funktionelle Stabilität und weniger auf die Sicherheit vor Manipulation gelegt haben. Das mag auch daran liegen, dass viele gar keine Kenntnis darüber haben, ob die Systeme auch wirklich am Internet angeschlossen sind. Zudem programmieren viele Hersteller festcodierte Universalpasswörter in die Applikation, damit der Hersteller auch bei einem Verlust der Zugangsdaten auf die Systeme zugreifen kann. Diese Notfallpasswörter haben den Vorteil, dass die Geräte auch bei einem Passwortverlust stabil weiterbetrieben werden können, haben aber natürlich auch einen gewissen Angriffsvektor. Ein weiterer Fall wurde im August 2012 durch den Sicherheitsforscher Justin W. Clarke publik. Clarke hatte im proprietären Betriebssystem Rugged OS, welches in Kraftwerken oder bei der Verkehrsüberwachung eingesetzt wird, einen fest-kodierten geheimen *RSA-Schlüssel* gefunden. Ist dieser Schlüssel bekannt, lässt sich der verschlüsselte Netzwerkverkehr entschlüsseln und abhören. Das ICS-CERT hat dazu anschliessend eine entsprechende Warnung herausgegeben.[5]

Eine andere Problematik ortete Phil Kernick, ein australischer Sicherheitsexperte. Praktisch bei allen *SCADA* Vorfällen, welche er untersucht hatte, war Schadsoftware im Spiel. Dabei war allerdings die Schadsoftware nicht speziell gegen SCADA Systeme gerichtet. Es handelte sich dabei beispielsweise um konventionelle E-Banking *Malware*. Diese Infektionen hatten zur Folge, dass die Systeme nicht mehr stabil liefen und von Zeit zu Zeit abstürzten. Dies kann bei SCADA Systemen gravierende Folgen haben. Ursache ist meist, dass Kontrollnetzwerke und Office-Netzwerke nicht strikt getrennt sind. Auch die Möglichkeit des Anschlusses von USB-Speichergeräten oder fremden Mobilcomputer (z.B. durch Mitarbeitende oder externe Vertragspartner) ist oft problematisch, weil die notwendigen Benutzer-Policies und/oder technische Hürden weitgehend fehlen.

Grundsätzlich sollten nur Maschinen ans Internet angeschlossen werden, wenn dies für den Betrieb absolut notwendig ist. Diese Systeme müssen natürlich ausreichend mit Firewall und starken Passwörtern geschützt werden. Um die Übertragung von Schadsoftware von Bürocomputern auf SCADA-Systeme zu verhindern, sollten diese beiden Netzwerke getrennt sein.

Nachdem MELANI im Halbjahresbericht 2011/2 bereits berichtete, wie mit der Suchmaschine SHODAN 34 anfällige Systeme in der Schweiz gefunden werden konnten, wurden auch im aktuellen Berichtsjahr solche Systeme identifiziert. Diese waren entweder gar nicht oder nur mit einem Standardpasswort geschützt, welches bei Inbetriebnahme hätte geändert werden müssen. Diese potenziellen Ziele sind zwar in der Regel nicht als heikel einzustufen, aber die Tatsache, dass bei der Installation eines Steuerungssystems mit Internetverbindung das Default-Passwort nicht geändert wird, bildet einen gravierenden Verstoss gegen die grundlegenden Informatiksicherheitsprinzipien. Die Möglichkeit, z.B. auf das Heizungs- oder Klimaanlagen-Netz eines fremden Betriebs zuzugreifen und es zu manipulieren, könnte unter bestimmten Umständen schwerwiegende Probleme verursachen.

---

[4] MELANI Halbjahresbericht 2011/2, Kapitel 3.9: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 28. Februar 2013).

[5] http://ics-cert.us-cert.gov/pdf/ICS-ALERT-12-234-01.pdf (Stand: 28. Februar 2013).

Weiter eröffnen die teilweise Einbindung und Zugriffsmöglichkeiten auf andere betriebsinterne Verwaltungsapplikationen wie Abrechnungssoftware und dergleichen zusätzliches Missbrauchspotential. Grundsätzlich sollten industrielle Kontrollsysteme nicht mit dem Internet verbunden werden. Falls dies unbedingt erforderlich ist, ist bei der Vorgehensweise besondere Vorsicht geboten.

3.4 Panne bei Verkehrsampeln im Waadtland

Aufgrund einer Informatikpanne des Verkehrsleitsystems des Kantons Waadt kam es am 16. Juli 2012 zu Verkehrsbehinderungen und einem kilometerlangen Stau auf dem Autobahnabschnitt zwischen Lausanne und Chexbres. Um 16 Uhr hatte die Verkehrsüberwachung der Waadtländer Polizei technische Probleme festgestellt. Kurz darauf reagierte das System nicht mehr, und die Signalisation verharrte im aktuellen Zustand. So blieb im Tunnel von Flonzaley die linke Fahrspur gesperrt und konnte nicht mehr freigegeben werden, was zu einem 15 Kilometer langen Stau führte. Nachdem ein Techniker manuell eingegriffen hatte, normalisierte sich die Verkehrssituation zwischen Lausanne und Chexbres ab 19:30 Uhr langsam wieder. Die Informatikpanne konnte aber erst in der Nacht um 01:40 Uhr behoben werden.

Zusätzlich war auch die Übertragung der Alarme aus den Tunnels der Waadtländer Autobahnen unterbrochen. Im Falle eines Brandes oder eines Unfalls hätten das Alarmsystem im Tunnel nicht funktioniert. Die Überwachungskameras lieferten zwar weiterhin Bilder, konnten aber nicht bewegt werden. Aus diesem Grund wurden an wichtigen Punkten Polizeikräfte postiert.[6]

Obschon es sich bei diesem Vorfall um eine Panne und nicht um einen Angriff gehandelt hat, zeigt das Beispiel deutlich, wie facettenreich die Abhängigkeit der heutigen Gesellschaft von der IKT ist. Auch bei der Signalisation im Strassenverkehr werden immer mehr IKT-Systeme eingesetzt, um das steigende Verkehrsaufkommen bei gleichbleibender Infrastruktur bewältigen zu können. Solche Systeme sind darauf ausgelegt, dass sie bei einer Fehlfunktion abschalten oder alle Signale auf gelbes Blinklicht umschalten. Eine Situation, bei der alle Verkehrsteilnehmer grün haben und es somit zu Unfällen kommen könnte, soll dabei ausgeschlossen sein.

3.5 Panne bei Ricardo

Am 28. Oktober 2012 hatte das Online-Auktionshaus ricardo.ch grosse Informatikprobleme. Ein Fehler in der Datenbank führte dazu, dass über mehrere Stunden rund ein Drittel der Kunden nicht mehr mitbieten konnten. Dies hatte zur Folge, dass Produkte meist deutlich unter ihrem Wert verkauft wurden, da die Auktionen trotz dieser Panne wie geplant zu Ende gingen, aber keine Gebote mehr abgegeben werden konnten. Bei einer Auktion sind bekanntermassen die letzten Minuten die lukrativsten. Ricardo.ch stellte daraufhin klar, dass Angebote, die während dieses Ausfalls zu Ende gingen, «in jedem Falle auch zum erzielten Preis dem Käufer überlassen werden müssen».

[6] http://www.vd.ch/autorites/departements/dse/police-cantonale/medias/communiques-de-presse/articles/disfonctionnement-reseau-informatique-gerant-la-signalisation-routiere-sur-les-autoroutes-vaudois/ (Stand: 28. Februar 2013).

Zwei Wochen später und wahrscheinlich auch nach diversen Kundenprotesten wurde obenstehende Aussage revidiert. Man habe angenommen, dass die betroffenen Angebote automatisch verlängert würden, was aber nicht überall der Fall war. Ricardo.ch kommunizierte nun, dass in diesen Fällen der Verkäufer nicht grundsätzlich an den Vertrag gebunden sei und betroffene Verkäufer sich an den Kundendienst wenden könnten[7]: Ricardo hat sich gegenüber seinen Kunden kulant gezeigt und den Verkäufern zum Teil höhere Summen zurückerstattet.

Wie praktisch jedes Unternehmen schliesst auch ricardo.ch die Haftung für technische Probleme aus. Das Risiko trägt daher in den meisten Fällen der Kunde. So steht auch in den Allgemeinen Geschäftsbedingungen von Ricardo.ch, dass das Unternehmen nur für grobfahrlässig oder vorsätzlich verursachte zeitweilige Nichtverfügbarkeit der Website, Ausfall einzelner oder sämtlicher Website-Funktionen oder Fehlfunktionen der Website haftet. Insbesondere haftet Ricardo.ch bei leichter Fahrlässigkeit nicht für technische Probleme, aufgrund derer Angebote oder Gebote nicht, verspätet oder fehlerhaft angenommen oder verarbeitet werden.[8] Bei einem Vorfall, insbesondere wenn es um Geld geht, steht den Allgemeinen Geschäftsbedingungen aber meist der öffentlichen Druck entgegen. Unternehmen beharren insbesondere wegen des drohenden Reputationsschadens in solchen Fällen häufig nicht auf den Allgemeinen Geschäftsbedingungen und zeigen sich kulant.

3.6 DDoS Angriff auf Inside Paradeplatz

Zwei Mal innerhalb von drei Monaten wurde die Website «Inside Paradeplatz» mit einem sogenannten *Distributed Denial of Service Angriff* (DDoS-Angriff) lahmgelegt. Bereits im Juni hatten es Unbekannte auf die Website abgesehen und sendeten tausende Anfragen pro Sekunde an die Webseite, so dass diese zeitweilig nicht mehr erreichbar war. Das Gleiche wiederholte sich Anfang September, dauerte allerdings wesentlich länger als der erste Angriff, der nach eineinhalb Tagen vorüber war. Zusätzlich wurde anscheinend parallel zum zweiten Angriff die persönliche Website des Betreibers kompromittiert und darauf eine *Drive-by-Infektion* platziert. Laut Betreiber wurde ein entsprechender Warnhinweis eingeblendet, wenn die Site via Google gesucht und angeklickt wurde.[9] Laut Betreiber sollte damit verhindert werden, dass die Informationen über einen anderen Kanal verbreitet werden konnten. Diese Tatsachen deuten auf einen gezielten Angriff hin. Die Urheberschaft herauszufinden, ist in solchen Fällen aber sehr komplex, da die Spuren des Angriffs verschleiert werden.

DDoS-Angriffe zählen mittlerweile zu den Hauptgefahren von Netzwerken. Eine Auswahl von DDoS Angriffen im Ausland finden Sie in Kapitel 4.2. Trotzdem ist obengenannter Angriff auffällig und entspricht eher nicht gängigen DDoS-Attacken. Gerade die Tatsache, dass die private Site des Betreibers ebenfalls angegriffen worden ist, um eine *Webseiteninfektion* zu platzieren, lässt Raum für Spekulationen. Der vom Betreiber angegebene Grund, dass die Angreifer mit der Websiteinfektion verhindern wollten, dass Informationen über einen anderen Kanal verbreitet werden können, ist nur zum Teil plausibel. Dies, weil die private Site für eine simple Verhinderung der Informationsverbreitung ebenfalls einfach mit einem DDoS-Angriff hätte lahmgelegt werden können.

---

7 http://blog.ricardo.ch/2012/11/teilausfall-von-ricardo-ch-am-28-oktober-2012/ (Stand: 28. Februar 2013).

8 http://www.ricardo.ch/ueber-uns/Portals/ch-ueber-uns/Docs/downloads-pdf-de/AGB_DE.pdf (Stand: 28. Februar 2013).

9 http://insideparadeplatz.ch/2012/08/28/inside-paradeplatz-im-visier-von-hackern/ (Stand: 28. Februar 2013).

Eine weitere mögliche Spekulation wäre, dass die Angreifer in diesem Fall gezielt Computer von Personen aus dem Umfeld des Betreibers mit einer Schadsoftware infizieren wollten, um an Informationen zu kommen. Bei Personen aus dem Umfeld des Betreibers ist die Wahrscheinlichkeit besonders gross, dass sie als erstes auf seine private Website gehen, um zu schauen, wieso die offizielle Site nicht mehr funktioniert.

3.7 Ein Geschenk von Apple oder doch ein möglicher Betrug?

Im November 2012 machte ein *SMS* in schlechtem Deutsch die Runde, welche vorgab, der Empfänger habe ein Geschenk von Apple erhalten. Aufgrund der hohen Melderate bei MELANI dürfte dieses SMS in grossem Stil versendet worden sein. Im SMS waren ein Gewinncode und ein Link enthalten. Die Domänennamen waren stets nach dem gleichen Muster aufgebaut und enthielten jeweils die *Top Level Domäne* «.cc»

Abbildung 4: SMS mit angeblicher Gewinnbenachrichtigung

Für den Erhalt des kostenlosen iPhone 5 müsse man auf der angegebenen Webseite den im SMS erhaltenen Code eingeben. Die Analyse ergab, dass irgendeine Zahl eingegeben werden konnte und man in jedem Fall auf eine nachfolgende Seite geleitet wurde. Allein dies lässt das SMS in einem schiefen Licht erscheinen und gibt einen Hinweis darauf, dass die ganze Aktion nur ein Vorwand gewesen ist, um die Empfänger zu irgendetwas zu verleiten.

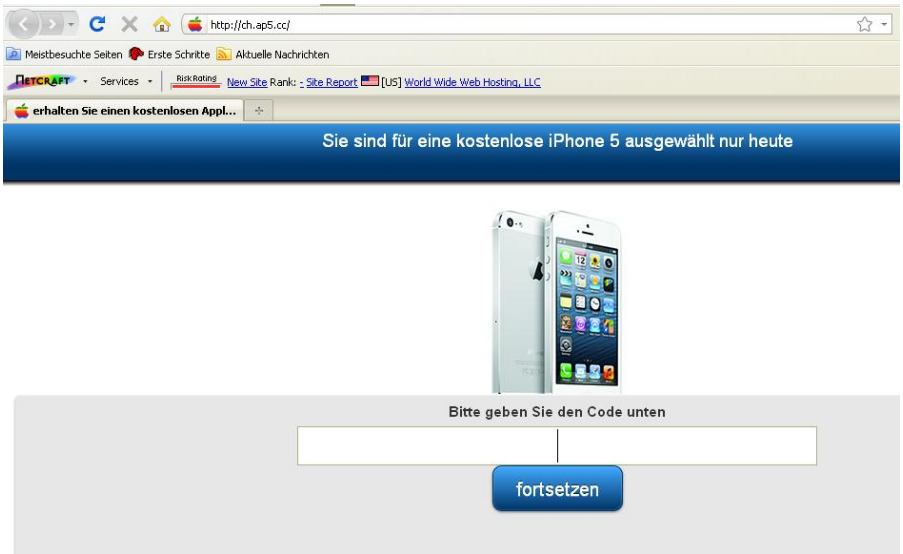


Abbildung 5: Seite auf welcher der angebliche Gewinncode eingegeben werden sollte

Nach der Eingabe des Gewinncodes wurde man auf die Webseite einer Firma mit dem Namen «Ziinga» umgeleitet. Diese Firma bietet so genanntes Entertainment Shopping an und

ist konkret eine Auktionsplattform. Auf dieser Seite wird man nach Name, Vorname und E-Mail Adresse sowie Geschlecht gefragt, und man muss auch die Allgemeinen Geschäftsbedingungen akzeptieren. Das ist für das Opfer durchaus plausibel, da es ja immer noch im Glauben ist, ein iPhone gewonnen zu haben. Mit dem Akzeptieren der AGBs schloss man jedoch eine Platin Mitgliedschaft für 89.99$ pro Monat ab.

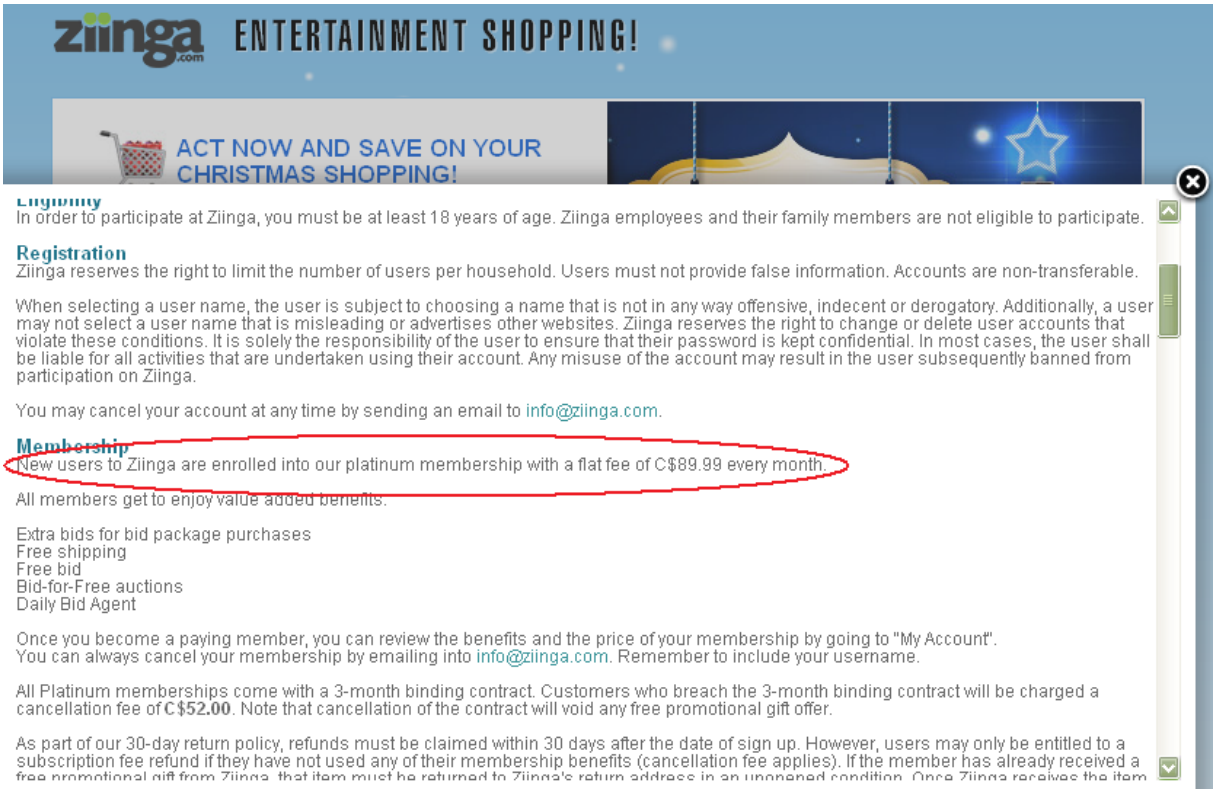


Abbildung 6: Allgemeine Geschäftsbedingungen von Ziinga (Stand: 30. November 2012).

Auf Wikipedia wird Ziinga ebenfalls erwähnt. Der Artikel ist als «Nicht Neutral» eingestuft, liefert aber dennoch einige Hinweise. Die versteckte Publikation der Mitgliedergebühr in den Allgemeinen Geschäftsbedingungen ist schon diverse Male bemängelt worden[10]. Die Mitgliedschaft kann zwar im Nachhinein jederzeit gekündigt werden, allerdings wird dann eine Kündigungsgebühr von £ 28 respektive USD 52 verlangt. In diesem Falle hat sich Ziinga allerdings von den versendeten SMS distanziert und einen Zusammenhang ausgeschlossen. Es bleibt aber die Frage, wer ausser Ziinga ein Interesse daran hatte, solche SMS zu versenden. Wer die SMS tatsächlich versendet hatte, konnte nicht eruiert werden. Schadsoftware wurde auf den angegebenen Seiten nicht gefunden.

Eine anderes Motiv des Versandes könnte auch die Verifikation von gültigen Mobilfunknummern gewesen sein. Jeder versendete Link war nämlich einmalig und beinhaltete einen Code, der auf die entsprechende Mobilfunknummer schliessen liess. Beim Anklicken des Links durch den Empfänger wurde dem Sender somit signalisiert, dass die Mobilfunknummer in Betrieb ist. Wenn die Anfrage zusätzlich noch mit der Eingabe einer E-Mail-Adresse gekoppelt ist, dann ist sogar eine Zuordnung der Mobilfunknummer zur E-Mail-Adresse möglich. Solche Daten könnten dann wiederum gezielt für Phishing Angriffe verwendet oder an interessierte Kreise weiterverkauft werden.

[10] http://en.wikipedia.org/wiki/Ziinga#Controversy (Stand: 28. Februar 2013).

3.8 Phone Phreaking – alte Masche auf dem Vormarsch[11]

Die ersten Praktiken des *Phreakings* gingen schon mit dem Aufkommen automatischer Vermittlungsstellen der Telefongesellschaften einher und erreichten ihren Höhepunkt in den 1970er bis Mitte der 1990er Jahre. Die Erfindung des Phreaking wird dabei einer Person mit Spitznamen «Cap'n Crunch» zugesprochen. Dabei war es das Ziel, Zugang zu Telefonsystemen zu erlangen, um danach beispielsweise gratis telefonieren zu können. Davon betroffen sind beispielsweise Festnetzanschlüsse und in neuerer Zeit auch *VoIP*-Systeme von Privaten sowie Telefonsysteme von Unternehmen jeder Grösse. Gelingt die Attacke, können Telefonsysteme für unterschiedliche Betrugsformen missbraucht werden.

Zugang zu einem Telefonsystem erlangen Kriminelle insbesondere durch die Wartungssoftware. Diese ist häufig lediglich durch eine Standard-*PIN* geschützt. Es gelingt den Tätern aber immer wieder, auch gut gesicherte und gewartete Telefonsysteme zu hacken. Um eine Identität vorzugaukeln und die Rückverfolgung zu erschweren, bedienen sich die Täter beispielsweise des sogenannten *Spoofings*. Mit *Spoofing* lässt sich die eigene Rufnummer verschleiern und eine andere Telefonnummer vortäuschen. Die dafür notwendige Technik und die Standard-PINs können im Internet gefunden werden.

Beim häufigsten Modus Operandi kommen sogenannte Mehrwertnummern zum Einsatz. Mehrwertnummern sind Dienstleistungen, die über die Telefonie hinaus gehen, jedoch über das Telefonabonnement bezahlt werden. Ein Beispiel dafür sind in der Schweiz die 0900-Nummern. Bei dieser Variante verschafft sich der Täter in einem ersten Schritt Zugang zum Telefonsystem eines Unternehmens. Dank der erlangten Kontrolle können Täter danach die Anschlüsse der Telefonanlage mit einer von ihnen eingerichteten Mehrwertnummer verbinden. Damit das Unternehmen den Vorgang nicht zu schnell bemerkt, werden die Angriffe ausserhalb der Arbeitszeiten durchgeführt. Da die Täter für diese Variante eine Vielzahl von Telefonanschlüssen des betroffenen Unternehmens belegen müssen, ist die Wahrscheinlichkeit, dass der Betrug bemerkt wird, während der Arbeitszeit wesentlich höher. Der Hauptattacke gehen häufig kleinere Angriffe voraus. Der Missbrauch der Mehrwertnummern wird in der Regel in Ländern eingerichtet, in denen eine Rückverfolgung der Täterschaft erschwert ist.

Eine weitere Variante betrifft Online-Zahlungssysteme. Karten mit Online-Guthaben werden von verschiedenen Verkaufsstellen wie Kiosken und Tankstellen vertrieben. Die Täter geben mittels *Spoofing* eine Servicenummer desjenigen Unternehmens vor, das die Karten mit Online-Guthaben herausgibt und kontaktieren damit einzelne Verkaufsstellen. Das Personal gibt, im Glauben mit einem Vertreter des Kartenherausgebers verbunden zu sein, Codes und Informationen der Karten mit Online-Guthaben preis. Die Guthaben werden von der Täterschaft umgehend im Internet eingelöst. Dies verunmöglicht es, den Schaden abzuwenden. Für diese Form des Phone *Phreakings* benötigen die Täter Insiderwissen. Einerseits muss die zuständige Servicenummer der Firma bekannt sein, andererseits müssen die Täter Kenntnisse der technischen Prozesse haben und auch mit den Abläufen des Supports vertraut sein.

Über gehackte *VoIP*-Systeme können auch sogenannte *Vishing*-Angriffe ausgeführt werden (siehe hierzu Kapitel 3.1).

[11] Dieser Artikel basiert auf einem Bericht von fedpol, Bundesamt für Polizei, der MELANI freundlicherweise zur Verfügung gestellt wurde.

Zwingende Voraussetzung für das Phone *Phreaking* sind technische Spezialkenntnisse. Im Internet finden sich zwar detaillierte Anleitungen, doch gilt es immer wieder, auf neue Sicherheitsvorkehrungen zu reagieren und die Vorgehensweise entsprechend anzupassen, was teilweise Programmiervorgänge bedingt. Um auch in gut gesicherte und geschützte Telefonsysteme einzudringen, sind zusätzlich Detailinformationen über Organisation, Abläufe und Mitarbeiter eines Unternehmens notwendig, was häufig Insiderwissen voraussetzt. Man muss aber davon ausgehen, dass Phone *Phreaking* in Zukunft immer einfacher und auch neue Bereiche erfassen wird. Es besteht beispielsweise die Gefahr, dass *Smartphones* zusehends betroffen sein werden – auch das Hacken von *Smartphones* kann man als *Phreaking* bezeichnen. Die durch das Hacken erlangte Kontrolle über das Mobiltelefon nutzen die Täter beispielsweise, um kostenpflichtige *SMS*-Dienste in Anspruch zu nehmen.

3.9 Zweite Paneuropäische Übung «Cyber Europe 2012» - Schweiz nahm wieder daran teil

Am 4. Oktober 2012 nahmen mehr als 500 Cyberspezialisten an der zweiten europaweiten Übung zur Cybersicherheit «Cyber Europe 2012» teil. Kernpunkt der Übung war die Kommunikation und Koordination auf nationaler und europäischer Ebene zur Verbesserung der Widerstandsfähigkeit kritischer Informationsinfrastrukturen. Cyber Europe 2012 war ein Meilenstein, um die Zusammenarbeit, Abwehrbereitschaft und Reaktionsfähigkeit im Fall einer gesamt Europäischen Cybersicherheitskrise zu stärken.[12]

Cyber Europe 2012 hatte drei Ziele:

- Das Testen der Effektivität und Skalierbarkeit von Standardprozeduren, welche die Zusammenarbeit der Behörden in Europa regeln.
- Das Testen der Zusammenarbeit zwischen dem öffentlichen und privaten Sektor in Europa.
- Das Finden von Lücken und Herausforderungen bei grossen länderübergreifenden Netzstörungen in Europa.

29 EU-Mitgliedstaaten und EFTA-Länder (Europäische Freihandelsassoziation) beteiligten sich an der Übung; 25 dieser Länder (darunter auch die Schweiz) nahmen aktiv an der Übung teil, während die restlichen vier als Beobachter anwesend waren. Darüber hinaus beteiligten sich auch verschiedene EU-Organe. Insgesamt wirkten 339 Organisationen mit insgesamt 571 Einzelakteuren mit. Entsprechend einer Empfehlung und im Gegensatz der vorangegangenen Übung «Cyber Europe 2010» beteiligten sich dieses Mal auch Akteure aus dem privaten Sektor. In der Schweiz waren dies je zwei Firmen aus dem Telekommunikations- sowie dem Finanzsektor. Die Zusammenarbeit zwischen Akteuren aus dem öffentlichen und dem privaten Bereich war in der Übungsanlage allerdings auf die nationale Ebene beschränkt, während der öffentliche Sektor auch grenzübergreifend kooperierte.

Im Mittelpunkt des Übungsszenarios standen weitreichende Netzstörungen in Europa, von denen alle teilnehmenden Länder betroffen waren. Das Szenario ging davon aus, dass sich Angreifer zu einem massiven Cyberangriff gegen Europa zusammengeschlossen hatten, der in erster Linie auf *DDoS*-Angriffe gegen elektronische Dienstleistungen abzielte. Betroffen waren beispielsweise E-Government- und Finanzdienste (E-Banking usw.). Diese Netzstö-

[12] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_DE_TRA.pdf (Stand: 28. Februar 2013).

rungen stellten sowohl eine Herausforderung für die Teilnehmer aus dem öffentlich als auch aus dem privaten Sektor dar und erforderten eine länderübergreifende Zusammenarbeit.

Dank der Übung «Cyber Europe 2012» konnten bestehende europäische Mechanismen, welche die Zusammenarbeit im Bereich der Cybersicherheit unterstützen, untersucht, verstanden und bewertet werden. Die Übung stärkte zudem die Zusammenarbeit der Teilnehmer .

Erfahrungen und Erkenntisse:

- Alle teilnehmenden Länder waren während der Übungsphase vollständig eingebunden. Während der Übung kam es zu zahlreichen bilateralen und multilateralen Interaktionen auf internationaler Ebene.
- Mit Hilfe einer Reihe von Standardprozessen und Kommunikationstools konnte während der simulierten Cybersicherheitskrise die Situation in den verschiedenen Ländern gut eingeschätzt werden.
- Die Standardprozesse zeigten allerdings angesichts der grossen Zahl an teilnehmenden Ländern gewisse Schwachstellen in Bezug auf die Skalierbarkeit.
- Um eine schnelle und wirksame Reaktionsfähigkeit in ganz Europa erreichen zu können, ist es entscheidend, dass die betroffenen Stellen mit den Standardprozessen vertraut sind.
- In der Schweiz waren die Kontakte mit den Teilnehmern des privaten Sektors gut etabliert. Die grosse Zahl an Informationen und deren Bearbeitung stellte allerdings eine Herausforderung dar.
- Um eine reibungslose und wirksame Zusammenarbeit zu ermöglichen, sind geeignete, stabile und moderne Kommunikationsinfrastrukturen und Werkzeuge unabdingbar.
- «Cyber Europe 2012» hat zum Vertrauensaufbau zwischen den Ländern beigetragen. Nur auf dieser Grundlage ist es möglich, bei realen Cybersicherheitskrisen erfolgreich und rechtzeitig Massnahmen zur Risikominderung zu ergreifen. Die Übung hat sich sowohl für neue als auch für bestehende Beziehungen als förderlich erwiesen.

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Cyberkonflikt in Nahost – Update

4.1.1 Gauss: Onlinebanking-Trojaner trifft Spionagesoftware

Im Rahmen der Untersuchungen zur Schadsoftware «Flame» [13] entdeckte der russische Antiviren-Software-Hersteller Kaspersky Lab eine weitere Schadsoftware, welche «Gauss» ge-

[13] Zu Flame siehe MELANI Halbjahresbericht 2012/1, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

tauft wurde. Auffallend ist, dass bei «Flame» und «Gauss», Architektur, Struktur der Module, Code-Basis und Kommunikationsformen mit dem *Command & Control Server* sehr ähnlich sind. Es ist hinsichtlich dieser Gemeinsamkeiten naheliegend, dass dieselbe Urheberschaft hinter diesen beiden Schadprogrammen steckt.

Hinweisen zufolge war Gauss seit September 2011 aktiv und konnte bis zu seiner Entdeckung im Juni 2012 vermutlich zehntausende Computer ausspionieren. Die Mehrheit der infizierten Geräte stand im Libanon, gefolgt von Israel und den Palästinensergebieten.

Die Funktionen von Gauss umfassen das Auslesen von Internet-Passwörtern, Angaben zu Online-Bankkonten, *Cookies* und besonderen Konfigurationsdaten der infizierten Computer. Die Schadsoftware wurde so programmiert, dass insbesondere die Beschaffung von Daten im Zusammenhang mit Konten bei libanesischen Banken ermöglicht wurde.

Es handelt sich bei Gauss um den ersten bekannten Fall, in dem eine ausgeklügelte, mutmasslich staatliche Spionagesoftware typische Charakteristiken eines Onlinebanking-Trojaners aufweist. Im Unterschied zu den bekannten Onlinebanking-Trojanern von kriminellen Internetbetrügern leitet die entsprechende Funktion von Gauss keine Bankgeschäfte zum finanziellen Schaden der Nutzer ein, sondern späht aus, welche Banktransaktionen mit dem infizierten Computer vorgenommen werden.

4.1.2 Shamoon: Spionage und Sabotage bei Öl- und Gasfirmen

Am 15. August 2012 wurden Computer im Büronetzwerk der saudischen staatlichen Ölgesellschaft Saudi Aramco auf Grund von Infektionen mit einer Schadsoftware lahmgelegt. Die «Shamoon» benannte Schadsoftware hatte auf befallenen Systemen Informationen zu Dateien gesammelt und an den Angreifer weitergeleitet, bevor die Dateien gelöscht und der *Master Boot Record (MBR)* überschrieben wurde. Die betroffenen Computer wurden auf diese Weise unbrauchbar gemacht und bedurften einer Neuinstallation. Gemäss Angaben von Saudi Aramco wurden über 30‘000 Computer im Unternehmensnetzwerk infiziert – auf die Ölförderung und den Handel hatte dies jedoch keinen Einfluss. Die betroffenen Geräte konnten allesamt wieder instand gestellt werden.

Kurz darauf musste auch der katarische Gasproduzent RasGas sein Büronetzwerk von der Aussenwelt trennen. Obwohl keine offizielle Bestätigung vorliegt, gehen verschiedene Experten davon aus, dass RasGas ebenfalls von Shamoon heimgesucht wurde.

Die beschriebene Funktionalität von Shamoon erinnert an die im Frühling 2012 entdeckte Schadsoftware «Wiper» [14], welche im Iran ihr Unwesen trieb. Die Analyse von Shamoon lässt jedoch darauf schliessen, dass es sich nicht um die selbe Urheberschaft handelt.
Der Aufwand, welcher für diesen Angriff betrieben werden musste, ist nicht unerheblich, was die Beteiligung eines Staates oder zumindest staatliche Unterstützung der Täterschaft wahrscheinlich erscheinen lässt. Verschiedene westliche Experten spekulierten denn auch, dass Bemühungen des Iran dahinter stehen könnten, dessen Energieexport durch die internationalen Sanktionen stark unter Druck geraten ist, um eine Erhöhung der Öl- und Gasproduktion der arabischen Staaten zu verhindern.

[14] Zu Wiper siehe MELANI Halbjahresbericht 2012/1, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

4.1.3 Hacktivismus im Zusammenhang mit dem Nahen Osten

Neben den zwei oben erwähnten aufsehenerregenden Angriffen fanden auch im zweiten Halbjahr 2012 verschiedene kleinere Attacken mit Bezug zum Nahen Osten statt. Hier eine Auswahl:

- Im August wurde zwei Mal die Blog-Plattform der Nachrichtenagentur Reuters und ein Mal der Twitteraccount @ReutersTech gehackt. Dies jeweils mit dem Ziel, Falschmeldungen zu Geschehnissen im Nahen Osten und Propaganda zu verbreiten.

- Ebenfalls im August wurden gezielt E-Mails an syrische Dissidenten verschickt, in welchen sie aufgefordert wurden, ein angebliches Sicherheitsprogramm namens «Anti Hacker» herunterzuladen, um sich vor boshaften Angreifern zu schützen. Dahinter verbarg sich jedoch eine Spionagesoftware.[15]

- Eine Gruppe von (selbstdeklariert) pakistanischen Hackern hatte im September durch Defacement verschiedener Webseiten gegen den umstrittenen Film «Innocence of the Muslims» protestiert. Mitte November wurden dann von dieser Gruppe insbesondere auch israelische Webseiten ins Visier genommen. Zu dieser Zeit lief auch die «Operation Israel» von Anonymous. Diese wurde ausgerufen, nachdem die israelische Regierung die Absicht geäussert hatte, Telekommunikationsverbindungen zum Gazastreifen zu kappen.

- Anonymous erklärte dem Assad-Regime in Syrien den «Krieg», da dieses die Internetverbindungen zum Ausland getrennt habe.[16]

- Eine Hackergruppe hatte verschiedene Nutzerkonten des israelischen Vizepremierministers übernommen und darüber pro-palästinensische Propaganda verbreitet. Dies war anscheinend jedoch nicht Teil der «Operation Israel» von Anonymous, sondern ein davon unabhängiger Akt der Solidarität mit Palästina.

- Aufgrund von Warnungen vor einem gross angelegten Angriff mit Schadsoftware gegen die israelische Polizei wurden die Polizeicomputer präventiv für eine gewisse Zeit vom Internet getrennt. Die Beamten wurden dahingehend sensibilisiert, keine USB-Geräte an ihre Dienstcomputer anzuschliessen. Das interne Computersystem der Polizei war aber jederzeit in Betrieb – nur der E-Mail-Verkehr mit den Behörden war vorübergehend nicht möglich.

- Die Internationale Atomenergiebehörde (IAEA) vermeldete einen Angriff, bei welchem persönliche Kontaktdaten von Wissenschaftlern beschafft und ins Internet gestellt wurden. Die Hacker drohten, weitere sensible Informationen zu veröffentlichen, sollten die Angriffe auf iranische Atomwissenschaftler weitergehen – in den letzten Jahren sind im Iran mehrere Wissenschaftler bei Anschlägen getötet worden, für welche die iranische Regierung Israel und die USA verantwortlich macht.

- Das Sicherheitsunternehmen Symantec entdeckte den Computerwurm «Narilam», welcher sich vor allem gegen Unternehmen im Iran gerichtet zu haben scheint. Die Analyse legt nahe, dass diese Schadsoftware nicht spionieren soll, sondern gezielt ökonomisch re-

---

15 https://www.eff.org/deeplinks/2012/08/syrian-malware-post (Stand: 28. Februar 2013).

16 http://www.youtube.com/watch?v=olZzqa6nwos; http://www.youtube.com/watch?v=xdmlPhWIAuw (Stand: 28. Februar 2013).

levante (z.B. Buchhaltungs-) Datenbanken angreift und dort Datensätze verändert oder löscht.[17]

Über die jeweilige Urheberschaft dieser Angriffe kann durchaus spekuliert werden. Es dürfte jedoch schwierig nachzuweisen sein, ob schliesslich staatliche Organisationen, patriotische Hacker oder Sympathisanten einer bestimmten Gruppierung dahinter stehen und von wem die Täter welche Unterstützung erhalten haben.

4.2 DDoS – Angriffe – Motive, Täter und Opfer

Angriffe auf die Verfügbarkeit von Webseiten, so genannte *Distributed Denial of Service (DDoS)* Angriffe werden in der Cyberwelt für verschiedene Zwecke eingesetzt. Wir haben schon in früheren Halbjahresberichten darüber berichtet.[18] Zu Beginn erfolgten Angriffe vor allem als einfache Vandalenakte. Inzwischen haben sich die Motivationen aber gewandelt. Man beobachtet beispielsweise DDoS als Rachewerkzeug, für die Schädigung der Konkurrenz, für Schutzgelderpressung oder politisch motivierte Angriffe. Während kleinere DDoS Angriffe meist im Verborgenen bleiben und nicht an die Öffentlichkeit gelangen, gibt es immer wieder grössere DDoS-Angriffe, welche darauf abzielen, eine grosse (Medien-) Aufmerksamkeit zu erreichen. Webseiten respektive Webserver gehören dabei zu den bevorzugten Zielen. Es können aber auch Mailserver, *DNS*-Server, *Router* und *Firewalls* oder andere Arten von Internetdiensten betroffen sein. Im zweiten Halbjahr 2012 gab es mit den Angriffen auf die US-Banken sicherlich eine neue Qualität von Angriffen. Doch auch andere Angriffe auf die Verfügbarkeit sorgten für Schlagzeilen:

4.2.1 DDOS auf US-Banken

Seit September 2012 werden zum Teil massive Denial of Service Angriffe (DDoS-Angriffe) gegen diverse US-Banken gemeldet. Betroffen sind beispielsweise die Bank of America, Citigroup, Wells Fargo aber auch noch diverse andere Banken. Bislang sind zwar keine Datendiebstähle bekannt geworden, bei den betroffenen Banken ist es aber immer wieder zu Beeinträchtigungen beim Zugriff auf die Webseiten gekommen.

Das Datenvolumen der Angriffe betrug zeitweise über 60 GB/s. Seit Attackenbeginn wurde von diversen Quellen vermutet, dass die Angriffe aus dem Iran und dort nicht aus dem kriminellen Umfeld stammen, sondern staatlichen Ursprungs seien oder zumindest staatlich unterstützt respektive toleriert werden. So wird auch in einem Artikel der New York Times erwähnt, dass nicht namentlich erwähnte Personen in der US-Regierung davon ausgehen, dass der Iran hinter diesen Angriffen steckt.[19] Ein Beweis, der diese These bestätigt, ist allerdings bis heute nicht erbracht worden. Bisher gibt nur die Tatsache, dass die Angriffe sehr ausdauernd und schwierig einzugrenzen sind, einen Hinweis darauf, dass es auch einen staatlichen Zusammenhang geben könnte. Zugegebenermassen sind in solchen Fällen Beweise schwierig zu erbringen und erfahrungsgemäss auch mit Vorsicht zu geniessen, da auf beiden Seiten ein grosses politisches Interesse besteht. Der Iran hat eine Beteiligung an diesen Angriffen immer kategorisch zurückgewiesen.

---

17 http://www.symantec.com/connect/blogs/w32narilam-business-database-sabotage (Stand: 28. Februar 2013).

18 Siehe auch HJB 2010/2 Kapitel 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 28. Februar 2013).

19 http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=1& (Stand: 28. Februar 2013).

Von verschiedener Seite wurde vermutet, dass der Grund der Angriffe im Wirtschaftsembargo der USA gegen den Iran zu suchen und als Vergeltungsmassnahme zu betrachten ist. Die Gruppe Izz ad-Din al-Qassam Cyber Fighters, welche sich schon zu Beginn öffentlich zu den Angriffen bekannte, gab als Angriffsgrund die Verbreitung des Mohammed Videos an.[20] Auch hierzu gab es Spekulationen, dass unter dem Deckmantel des Hacktivismus' andere Motivationen verschleiert werden sollten.[21]

Auch von Schweizer Computern gingen Angriffe aus. Meist waren dies Webserver mit relativ grosser Bandbreite, die speziell für diesen Zweck von den Angreifern kompromittiert wurden. Deren Betreiber wurden von der Melde- und Analysestelle Informationssicherung (MELANI) informiert.

Nach Aussage der US-Banken dauern die DDoS-Angriffe weiter an, haben aber mittlerweile weniger gravierende Auswirkungen. Die DDoS bedingten Ausfälle sollen in den ersten Januarwochen zurückgegangen sein, obschon die Angreifer Anfang des Jahres wiederum massive Angriffe angekündigt hatten. Beobachter sehen dies als Beweis, dass die Finanzinstitute mittlerweile die Fähigkeiten verbessert haben, solche Angriffe erfolgreich abzuwehren.[22] So zeigte die Traffic-Statistik von 13 führenden US-Institutionen im Januar 2013 eine zeitliche Verfügbarkeit von 97%, währendem in der ersten Phase der Angriffe nur eine Verfügbarkeit von 95 % erreicht wurde (1% eines Tages entspricht ca. 15 Minuten).

Neben den technischen Vorbereitungen sind bei einem DDoS-Angriff vor allem organisatorische und kommunikative Massnahmen zu treffen. Was ein Unternehmen kommuniziert und wie es dies tut, ist unbestritten ein entscheidender Faktor. Eine Kommunikationsstrategie kann als erste Massnahme gegen Auswirkungen von DDoS-Angriffen fungieren. Unbedachte Kommunikation kann demgegenüber aber auch der Auslöser einer (respektive weiterer) DDoS-Attacke sein. Die Risiken und Auswirkungen einer Kommunikation in der breiten Öffentlichkeit müssen deshalb im Vorfeld abgeschätzt werden.

Als zweiter entscheidender Faktor ist sicherlich die technische Vorsorge zu sehen. Es ist viel einfacher, im Vorfeld eines Angriffs Vorbereitungen zu treffen, als erst, wenn die Firmeninfrastruktur unter Attacke steht. Dies gilt vor allem für Firmen, deren Existenz weitgehend von Online-Dienstleistungen oder -verkäufen abhängig ist. Im Normalfall hat hier der Upstream-Provider die Erfahrung und Möglichkeit, entsprechende Lösungen zur Verfügung zu stellen, um DDoS-Angriffe abzuwehren.

Oben genannte Massnahmen gelten natürlich insbesondere für kritische Informationsinfrastrukturen. Betrifft ein DDoS-Angriff einen gesamten Wirtschaftssektor oder ist er sogar sektorübergreifend, ist der Informationsaustausch zwischen den Firmen äusserst wichtig. So wird es möglich, die Angriffe zu verhindern oder zumindest abzufedern. Einen solchen Informationsaustausch stellt MELANI für die Betreiber der Kritischen Infrastrukturen in der Schweiz sicher.

---

[20] http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0 (Stand: 28. Februar 2013).

[21] http://blogs.techworld.com/war-on-error/2013/01/iran-v-usa---the-worlds-first-cyberwar-has-started/index.htm (Stand: 28. Februar 2013).

[22] http://www.bankinfosecurity.com/are-banks-winning-ddos-battle-a-5434 (Stand: 28. Februar 2013).

4.2.2 DDoS-Angriff auf deutschen Stromversorger

Die Webserver des deutschen Stromnetz-Betreibers «50 Hertz Transmission» waren mehrere Tage Opfer eines DDoS-Angriffs. Das Unternehmen bindet fast einen Drittel Deutschlands an das Stromnetz an. Allerdings war die Stromversorgung durch den Angriff zu keinem Zeitpunkt beeinträchtigt, da es die Angreifer nicht auf die Steuerungssysteme (*SCADA*) sondern «lediglich» auf die Webserver des Unternehmens abgesehen hatten. Die E-Mail Kommunikation war ebenfalls vom Angriff betroffen und gestört. 50 Hertz reagierte damit, dass sie die Server vom Netz trennte.

Laut Medienberichten wurden beim Angriff tausende *IP-Adresse*n aus dem osteuropäischen Raum und im Speziellen aus Russland verwendet.[23] Ob die Täterschaft wirklich aus dieser Region stammt oder ob jemand einfach nur ein Botnetz von dort angemietet hat, ist genauso unklar wie auch das Motiv dieses Angriffs.

Ökonomischer Druck führt immer mehr dazu, dass Systeme vereinheitlicht und nicht nur einzelne Komponenten, sondern ganze Unterstationen ferngesteuert und unbemannt betrieben werden. Verwaltungs- und Steuerungsnetzwerk sind allerdings in den meisten Fällen immer noch strikte getrennt. Allerdings verleitet die durchgängig gleiche Netzwerktechnologie immer mehr dazu, das Geschäfts- mit dem Kontrollnetzwerk zu verbinden, um administrative Prozesse zu vereinfachen. Die unterschiedlichen Anforderungen an und die Möglichkeiten für Sicherheitsvorkehrungen müssen dabei aber unbedingt berücksichtigt werden.

Zusätzlich ist zu bedenken, dass gerade bei Stromversorgern nicht nur der Angriff auf die Steuersysteme Auswirkungen auf die Stromnetzstabilität haben kann; auch Systeme, die Informationen für die Erhaltung der Netzstabilität liefern, können essentiell sein. Gerade diese Systeme werden vermehrt mit dem Verwaltungsnetzwerk verbunden und bilden dann einen möglichen Angriffspunkt.

4.2.3 DDoS-Angriff auf Schwedische Regierungsserver und Banken

Anfang Oktober wurden DDoS-Angriffe gegen verschiedene Schwedische Unternehmen und Behörden verzeichnet. Ziel waren neben Banken auch die Website der Schwedischen Staatsbahn SJ, der Nachrichtenagentur TT und Server des Militärs. Der Grund hinter den Attacken wurde im Auslieferungsbegehren Schwedens für Julian Assange vermutet. Nur drei Tage später waren Schwedische Server erneut Ziel einer DDoS-Attacke. Diesmal standen die Schwedische Zentralbank, der Schwedische Reichstag und der nationale Nachrichtendienst Säpo im Fokus. Diese DDoS-Angriffe wurden von Anonymous angekündigt. Hintergrund war der Protest gegen die Schwedische Justiz. Diese ging im Vorfeld gegen Plattformen vor, die das Herunterladen von Filmen und anderen Inhalten mit *BitTorrent* ermöglichten.

4.2.4 Angriffe auf DNS-Infrastruktur

Zunehmend steht auch die DNS-Infrastruktur im Fokus von Attacken. Mit Hilfe des *Domain Name Systems (DNS)* lassen sich das Internet und dessen Dienste benutzerfreundlich verwenden, da man anstelle von *IP-Adressen* so genannte *URLs* (z.B. www.melani.admin.ch) verwenden kann. In der Hierarchie zuoberst befinden sich die Root-Server, welche als obers-

[23] http://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html (Stand: 28. Februar 2013).

te Instanz für Informationen betreffend *Top-Level-Domains* (TLD, z.B. .com, .net, .ch) zuständig sind. Neben diesen TLD-Name Servern laufen bei jedem Provider DNS Server, welche die oberste DNS-Information zwischenspeichern und (den Computern) seiner Kunden zur Verfügung stellen.

Die Deutsche Telekom hatte zwischen dem 3. und 6. September 2012 mit einem massiven Angriff auf diese DNS-Infrastruktur zu kämpfen. Der Angriff konnte aber erfolgreich abgewehrt werden. Eine Einschränkung bei der Namensauflösung wurde nicht beobachtet.

Anfang Jahr 2013 war die SWITCH ebenfalls von einem Angriff auf ihre DNS-Infrastruktur betroffen. Auch dieser Angriff konnte abgewehrt werden.[24] Es war dies das erste Mal, dass die CH-TLD-Infrastruktur angegriffen wurde. Bei diesem Angriff «*DNS-Amplification Attack*» war allerdings nicht die CH-Infrastruktur das Ziel. Sie war nur Mittel zum Zweck, um Webserver in den USA anzugreifen. Bei der beschriebenen Angriffsmethode «DNS-Amplification Attack» wird ausgenutzt, dass Name-Server in bestimmten Fällen auf kleine Anfragepakete mit sehr grossen Paketen antworten. Theoretisch kann eine 60 Byte lange Anfrage eine mehr als 3000 Byte grosse Antwort provozieren. Diese grossen Antworten werden dann auf die eigentlichen Ziele gelenkt. Durch diesen Trick benötigen die Angreifer eine kleinere Angriffsinfrastruktur (Botnetz), um einen grossen Datenstrom zu erzeugen.

DDoS-Angriffe zählen zu den Hauptgefahren von Netzwerken. Dabei nimmt nicht unbedingt die Anzahl der Angriffe, sondern vor allem deren Komplexität zu. Zunehmend werden auch Angriffe auf die DNS-Protokolle beobachtet.[25] SWITCH schreibt in ihrem Blog, dass das DNS-Protokoll das momentan am häufigsten missbrauchte Protokoll für DDoS-Angriffe ist. Zudem würden heute zunehmend *autoritative DNS-Server* benutzt an Stelle von öffentlich erreichbaren *DNS-Resolvern*, wie es früher der Fall gewesen ist.[26]

4.3 Schwachstelle bei PoS-Terminals

Bislang lag der Fokus der Angreifer bei Kreditkartenterminals, so genannten *POS (Point of Sales),* vor allem auf den klassischen *Skimming* Methoden, die eine zusätzliche Hardware in das Terminal einbringen, um den Magnetstreifen und die *PIN* auszulesen. Ein solcher Modus Operandi wurde auch in Schweizer Geschäften angewandt.[27] Eine neue Sicherheitslücke, die von den deutschen Sicherheitsexperten Thomas Roth und Karsten Nohl vom SRLab Anfang Juli 2012 publiziert worden ist, macht nun auf eine weitere Gefahr aufmerksam.

Die Sicherheitsexperten fanden eine kritische Sicherheitslücke in den Kartenterminals «Hypercom Artema Hybrid» des Herstellers Verifone. Der Kartenleser wird mittels *Pufferüberlauf* im *Netzwerk-Stack* angegriffen, was dazu führt, dass der Applikationsprozessor übernommen werden kann. Der Angreifer bekommt dadurch über das Netzwerk Zugang zum Terminal und kann das Eingabefeld und das Display kontrollieren sowie die PIN und auch die Magnetstreifendaten abfangen. Ein potenzieller Angreifer muss sich nicht mehr direkten Zugriff auf das Gerät verschaffen. Es genügt ein Zugriff via *TCP/IP* auf das Terminal. Dabei

---

[24] Ein ausführlicher Bericht zu diesem Angriff folgt im Halbjahresbericht 2013/1

[25] http://www.all-about-security.de/security-artikel/applikations-host-sicherheit/applikationen-web-services/artikel/14953-ddos-angriffe-bleiben-groesste-gefahr-fuer-netzwerke/ (Stand: 28. Februar 2013).

[26] http://securityblog.switch.ch/2012/12/04/ddos-angriffe-durch-reflektierende-dns-amplifikation-vermeiden/ (Stand: 28. Februar 2013).

[27] MELANI Halbjahresbericht 2011/1, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (Stand: 28. Februar 2013).

wird nicht unbedingt physischer Zugriff auf das entsprechende Firmennetzwerk benötigt. Zugang können sich Angreifer beispielsweise auch verschaffen, indem eine Schadsoftware auf den Computer eines Mitarbeiters geschleust wird. Noch einfacher geht es natürlich, wenn das Kartenterminal direkt vom Internet her zugänglich ist, also eine *Public IP-Adresse* besitzt.

Lokale Angriffe direkt am Gerät über die serielle Schnittstelle oder die *JTAG*-Schnittstelle des Applikationsprozessors sind ebenfalls möglich. Bei JTAG operiert man unterhalb der Softwareebene. Der Zugriff über die JTAG-Schnittstelle erfolgt direkt auf den Prozessor, weshalb die Schwachstelle nicht komplett durch ein Software-Update behoben werden kann. [28]

Die Melde- und Analysestelle Informationssicherung (MELANI) wurde frühzeitig über diese Schwachstelle informiert. Sie leitete diese Informationen an die für den Betrieb dieser Terminals zuständigen Firmen in der Schweiz weiter. Die Firmen konnten ihrerseits entsprechende Gegenmassnahmen treffen.

4.4 Angriffe auf EU-Institutionen

Gemäss der US-Nachrichtenagentur Bloomberg soll sich eine Gruppe chinesischer Spione in das Informatiksystem des EU-Rates eingeklinkt haben. Diese als «Byzantine Candor» bezeichnete Gruppe habe E-Mails von Herman Van Rompuy sowie weiterer hoher EU-Beamter abgeschöpft. Im Bloomberg-Artikel steht zudem, die Hacker hätten Verbindung zur chinesischen Volksbefreiungsarmee und das Ganze sei nur dank einer US-amerikanischen Gruppe von Universitätsprofessoren, Unternehmern und IKT-Sicherheitsfachleuten aufgedeckt worden. Ausser dem EU-Rat seien den Hackern mindestens 20 Unternehmen zum Opfer gefallen. All diesen Opfern sei gemeinsam, dass sie Technologien besässen, die China wirtschaftlich einen Wettbewerbsvorteil verschaffen könnten. Die EU hat zu diesen Angriffen keine Stellung genommen.

Laut Bloomberg sei Byzantine Candor nur eines von vielen Beispielen, das geradezu als chinesische Cyberspionage-Industrie bezeichnet werden müsse.

In den letzten zwei Jahren gab es vermehrt Berichte zu ähnlichen Vorfällen (siehe dazu insbesondere die MELANI-Berichte 2011/1 und 2011/2)[29]; Die angeblichen Spionagetätigkeiten von «Byzantine Candor» sowie ihre möglichen Verbindungen zur chinesischen Armee wurden bereits im Dezember 2010 von verschiedenen Medien thematisiert, nachdem Wikileaks eine entsprechende geheime US-Depesche von 2008 veröffentlicht hatte. Darin wurde beschrieben, dass sich die Spionagetätigkeiten aus China in den letzten Jahren vervielfacht hätten. Erst im Februar 2013 hatte die US-Sicherheitsfirma Mandiant einen Bericht veröffent-

[28] http://www.golem.de/news/verifone-ec-kartenterminals-in-deutschland-gehackt-1207-93144.html (Stand: 28. Februar 2013).

[29] Siehe MELANI Halbjahresbericht 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (Stand: 28. Februar 2013).
Siehe MELANI Halbjahresbericht 2011/2: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 28. Februar 2013).

licht, der diverse Spionagetätigkeiten der vergangenen Jahre mehrheitlich gegen US-Firmen der chinesischen Armeeinheit 61398 zuschreibt.[30] Die chinesischen Behörden streiten jedoch die Existenz dieser Art von staatlicher Cyberspionage-Tätigkeit kategorisch ab.

4.5 Eröffnung des CERT der Europäischen Union und des Europäischen Zentrums zur Bekämpfung der Cyberkriminalität (EC3)

Das *CERT* (Computer Emergency Response Team) der Europäischen Union hat seine Arbeit am 11. September 2012 nach einer einjährigen Pilotphase mit anschliessender Evaluation aufgenommen. Sein Kernauftrag ist der Schutz der EU-Institutionen vor Cyberangriffen. Das CERT setzt sich aus IKT- und Sicherheitsfachleuten aus den wichtigsten EU-Institutionen zusammen. Zu seinem Auftrag gehört auch die Zusammenarbeit mit den CERTs der EU-Mitgliedstaaten und mit verschiedenen Sicherheitsfirmen. Die EU-Kommission ist in den vergangenen Jahren mehrmals Cyber-Attacken zum Opfer gefallen[31] [32], was die Notwendigkeit einer solchen Einrichtung verdeutlicht.

Das Europäische Zentrum zur Bekämpfung der Cyberkriminalität (EC3) ist am 11. Januar 2013 in den Räumlichkeiten von Europol in Den Haag eröffnet worden. Das Zentrum versteht sich als Anlaufstelle auf EU-Ebene zur Bekämpfung der Cyberkriminalität. Gemäss EU-Innenkommissarin Cecilia Malmström bietet das EC3 der EU viel mehr Möglichkeiten zur Bekämpfung der Cyberkriminalität und ermöglicht den Schutz eines freien, offenen und sicheren Internet. Der MELANI-Bericht 2012/1[33] enthält eine ausführliche Beschreibung des Zentrums und seiner Kompetenzen.

4.6 Sesam öffne dich: Elektronische Türschlösser in Hotels

Im Juli 2012 führte ein 24-jähriger Hacker an der Konferenz «Black Hat»in Las Vegas den Anwesenden vor, wie sich bestimmte elektronische Schlösser von Zimmertüren in Hotels mühelos entriegeln lassen. Die Methode besteht darin, über den Programmierstecker, der sich offenbar ungeschützt am Hotelschloss befindet, die Sicherheitsschlüssel zu suchen, die uncodiert im Kontrollchip des Türschlosses abgespeichert sind. Medienberichten zufolge weisen offenbar vor allem die Codeschlösser der Firma Onity eine solche Schwachstelle auf.

Ein weiterer Hacker schlug dem Publikum - gestützt auf das soeben zitierte Beispiel - eine besonders wirksame Implementierung dieser Methode vor. Er erklärte auf seinem Blog in allen Einzelheiten die Herstellung eines Geräts, mit dem man in ein Hotelzimmer eindringen kann, das durch ein elektronisches System «geschützt» ist. Das Gerät hat die Grösse und

---

30 Dieses Thema wird ausführlich im nächsten Halbjahresbericht 2013/1 beschrieben.

31 Siehe MELANI Halbjahresbericht 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

32 Siehe MELANI Halbjahresbericht 2011/1: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (Stand: 28. Februar 2013).

33 Siehe MELANI Halbjahresbericht 2012/1: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

Form eines Kugelschreibers und kann also problemlos transportiert werden, ohne aufzufallen.

Ein Update der Türschlösser lässt sich nur mit einem Wechsel der *Platine* bewerkstelligen. Die Kosten werden vom Hersteller allerdings nicht übernommen und müssen von den Hotels selbst bezahlt werden. Der Hersteller bietet alternativ auch eine kostenlose Variante an, bei der ein Deckel den Zugang zum Programmierstecker verhindern soll. Über vier Millionen Türschlösser sollen weltweit betroffen sein.[34]

Anscheinend war die Sicherheitslücke schon länger bekannt. Da der Entdecker die Befürchtung hatte, dass auch Behörden und Geheimdienste Kenntnis von dieser Schwachstelle hatten, machte er die Sache nun öffentlich.

Schon seit einigen Jahren sind nicht mehr bloss Computer oder Server die Zielscheibe von Cyberangriffen. Jedes Informatiksystem kann ins Visier von Hackern geraten. Eine elektronisch gesicherte Hoteltüre zu knacken, ist nur eines von vielen Beispielen, die diese Tatsache illustrieren. Beim Entwerfen von Produkten, die mit einem elektronischen Identifikationsverfahren ausgestattet sind, sollte dieses Risiko systematisch berücksichtigt werden.

Der Zugang zu einem Hotelzimmer kann einem Unbefugten Einblick in vertrauliche Daten verschaffen. Dabei spielt es keine Rolle, ob diese Daten sich, auf einem Laptop, einem *USB*-Stick oder auf Papier befinden. Der vorliegende Fall öffnet deshalb noch einen ganz anderen Teilaspekt und zeigt auf, dass Firmen unbedingt regeln müssen, wie Mitarbeiter auf Dienstreisen mit sensiblen Daten umgehen müssen. Dazu gehören beispielsweise die Sensibilisierung der Mitarbeiter und das Treffen von entsprechenden Vorkehrungen (z.B. die verschlüsselte Ablage von Informationen auf Datenträgern) im Vorfeld einer Geschäftsreise.

4.7 An das Mobilfunknetz angeschlossene Geräte – Grosse Vielfalt und kleines Sicherheitsbewusstsein

Auch das Mobilfunknetz steht bei Sicherheitsfachleuten vermehrt im Fokus. Im Juli 2012 lieferte ein deutscher Forscher den Nachweis für die potentiellen Sicherheitsmängel des Netzes und der daran angeschlossenen Geräte.[35] Mit Hilfe einer *RIPE*-basierten Abfrage suchte der Forscher zunächst nach *IP-Adressen*, die von den Betreibern für an das Mobilfunknetz angeschlossene Geräte vergeben werden. Danach konnte er mit einem einfachen Portscanner verschiedene Informationen zusammentragen. Eine erste Erkenntnis aus diesen Versuchen ist, dass sich auf diesem Netz eine riesige Vielfalt von Geräten tummelt: *GSM/GPRS-Router*, Kameras, *Smart Meter* (Energieverbrauchszähler), *Barcode-Scanner*, Verkehrsleitsysteme usw. Dem deutschen Forscher gelang es sogar einige Male, Lokalisierungsangaben von Geräten zu erhalten, ohne sich vorgängig zu identifizieren. Ein Versuch, sich in Geräte einzuloggen und diese Geräte fernzusteuern, wurde nicht unternommen.

Ziel der Demonstration war es, auf die potenziellen Folgen der Vielzahl an Geräten in diesem Netz aufmerksam zu machen und zu verdeutlichen, wie einfach sie identifiziert werden können. Das kann Personen mit unlauteren Absichten dazu verleiten, nach Sicherheitslücken zu suchen, um die Kontrolle über die Geräte zu erlangen. Solche Personen könnten dann auf

[34] http://www.t-online.de/computer/sicherheit/id_58856082/hacker-knacken-hotel-tueren-binnen-sekunden.html (Stand: 28. Februar 2013).

[35] http://www.heise.de/security/meldung/Scan-in-Mobilfunknetzen-foerdert-tausende-ungeschuetzte-Geraete-zu-Tage-1653619.html (Stand: 28. Februar 2013).

Geräte zugreifen, die im privaten, öffentlichen oder sogar industriellen Bereich genutzt werden.

Immer mehr werden auch kritischere Geräte meist aus Kostengründen über GSM/GPRS angebunden, darunter auch *SCADA* Systeme, Kreditkartenterminals oder Geldautomaten.

4.8 App Stores

Die weltweit führenden Smartphone Contentprovider haben für ihre eigene Kunden virtuelle Shops geschaffen, wo die diversen Anwendungen (Apps) gekauft werden können. Es stellt sich hierbei natürlich die Frage, welche Vor- und Nachteile diese Plattformen unter dem Aspekt der Sicherheit haben.

App Store iOS
Beim «App Store iOS» handelt sich um die im Jahr 2008 lancierte Plattform von Apple. Um zum Apple-Markt Zugang zu haben, sprich um die Apps anbieten zu können, muss sich ein Hersteller zwangsläufig den internen Prüfprozessen von Apple unterstellen[36]. Nur nach einer entsprechenden Analyse wird eine Anwendung im Apple-Shop zugelassen. Ein solcher Prozess soll insbesondere dazu dienen, die Funktionsweise einer Anwendung zu prüfen. Werden die von Apple vorgeschriebenen Kriterien nicht erfüllt, wird die App nicht veröffentlicht. Viele dieser Kriterien betreffen die Sicherheit des Endbenutzergeräts. Eine Anwendung wird beispielsweise nicht veröffentlicht, wenn sie zusätzlichen Programmcode installiert und ausführt, Zugang zu geschützten Daten erlaubt oder solche Daten ohne vorherige Bewilligung an Drittpersonen weitergibt.

Im Falle des «App Store iOS» vertraut der Endbenutzer die Sicherheit vollumfänglich Apple an. Wie wirksam ist aber diese Lösung? Schädliche Anwendungen im System von Apple kommen nur selten vor. In einigen seltenen Fällen wurden die Prüfprozesse umgangen. Der berühmteste Fall ist wahrscheinlich derjenige von Charlie Miller, einem Forscher, dessen Anwendung durch Apple geprüft und akzeptiert wurde. Sie verstiess gegen die Grundregel, keinen Zusatzcode[37] herunterzuladen und auszuführen. Nachdem Millers Heldentat veröffentlicht wurde, entzog ihm Apple die Entwicklerlizenz. Vor kurzem äusserte sich Mike Lee, ein ehemaliger Apple-Angestellter, in einem Interview zu Apple's Überprüfungsstruktur[38]. Lee ist der Ansicht, dass das von Apple zur Analyse der Anwendungen angestellte Team unterdotiert sei. Die Prüfung vieler Anwendungen sei zudem für die Prüfer monoton und uninteressant. Dies gilt sowohl für den (oftmals pornografischen) Inhalt als auch die Tatsache, dass es sich bei vielen Apps um Kopien respektive Updates bereits bestehender Apps handelt. Die monotone Arbeit könne deshalb zu Flüchtigkeitsfehlern führen, wie es beispielsweise bei «Find and Call» (Trojan:iOS/Fidall) der Fall war. Diese App konnte die Liste der Kontakte stehlen und sie an einen Server weiterleiten.

Play Store (Android)
Wie in einem früheren Halbjahresbericht bereits erwähnt[39], verfolgt Google in Bezug auf die

---

36 https://developer.apple.com/appstore/guidelines.html (Stand: 28. Februar 2013).

37 http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (Stand: 28. Februar 2013).

38 http://www.businessinsider.com/heres-why-it-really-sucks-to-be-an-app-reviewer-for-apple-2012-7#ixzz1zaB9ki4H (Stand: 28. Februar 2013).

39 MELANI Halbjahresbericht 2011/2, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 28. Februar 2013).

Anwendungen eine andere Politik. Die Sicherheit wird in diesem Fall vor allem dem Endbenutzer übertragen. Diese Policy ermöglicht es dafür den Benutzern, die Anwendungen für Android von irgendeiner Website aus herunterzuladen. Sie müssen dabei nicht zwangsläufig über den offiziellen Shop von Google, den Play Store, gehen. Trotzdem hat Google das Ziel, seinen Kunden beim Besuch der eigenen Plattform sichere Anwendungen anzubieten. Anfang 2012 führte Google deshalb das System «Bouncer» ein. Dieses System analysiert automatisch alle Anwendungen des Play Stores und durchsucht diese nach schädlichem Code. Im Juli zeigten allerdings zwei Forscher - der bereits erwähnte Charlie Miller und Jon Oberheide - dass es möglich ist, «Bouncer» zu überlisten und ein Android-Smartphone[40] über eine präparierte App zu infizieren.

Google versucht den Spagat zwischen Sicherheit und Flexibilität: Einerseits möchte man den Android-Benutzern einen möglichst offenen und flexiblen Dienst anbieten, was Kriminelle natürlich anzieht. Andererseits will Google dem Endbenutzer auch die grösstmögliche Sicherheit bieten.

Amazon Appstore (Android):
Amazon lancierte im ersten Halbjahr 2011 den eigenen Android-Appstore. Zudem begann Amazon Ende 2011 auch ein entsprechendes eigenes Tablet zu vertreiben. Auf diesem Tablet der neuesten Generation läuft ein verändertes Android 4.0 System «Ice Cream Sandwich», das ausschliesslich zum virtuellen Shop von Amazon Zugang hat. Nach der Lancierung des Appstores äusserten die Experten einige Sicherheitsbedenken. Bemängelt wurde insbesondere, dass Android-Benutzer, welche ohne Amazon Tablet den Store benutzen, die Option «Installation von Apps aus unbekannten Quellen» einschalten müssen, um den Amazon Appstore überhaupt nutzen zu können. Die Downloadrestriktionen werden damit gelockert und es wird eine Möglichkeit geschaffen, dass auch von einer nicht vertrauenswürdigen Website x-beliebige, möglicherweise schädliche Apps installiert werden können. Gemäss dem F-Secure-Bericht des zweiten Quartals 2012[41] wurden nämlich die meisten schädlichen Anwendungen für Android auf «Parallelmärkten» des Google Play Stores festgestellt. Im gleichen Quartal ermittelte F-Secure den ersten Drive-by-Download für Android. Schliesslich überrascht der Bericht der Sicherheitsfirma TrustGo, der nach der Analyse von 2.2 Millionen Apps in insgesamt 187 Märkten zum Schluss kommt[42], dass Play Store und Amazon Appstore bezüglich Sicherheit nur die Plätze vier und fünf belegen. Die fünf «gefährlichsten» virtuellen Android-Shops sollen sich gemäss diesem Bericht allesamt in China befinden.

In geschlossenen Systemen wie demjenigen von Apple liegt die Sicherheit des Endbenutzers in den Händen der Herstellerfirma. Dies hat den Vorteil, dass die komplexen Sicherheitsaufgaben einem Unternehmen anvertraut werden, welches über die entsprechenden Möglichkeiten und die Kenntnisse verfügen sollte. Wie bereits erwähnt, kommen schädliche Anwendungen im System von Apple nur selten vor. Der Nachteil besteht darin, dass die Kunden des App Stores vollumfänglich dem Unternehmen vertrauen müssen und das tatsächliche Geschehen im eigenen System nicht kontrollieren können.

Andererseits wurde das Sicherheitssystem des Play Stores bereits erfolgreich angegriffen und Amazon fordert wie erwähnt die eigenen Anwender auf, die Sicherheitseinstellungen dahingehend zu ändern, dass Anwendungen von ausserhalb des Originalmarktes heruntergeladen werden können. Kriminelle platzieren ihre schädlichen Apps auf verschiedenen Android-Märkten oder Websites und tarnen diese als rechtmässige Anwendungen. Auf den

[40] http://jon.oberheide.org/files/summercon12-bouncer.pdf (Stand: 28. Februar 2013).
[41] http://www.f-secure.com/weblog/archives/MobileThreatReport_Q2_2012.pdf (Stand: 28. Februar 2013).
[42] http://www.trustgo.com/images/en-GB/trustgo_q4_mobile_mayhem.pdf (Stand: 28. Februar 2013).

diversen Märkten zirkulieren Tausende von schadhaften Programmen. Auch wenn der Benutzer bei Android die nötigen Informationen erhält, um die benötigten Rechte der Anwendungen zu beurteilen, wird diese Möglichkeit nur selten genutzt. Für den gewöhnlichen Benutzer, der eine App möglichst einfach und schnell installieren möchte, wird der Sicherheitsaspekt zweitrangig. Diesen Aspekt muss auch der Marktbetreiber berücksichtigen, der ja einen hohen Sicherheitsgrad erzielen will.

4.9 Meldepflicht von Hackerfällen und Netzkontrolle – Pro und Kontra

Einige Länder wie beispielsweise Frankreich, die USA und Deutschland haben angekündigt, rechtliche Vorstösse zur Einführung einer Meldepflicht für gravierende Cyber-Attacken vorzubereiten. Auch die Europäische Kommission möchte gemäss der Cyber-Strategie der Europäischen Union (EU) das Internet mit einer einheitlichen Meldepflicht für Unternehmen, die eine öffentliche Dienstleistung von nationaler Bedeutung anbieten, sicherer machen. Die Telekommunikationsanbieter unterliegen bereits seit der Verabschiedung des Telekommunikationspakets der EU einer Meldepflicht.

Gegen ein solches Vorgehen wehren sich insbesondere die Wirtschaft, Anbieter von Internetdiensten und die Industrie, zumal sie befürchten, dass sich eine Meldung negativ auf ihr Unternehmen auswirken könnte und mit einem Reputationsschaden verbunden sein könnte. Der administrative Aufwand wird als sehr hoch eingestuft. Was genau als Angriff oder Sicherheitslücke gelten soll, muss ausführlich geklärt werden. Grundsätzlich bevorzugen Unternehmen und Betreiber kritischer Infrastrukturen eine bedarfsgerechte, freiwillige Zusammenarbeit mit den Behörden.

Die Vor- und Nachteile von Meldepflicht respektive von einem freiwilligen Informationsaustausch werden in verschiedenen Ländern jeweils kontrovers diskutiert. Auf der einen Seite ist der Aufbau eines solchen freiwilligen Datenaustausches ein Prozess, der auf Vertrauen basiert und eine dementsprechend lange Zeit in Anspruch nehmen kann. Sofortige Erfolge sind selten zu verzeichnen. Hat sich allerdings eine solche Partnerschaft etabliert, ist der Austausch von Informationen qualitativ meist hochwertiger, als dies bei einer Meldepflicht der Fall wäre. Andererseits fliessen bei einer Meldepflicht definitionsgemäss die Informationen von Anfang an. Diese sind aber in ein enges gesetzliches Korsett gezwängt, das sowohl den Behörden als auch den Unternehmen wenig Spielraum lässt. Die Gefahr, dass die Informationen zwar fliessen, aber einen zu kleinen Nutzen generieren, ist daher nicht von der Hand zu weisen. Die Diskussion im Vorfeld eines Meldegesetzes, welche Informationen in welcher Ausführlichkeit und Form gemeldet werden müssen, nimmt erfahrungsgemäss ebenfalls viel Zeit in Anspruch.

Eine Aussage, welche Variante die bessere ist, lässt sich allgemein nicht treffen. Dies hängt sehr stark von der Struktur und der Grösse des jeweiligen Landes ab. Da es in einem grossen Land auch mehr Akteure respektive Firmen gibt, ist der Aufbau eines Vertrauensverhältnisses sicherlich eine grössere Herausforderung. In der Schweiz hat sich über die letzten Jahre der freiwillige Informationsaustausch im Rahmen eines Public Private Partnerships (PPP) etabliert.

5 Tendenzen / Ausblick

5.1 Lücken in Browsern – Zwei Browser Strategie und andere Möglichkeiten

Es gehört mittlerweile zum Standard, vorhandene Sicherheitsupdates von Betriebssystemen und Applikationen regelmässig, am besten automatisch einzuspielen. Trotzdem gibt es immer wieder sogenannte *0-Day* Schwachstellen, also Schwachstellen, für die noch kein Sicherheitsupdate besteht. Fast täglich tauchen solche Sicherheitslücken in verschiedensten Applikationen auf. Davon sind auch die Internet*browser* nicht ausgenommen. Je nach Schwere der bekannt gewordenen Sicherheitslücke kann es sinnvoll sein, zumindest vorübergehend auf einen anderen Browser umzusteigen, bis die Sicherheitslücke durch den Hersteller behoben worden ist.

Was für den privaten Bereich trivial ist, kann in der Geschäftswelt durchaus zu Problemen führen. Anders als bei privaten Computern ist es bei Geschäftscomputern oft nicht so einfach, auf einen alternativen Browser umzusteigen. Beispielsweise, weil keine so genannte Zweibrowserstrategie besteht. Dies ist oft der Fall, damit die zuständige IKT-Abteilung nur einen Browser warten muss.

Kommt es zu einer schwerwiegenden Sicherheitslücke, können durchaus auch vertrauliche oder gar geheime Daten gefährdet sein. Es ist daher sinnvoll, sowohl im Privatleben als auch in der Geschäftswelt für den Ernstfall vorbereitet zu sein, um möglichst schnell auf einen alternativen Browser umsteigen zu können.

Folgende Möglichkeiten sind in der Geschäftswelt denkbar. Die Aufzählung ist dabei nicht abschliessend:

Flächendeckende Ausrüstung aller Arbeitsplätze mit mindestens zwei Browsern
Sämtliche Arbeitsplätze in einem Unternehmen werden mit mindestens zwei Browsern ausgerüstet. Im Notfall kann die Belegschaft angewiesen werden, den betroffenen Browser bis zu einer gegenteiligen Mitteilung nicht mehr zu verwenden. Dies kann allenfalls auch direkt über den *Proxy* gesteuert werden, indem der Zugriff ins Internet für den betroffenen Browser unterbunden wird. Jedoch ist diese Lösung relativ kostenintensiv, da mehrere Browser gewartet werden müssen und für die Benutzer oft nicht klar ist, wann sie welchen Browser verwenden dürfen.

Punktuelle Ausrüstung mit mindestens zwei Browsern
Arbeitsplätze, die unbedingt Zugriff ins Internet benötigen, werden mit mehreren Browsern ausgerüstet. Ist einer der Browser von einer Sicherheitslücke betroffen, kann der Internetzugriff unterbunden werden. Der Zugriff ins Internet ist nur noch mit einem alternativen Browser möglich. Diese Lösung hat den gravierenden Nachteil, dass im Notfall ein Teil der Belegschaft vorübergehend keinen Zugriff ins Internet hat. Auch, wenn dies für die Arbeit vielleicht keinen grossen Einfluss hat, können sich die betroffenen Anwender bevormundet oder benachteiligt fühlen.

White List
Alle Abteilungen eines Unternehmens melden ihrer IKT-Abteilung jene *URLs*, deren Aufruf auch im Notfall möglich sein muss. Diese werden auf einer sogenannten «White List» eingetragen. Tritt eine Sicherheitslücke auf, werden alle URLs gesperrt, die nicht auf der «White List» vermerkt sind. Mit dieser Massnahme kann auf alternative Browser verzichtet werden. Das Schadenrisiko wird minimiert, indem nur noch bestimmte URLs erreichbar sind. Trotzdem besteht weiterhin ein gewisses Risiko. Das Einspielen von Sicherheitsupdates muss

schnell möglich sein, damit die vorübergehende Sperrung von URLs ausserhalb der «White List» möglichst rasch aufgehoben werden kann.

Wie auch immer man sich in der privaten oder geschäftlichen IKT entscheidet: Es ist eine Illusion zu glauben, alternative Browser seien sicherer. Früher oder später taucht bei jedem Browser eine Sicherheitslücke auf. Nur weil momentan von einem bestimmten Browser keine Lücke bekannt ist, bedeutet das nicht, dass der Browser zu 100 Prozent sicher ist. Man sollte sich daher immer mit der notwendigen Vorsicht und gesundem Menschenverstand im Internet bewegen.

5.2 Cyber-Strategien im Überblick

Bis anhin haben über 20 Länder umfassende Cyber-Sicherheitsstrategien veröffentlicht . Die meisten Länder betrachten die Bedrohung aus dem Cyber-Raum als eine der grössten Herausforderungen im 21. Jahrhundert und integrieren als Folge von zunehmenden Cybervorfällen (z.B. Stuxnet, Duqu, Flame und Ghostnet) Cybersicherheit in die nationalen sicherheitspolitischen Strategien (z.B. Frankreich, die Niederlande und Grossbritannien).

In allen Cyberstrategien wird der Einsatz von Informations- und Kommunikationstechnologien (IKT) als Treiber für wirtschaftlichen Fortschritt und sozialen Wohlstand definiert. Gleichzeitig wird die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen und die Minimierung von Cyber-Risiken als nationale Priorität beschrieben.

Cyber als Querschnittsaufgabe
Die Koordination der behördlichen Aktivitäten auf politisch-strategischer sowie auf technisch-operativer Ebene wird als zentral betrachtet. Dies, weil die Bewältigung von Cyber-Risiken als Querschnittsaufgabe verstanden wird und verschiedene Ämter und Akteure im Rahmen ihres Kernauftrags neu auch die Cyber-Ausprägung abdecken müssen. Um dies zu gewährleisten, haben einige Länder sogenannte Cyber-Abwehrzentren geschaffen (z.B. Deutschland und die Niederlande).

Public Private Partnership
Da ein Grossteil der öffentlichen Infrastrukturdienstleistungen in privaten Händen liegt, ist die Zusammenarbeit von Staat und Wirtschaft wesentlich. In den meisten Strategien wird der Bedarf ausgewiesen, diese Zusammenarbeit zu intensivieren und zu institutionalisieren. Vielen Cyber-Strategien liegt die Überlegung zugrunde, den Cyber-Raum nicht mit Vorschriften und staatlichen Markteingriffen, sondern auf freiwilliger Basis mit verstärkter Kooperation sicherer zu machen (z.B. die Schweiz, Grossbritannien und die Niederlande).

Internationale Zusammenarbeit
Die wirksame Minimierung von Cyber-Risiken bedarf auch einer stärkeren internationalen Zusammenarbeit. Diese Erkenntnis findet sich in allen Cyber-Strategien wieder. Dennoch beschreiben die wenigsten Länder detailliert, wie die Zusammenarbeit auf internationaler Ebene verbessert und institutionalisiert werden kann und soll. Eine Ausnahme bilden die USA, deren Cyber-Strategie explizit international ausgerichtet ist. Auch Grossbritannien fördert mit der 2011 initiierten Londoner Conference on Cyberspace einen internationalen Dialog, um internationale Verhaltensregeln für den Cyber-Raum zu definieren. Den internationalen Organisationen (z. B. Europäische Union, G8, die Vereinten Nationen und die Organisation für Sicherheit und Zusammenarbeit in Europa) kommt bei der Erarbeitung von Verhaltensregeln ebenfalls eine wichtige Rolle zu. Sowohl Deutschland als auch Australien setzen sich für gemeinsame Frühwarnsysteme und den Aufbau von Ansprechpartnern ein, über die die Kommunikation im Krisenfall laufen soll.

Mit der Verabschiedung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» setzt die Schweiz im Umgang mit Cyber-Risiken verstärkt auf die Zusammenarbeit zwischen öffentlichen und privaten Akteuren. Der Ansatz des Public Private Partnership (PPP) ist für die Schweiz nicht neu, zumal staatliche Behörden seit der Privatisierung verschiedenster öffentlicher Dienstleistungen, wie beispielsweise des Telekommunikationssektors, den Informationssicherungsprozess der kritischen Infrastrukturen subsidiär unterstützen. Die seit 2004 bestehende Melde- und Analysestelle Informationssicherung MELANI informiert die Betreiber kritischer Infrastrukturen über Vorfälle und Bedrohungen im Cyber-Raum und liefert dadurch einen Beitrag für das Risikomanagement der Unternehmen. MELANI ist denn auch in ihrem Aufbau mit den in anderen Ländern geschaffenen Cyber-Abwehrzentren vergleichbar. Im Vergleich zu einigen Bemühungen in anderen Ländern in diese Richtung, geht die Zusammenarbeit und der Auftrag von MELANI sogar noch weiter.

Diese Zusammenarbeit zwischen Behörden und Wirtschaft hat sich bewährt und funktioniert gut. Mit der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» werden die bestehenden, dezentralen Strukturen gestärkt. Verglichen mit anderen Staaten verzichtet die Schweiz darauf, ein zentrales Steuerungs- und Koordinationsorgan aufzubauen.

5.3 Regulierung versus Freiheit – Wie macht man das Internet sicher?

Das Internet, einst ein amerikanisches militärisches Forschungsprojekt der «Advanced Research Projects Agency» (*ARPA*), hat sich als Informations- und Angebotsplattform durchgesetzt und sich von einem reinen Wissenschaftsnetz zu einer kommerziell genutzten Infrastruktur der Superlative entwickelt. Diese rasante Entwicklung lässt sich an der Zahl der Internet-Nutzer erkennen: Wurde 1991 das Internet erst von ca. 500‘000 Menschen genutzt, sind es heute ungefähr 2.5 Milliarden Menschen. Man schätzt, dass 2020 bis zu 5 Milliarden Menschen – ca. 60% der Weltbevölkerung – einen Internetanschluss haben werden.

Bis zum heutigen Zeitpunkt wird das Internet nicht staatlich reguliert und lässt sich als freier Raum weitgehend über technische Standards und Verwaltungsrichtlinien (so genannte Policies) regeln. Die «Internet Corporation for Assigned Names und Numbers» (ICANN) und die «Internet Society» (ISOC) entwickeln dabei als nichtstaatliche Organisationen diese technischen und administrativen Vorgaben weiter und ermöglichen die Zusammenarbeit von Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft bei der Internetverwaltung. Westliche Regierungen befürworten dieses Multistakeholder-Governance-Modell, und erachten es als zielführend, um die Informationsfreiheit zu gewährleisten.

Es gibt auf der anderen Seite eine starke Koalition von Ländern, die sich für eine Internetregulierung einsetzen, um ihre staatliche Kontrollmacht auf den Cyber-Raum auszudehnen, und die ihre Souveränität stärken respektive sicherstellen wollen.

Die Ende 2012 durchgeführte Weltkonferenz der Internationalen Fernmeldeunion (ITU) – eine Sonderorganisation der Vereinten Nationen – sah in Dubai vor, den Vertrag über die Zusammenarbeit bei Telefonienetzen (International Telecommunication Regulations, ITRs) auch auf das Internet auszudehnen. Die Tatsache, dass 55 von 144 Staaten diesen nicht unterzeichnet haben, obwohl die Internetverwaltung nicht konkret sondern höchstens im Rahmen von Interpretationen berührt wird, illustriert die Uneinigkeit der internationalen Gemeinschaft über die Kompetenzverteilung bei der Internetverwaltung.

Einen nicht zu unterschätzenden Einfluss besitzen globale Firmen wie Anbieter von Software, Suchmaschinen und Social Websites, aber auch die Musik- und Filmindustrie. Diese Firmen haben ein grosses Interesse daran, das Internet so zu entwickeln, dass ihre Ge-

schäftsfelder funktionieren. Solche Firmen versuchen ebenfalls gegen Vorschriften aber auf der anderen Seite auch für fehlende Vorschriften, welche auf der einen Seite Geld kosten oder auf der anderen Seite die eigenen Marktchancen vermindern, zu lobbyieren.

5.4 Spuren im Internet – Welche Daten Benutzer beim Besuch einer Webseite preisgeben

Informationen sind die neue Währung im Internet. Diesen Satz hört man zusehends, wenn es um das Sammeln von Informationen im Internet geht. Immer bessere Programme und eine immer grösser werdende Rechenleistung ermöglichen qualitativ immer besser werdende Auswertungen von grossen Datenmengen, welche dadurch auch besser kommerzialisiert werden können. In solchen Fällen geht zwar die einzelne Person in der Datenflut unter, trotzdem stellen sich viele Benutzer, die tagtäglich elektronische Geräte verwenden, die Frage, welche Daten über sie erhoben und zu welchen Zwecken diese bearbeitet und gespeichert werden.

Verschiedenste Onlineanbieter sind besonders am Benutzerverhalten interessiert, um möglichst spezifisch Werbeanzeigen einblenden und deren Erfolg messen zu können. Bekanntestes Beispiel ist hier sicherlich Google, wo anhand der Suchanfragen des Benutzers die eingeblendete Werbung «personalisiert» wird. Firmen, die Werbung einblenden, leben davon, dass der Benutzer auf den entsprechenden Link klickt. Es ist also für die Firmen bares Geld wert, die Werbung möglichst gezielt und auf den Benutzer zugeschnitten zu platzieren. Der Werbebanner kommt dabei in den meisten Fällen nicht von der Seite selbst, sondern wird von der Werbefirma als Seite in der Seite (als so genannter *IFrame*) eingeblendet. Gleichzeitig sind auf dem IFrame der Werbefirma kleine Skripte eingebaut, die Daten, wie IP-Adresse, *Domain*, *Browser*, lokale Uhrzeit und Betriebssystem sammeln.[43] Auf je mehr Seiten Werbebanner und damit auch Informationssammler platziert sind, desto feiner lassen sich die Nutzungs-Profile erstellen. Allerdings muss der Benutzer natürlich auf den diversen Seiten wiedererkannt werden. Um das zu bewerkstelligen, werden so genannte *Cookies* eingesetzt. Cookies sind prinzipiell nichts Böses, sondern werden verwendet, um persönliche Einstellungen dem entsprechenden Nutzer zuzuordnen, so dass die Eingaben nicht bei jedem Besuch respektive auf jeder Seite erneut gemacht werden müssen. Werbefirmen haben diese Technik aber schnell für ihre Zwecke entdeckt und in ihre Werbebanner eingebaut.

In einer im August 2010 vom Wall Street Journal veröffentlichten Studie wurden 50 der meistbesuchten Seiten angesurft. Der Testcomputer hatte danach 3‘180 Tracking-Cookies gespeichert, welche mehrheitlich von Werbeunternehmen stammten. Die Informationen aus den Cookies werden mit anderen Informationen wie beispielsweise dem Wohnort verfeinert, um ein möglichst präzises Profil der Benutzers erstellen zu können.[44]

Diese Angaben sind abgesehen von der IP-Adresse immer noch mehr oder weniger anonym. Dies ändert sich aber, wenn Firmen diese Nutzungsprofile mit Personendaten abgleichen können. In diesem Zusammenhang wird regelmässig der Like-Button von Facebook thematisiert. Analog zum Werbebanner lässt sich auch hier anhand der auf den diversen Seiten befindlichen Facebook Buttons ein Nutzungsprofil erstellen. Noch bevor der Nutzer

[43] http://de.wikipedia.org/wiki/DoubleClick (Stand: 28. Februar 2013).

[44] http://online.wsj.com/article/SB10001424052748703977004575393173432219064.html (Stand: 28. Februar 2013).

auf den Facebook Button geklickt hat, werden Daten zu Facebook übertragen.[45] Ist der Nutzer nun gleichzeitig bei Facebook eingeloggt, wäre es für Facebook möglich, den Aufruf der Seite direkt der Person zuzuordnen. Auch werden Cookies mit langer Gültigkeitsdauer von bis zu 2 Jahren eingesetzt, so dass die Zuordnung auch im Nachhinein noch möglich wäre.

Neben den im Hintergrund angegebenen Daten kommen auch noch die willentlich abgegebenen Daten wie beispielsweise auf Facebook, Xing oder anderen Social Media Plattformen dazu. Jeder muss sich hier natürlich selber bewusst werden, was er für Daten angeben will und welche nicht. Die Gefahr besteht jedoch, dass im Hintergrund gesammelte Daten mit den willentlich angegebenen Daten verknüpft werden.

Neue Technologien wecken immer auch neue Begehrlichkeiten. Da sich das Surfen vom «normalen» Computer immer mehr auf das *Smartphone* verschiebt, wird Werbung zusehends ortsabhängig eingeblendet. Entsprechend werden *GPS*-Daten zukünftig eine immer grössere Rolle spielen. Ein erster Schritt ist die Ankündigung vom Mobilfunkanbieter «Telefonica», Geodaten kommerziell zu nutzen. Telefonica hat Anfang Oktober 2012 die Abteilung «Telefonica Dynamic Insight» gegründet. Diese Firma ist für die Aufbereitung und Analyse von Informationen – unter anderem auch Geodaten der Telecom Provider – zuständig, welche dann auch kommerziell genutzt werden können. Anhand dieser Daten soll es beispielsweise möglich sein, Personenströme in Abhängigkeit von Wetter, Wochentag und Tageszeit vorauszusagen. Solche Informationen dienen beispielsweise dem Gewerbe, um entsprechend Personal bereitzustellen und Waren einzukaufen oder Gemeinden, um Personenströme zu kontrollieren.

Immer mehr Bedeutung werden Smartphone *Apps* erhalten. Gerade hier herrscht heute jedoch noch eine geringe Transparenz, welche Daten an den Hersteller übertragen werden. Auch neue Techniken wie Gesichtserkennung werden Begehrlichkeiten auf Seiten der Werbebranche wecken. Die Herausforderung für jeden Einzelnen, zu bestimmen, welche Daten über ihn bearbeitet und allenfalls an Dritte weitergegeben werden und welche nicht (informationelle Selbstbestimmung), wird zukünftig kaum einfacher.

Dass man sehr bewusst mit persönlichen Daten im Internet umgehen soll, ist mittlerweile bei den meisten Leuten bekannt. Im Hintergrund werden aber zahlreiche andere Daten über das Surfverhalten gesammelt; meist mit dem Zweck, die geeignete Werbung einzublenden, sprich am meisten Geld zu verdienen.

Um zu verhindern, dass Firmen Informationen über das eigene Surfverhalten erhalten können, haben die Browserhersteller entsprechende Einstellungen bereitgestellt. Eine erste Eingrenzung schafft das Abschalten der Funktion «Cookies von Drittanbietern akzeptieren». Diese Funktion kann neben anderen Privatsphäreneinstellungen in jedem Browser getätigt werden. Firefox und Internet Explorer (die genauen Versionsnummern sind hier[46] ersichtlich) bieten zusätzlich die «Do not Track»-Option an, die man zusätzlich aktivieren kann und einer Webseite per *«opt-out»* mitteilt, dass kein Surfprofil erstellt werden soll. Zusätzlich soll hier noch das Firefox Add-on «Ghostery»[47] erwähnt werden, welches anhand einer Blacklist Tracking Versuche grösstmöglich unterbindet. Es gibt jedoch hier und auch bei den anderen Verfahren keine hundertprozentige Sicherheit, dass keine Daten gesammelt und gegebenenfalls miteinander verknüpft werden können.

---

[45] http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html (Stand: 28. Februar 2013).

[46] http://ie.microsoft.com/testdrive/browser/donottrack/default.html (Stand: 28. Februar 2013).

[47] http://www.ghostery.com/ (Stand: 28. Februar 2013).

5.5 Daten von Drittfirmen auf Firmenseiten – ein Sicherheitsproblem?

Auf vielen Webseiten wird Werbung eingeblendet. Diese Werbung stammt allerdings in den wenigsten Fällen von der Firma selbst, sondern wird von einer Drittfirma produziert und verwaltet (siehe hierzu auch Kapitel 5.4) Nebst Werbung gibt es natürlich noch diverse andere Inhalte, die nicht von den Firmen selbst, sondern von externen Lieferanten generiert werden. Dies kann beispielsweise ein Statistikdienst sein oder ein Dienst, der News oder Börsenkurse einblendet. Dabei wird nicht nur ein Bild, sondern in der Regel eine voll funktionsfähige Seite in der Seite (*IFrame*) mit all den gleichen Rechten wie auch die Hauptseite eingeblendet. Besonders Newsportale nutzen diese Funktionen, da sie darauf angewiesen sind, Informationen von diversen Seiten einbinden zu können.

Abbildung 7: URLs von Drittfirmen, welche auf den Webseiten von zwei Schweizer Zeitungen Inhalte publizieren und Javascript verwenden. Hierzu wurde das Programm NoScript verwendet, welches Drittseiten blockiert, die Javascript benutzen und diese anzeigt.

Abbildung 7 zeigt die diversen Fremdinhalte, welche auf der Webseite von zwei Schweizer Tageszeitungen eingeblendet werden. Beide Seiten beziehen Werbeinhalte von Fremdfirmen. Zum Teil sind die gleichen Firmen und Server für die Auslieferung der Inhalte zuständig. Diesen Servern kommt also eine zentrale Rolle zu. Die Kompromittierung eines solchen Servers kann entsprechend weitreichende Konsequenzen haben und schlimmstenfalls einen beträchtlichen Teil der Computer der Schweizer Bevölkerung infizieren. In den letzten Jahren gab es verschiedentlich kleinere Vorfälle dieser Art. So wurde Mitte Mai 2012 über ein Werbebanner auf wetter.com eine *Schadsoftware* verteilt[48]. Auch Schweizer Firmen waren bereits von solchen Vorfällen betroffen und verteilten auf ihrer Webseite unwissentlich Schadsoftware über eingebundene Werbebanner von Drittfirmen.

Neben all den Vorteilen und der Kosteneinsparung, die eine Zentralisierung von Webinhalten bietet, sollte sich jede Firma auch der damit verbundenen Risiken bewusst sein. Neben der

[48] MELANI Halbjahresbericht 2012/1, Kapitel 4.9: http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=de (Stand: 28. Februar 2013).

Gefahr von Schadsoftware-Infektionen auf Computern der Websitebesucher besteht bei einem Vorfall auch die Gefahr des Vertrauensverlustes in die Firma.

Zwingend sollte schon im Vorfeld definiert werden, wie im Falle von kompromittierten Inhalten von Drittanbietern vorgegangen werden soll. Hat die Firma Zugriff auf die Drittinhalte, respektive kann sie diese im Notfall beeinflussen und unterbinden? Vor allem sollten schon im Vorfeld die Kontakte zu den IKT-Sicherheitsabteilungen der Drittfirmen abgeklärt werden, damit bei einem Vorfall schnell die richtigen Leute benachrichtigt und geeignete Gegenmassnahmen eingeleitet werden können.

5.6 Vertrauen in die Supply Chain

Ende April 2012 wurde bekannt, dass Sunrise den Betrieb und den Unterhalt des Mobil- und Festnetzes für die nächsten fünf Jahre an Huawei auslagern wird. Seit dem 1. September 2012 hat Huawei sodann die gesamte operative Verantwortung von Sunrise übernommen. Anfang Februar 2013 ist auch Swisscom eine Partnerschaft mit dem chinesischen Anbieter eingegangen. Der auf acht Jahre befristete Auftrag umfasst den Glasfaserausbau bis kurz vor die Gebäude (Fibre to the Street, FTTS). In diesem Zusammenhang stellt sich jeweils die Frage, ob das Eindringen ausländischer Firmen in nationale Telekommunikationsmärkte die nationale Sicherheit gefährden könnte. Dies namentlich im Hinblick auf den Zugang zu sensitiven Informationen oder auch auf eine mögliche Sabotage der Informationsinfrastruktur.

Obwohl aktuell keine Kenntnisse über solche Vorfälle vorliegen, kann natürlich nie gänzlich ausgeschlossen werden, dass die Beteiligung ausländischer Telekommunikationsunternehmen am Aufbau oder Betrieb von schweizerischen Telekommunikationsnetzen durch fremde Nachrichtendienste missbraucht werden könnte. Allerdings haben Telekommunikationsunternehmen mit weltweiten Verträgen kein Interesse daran, sich solchen Machenschaften bewusst auszuliefern. Bei einem Bekanntwerden eines solchen Falles müsste neben einem Vertrauensverlust und Reputationsschaden auch mit Sanktionen wie beispielsweise Zugangssperren zu bestimmten Märkten gerechnet werden.

Eine mögliche Einflussnahme durch irgendeinen Staat kann nie gänzlich ausgeschlossen werden, zumal sich auch das äussere politische Umfeld jederzeit verändern kann. Da viele solcher Geräte eine *Firmware* besitzen, ist die Platzierung von *Schadsoftware* zudem auch zu einem späteren Zeitpunkt möglich. Dem Vertrauen in einen Hersteller steht eine Kontrollmöglichkeit gegenüber, welche aber bei jedem Produkt und jedem Firmware-Update eine zeitlich sehr aufwändige und kostenintensive *Sourcecode*-Analyse und Sicherheitstests bedingt. Die Wahrheit liegt auch hier wohl irgendwo in der Mitte. Risiko- und Verwundbarkeitsanalysen gehören zu den Grundelementen jeder Unternehmensstrategie. Die Unternehmen sollten sich daher weniger auf das Ursprungsland des Herstellers fokussieren, sondern auf die Möglichkeiten, unabhängig vom eingesetzten Gerät weitere Sicherungsmassnahmen nachgelagert einzubauen.

6 Glossar

0-Day Exploit	Exploit, der am selben Tag erscheint, an dem die Sicherheitslücke öffentlich bekannt wird.
App	Der Begriff App (von der englischen Kurzform für Application) bezeichnet im Allgemeinen jede Form von Anwendungsprogrammen. Im Sprachgebrauch sind damit mittlerweile jedoch meist Anwendungen für moderne Smartphones und Tablet-Computer gemeint.
Autorativer DNS Server	Ein autoritativer Nameserver ist verantwortlich für eine Zone. Seine Informationen über diese Zone werden deshalb als gesichert angesehen.
Advanced Research Projects Agency Network (ARPANet)	Das Arpanet wurde ursprünglich im Auftrag der US-Luftwaffe ab 1962 von einer kleinen Forschergruppe unter der Leitung des Massachusetts Institute of Technology und des US-Verteidigungsministeriums entwickelt. Es ist der Vorläufer des heutigen Internets.
Barcode Scanner	Ein Barcodeleser ist ein Datenerfassungsgerät, das verschiedene Barcodes lesen und weitergeben kann. Die Erkennung dieser Strichcodes erfolgt dabei rein optisch entweder mit Rot- oder Infrarotlicht.
BitTorent	BitTorrent ist ein kollaboratives Filesharing-Protokoll, das sich besonders für die schnelle Verteilung grosser Datenmengen eignet.
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.
Computer Emergency Response Team (CERT)	Als CERT (auch CSIRT für Computer Security Incident Response Team) bezeichnet man ein Team, das sich mit der Koordination und Ergreifung von Massnahmen im Zusammenhang mit sicherheitsrelevanten Vorfällen in der IT befasst.
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.
Cookies	Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.

Defacement	Verunstalten von Webseiten-Inhalten
Denial-of-Service Angriff (DDoS-Angriff)	Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.
Domain Name System (DNS)	Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch).
DNS-Amplification Attack	Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und diese als Amplifier (Verstärker) benutzt.
DNS Resolver	DNS Resolver sind einfach aufgebaute Software-Module, die auf dem Rechner eines DNS-Teilnehmers installiert sind und die Informationen von Nameservern abrufen können. Sie bilden die Schnittstelle zwischen Anwendung und Nameserver.
Domain	Der Domain Name (z. B. www.example.com) kann durch das DNS (Domain Name System) in eine IP-Adresse aufgelöst werden, die dann verwendet werden kann, um Netzwerkverbindungen zu diesem Rechner aufzubauen.
Drive-By Angriff	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.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf Ihrem Rechner – installiert.
Firmware	Befehlsdaten zur Steuerung eines Gerätes (z.B. Scanner, Grafikkarten, usw.), die in einem Chip gespeichert sind. Diese Daten können in der Regel über Upgrades geändert werden.
General Packet Radio Service (GPRS)	General Packet Radio Service (deutsch: «Allgemeiner paketorientierter Funkdienst») ist ein paketorientierter Dienst zur Datenübertragung, welcher in GSM-Netzen (Mobilfunknetzen) verwendet wird.
Global Positioning System (GPS)	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur

	Positionsbestimmung und Zeitmessung.
Global System for Mobile Communications (GSM)	Das Global System for Mobile Communications (früher Groupe Spécial Mobile, GSM) ist ein Standard für volldigitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Messages) genutzt wird.
HyperText Transfer Protocol Secure (https)	HyperText Transfer Protocol Secure (kurz HTTPS; engl. «sicheres Hypertext-Übertragungsprotokoll») ist ein Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen.
IFrame	Ein IFrame (auch Inlineframe) ist ein HTML-Element, das der Strukturierung von Webseiten dient. Es wird benutzt, um externe Webinhalte in der eigenen Homepage einzubinden.
IP-Adresse	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
Master Boot Record (MBR)	Der Master Boot Record ist der erste Datenblock (512 Byte) eines Speichermediums. Der MBR enthält Informationen, die die Aufteilung des Datenträgers beschreibt und optional, ein Programm, das ein Betriebssystem auf einer der Partitionen startet.
Netzwerk-Stack	Netzwerkstack ist in der Datenübertragung eine konzeptuelle Architektur von Kommunikationsprotokollen.
Opt-out	Opt-out ist ein Verfahren im Marketing, dass eine automatische Aufnahme in eine Verteilerliste vorsieht und der Kunde erst beim ersten Versand, die Möglichkeit erhält, sich aus der Verteilerliste auszutragen.
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.
Phreaking	Mit Phreaking werden Manipulationen von Telefonanlagen bezeichnet.
Persönliche Identifikationsnummer (PIN)	Eine Persönliche Identifikationsnummer (PIN) oder Geheimzahl ist eine Zahl, mit der man sich gegenüber einer Maschine authentisieren kann.

Leiterplatte (Platine)	Eine Leiterplatte ist ein Träger für elektronische Bauteile. Sie dient der mechanischen Befestigung und elektrischen Verbindung. Nahezu jedes elektronische Gerät enthält eine oder mehrere Leiterplatten.
Point of Sales (POS)	Ein POS-Terminal (in der Schweiz EFT/POS-Terminal) ist ein Online-Terminal zum bargeldlosen Bezahlen an einem Verkaufsort (Point of Sale).
Proxy	Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk. Er arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene Adresse eine Verbindung zur anderen Seite herzustellen.
Public IP-Adresse	IP-Adresse, die direkt und von jedem Punkt im Internet erreichbar ist.
Pufferüberlauf	Pufferüberläufe (englisch buffer overflow) gehören zu den häufigsten Sicherheitslücken in aktueller Software, die sich u. a. über das Internet ausnutzen lassen können.
Réseaux IP Européens (RIPE)	Das Réseaux IP Européens Network Coordination Centre (RIPE NCC) ist eine Regional Internet Registry, zuständig für die Vergabe von IP-Adressbereichen und AS-Nummern in Europa, dem Nahen Osten und Zentralasien.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
RSA-Schlüssel	Abkürzung für Rivest-Shamir-Adleman Verschlüsselung. Verschlüsselungsverfahren mit öffentlichen Schlüsseln, das 1978 eingeführt wurde. RSA ist ein asymmetrisches Verfahren.
Supervisory Control And Data Acquisition Systeme (SCADA)	Supervisory Control And Data Acquisition Systeme werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Siehe auch Malware.
Skimming	Skimming (englisch: Abschöpfen) ist ein englischer Begriff für einen Man-in-the-middle-Angriff, der illegal die Daten von Kreditkarten oder Bankkarten ausspäht. Beim Skimming werden Kartendaten erlangt, indem Daten von Magnetstreifen ausgelesen und auf gefälschte

	Karten kopiert werden.
Smart Meter	Ein Smart Meter (deutsch: intelligenter Zähler) ist ein Zähler für Energie, der dem jeweiligen Anschlussnutzer den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit anzeigt, die auch an das Energieversorgungsunternehmen übertragen werden können.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
Short Message Service (SMS)	Short Message Service zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Sourcecode (Quellcode)	Unter dem Begriff Quellcode (englisch source code) wird in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes verstanden.
Spoofing	Spoofing nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.
Transaktionssignierung	Zusätzliches Sicherheitselement beim E-Banking. Gibt der Kunde eine Zahlung in Auftrag, bekommt er beispielsweise per SMS einen Code auf sein Handy geschickt. Erst nach Eingabe des Codes im E-Banking-System wird die Zahlung durch die Bank ausgelöst
Transmission Control Protocol / Internet Protocol (TCP/IP)	Transmission Control Protocol / Internet Protocol (TCP/IP) ist eine Familie von Netzwerkprotokollen und wird wegen ihrer großen Bedeutung für das Internet auch als Internetprotokollfamilie bezeichnet.
Top-Level-Domain	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Die Bezeichnung Top-Level-Domain bezeichnet dabei den letzten Namen dieser Folge und stellt die höchste Ebene der Namensauflösung dar. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
Uniform Resource Locator (URL)	Die Web-Adresse eines Dokuments bestehend aus Protokoll, Server-Name, sowie Dateiname mit Pfad (Beispiel: http://www.melani.admin.ch/test.html).
Universal Serial Bus (USB)	Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.

Voice-Phishing	Voice Phishing ist eine Form des Trickbetrugs im Internet und ist von dem englischen Begriff für abfischen (fishing) sowie der Methode der eingesetzten VoIP-Telefonie abgeleitet.
Voice over IP (VoIP)	Voice over IP. Telefonie über das Internet Protokoll (IP). Häufig verwendete Protokolle: H.323 und SIP.
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.
Zertifikat	Beglaubigt die Zugehörigkeit eines öffentlichen Schlüssels (PKI) zu einem Subjekt.