Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

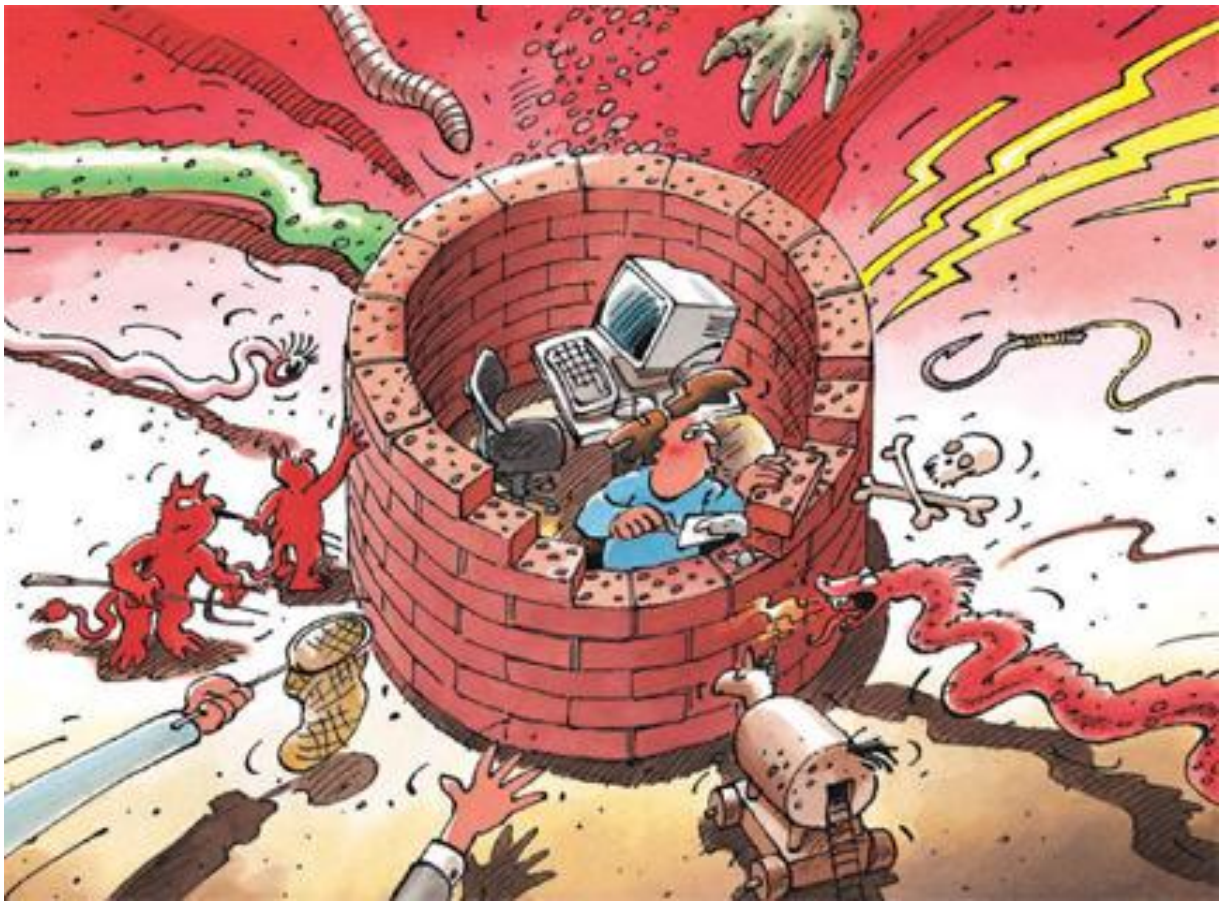
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

# Informationssicherung

## Lage in der Schweiz und international

Halbjahresbericht 2014/I (Januar – Juni)



# Inhaltsverzeichnis

# 1 Schwerpunkte Ausgabe 2014/I

- **Sicherheitslücke in einer der wichtigsten Verschlüsselungsbibliotheken**
  Eine am 7. April 2014 publik gewordene Lücke in OpenSSL - eine der wichtigsten Verschlüsselungsbibliotheken - betraf unzählige Internetbenutzer direkt oder indirekt. OpenSSL ist standardmässig auf vielen Webservern und Internetdiensten installiert, um die Kommunikation zu sichern. Durch die bekannt gewordene Lücke konnten Angreifer einen Teil des Speichers eines betroffenen Servers einsehen, in dem sich die von Benutzern übertragenen Daten während eines kurzen Zeitraums befinden.

  ► Aktuelle Lage International: Kapitel 4.1

- **Social Engineering: Eine Bedrohung mit vielen Gesichtern**
  Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen. Beispiele, bei denen solche Methoden zum Einsatz kommen, sind zahlreich und in den MELANI-Halbjahresberichten immer wieder erwähnt. So hat MELANI auch im ersten Halbjahr 2014 wiederum Meldungen über Betrugsversuche mit Hilfe von Social Engineering gegen Schweizer Firmen erhalten. Zurzeit sind alle in der Schweiz tätigen Unternehmen potenzielle Angriffsziele für Attacken mit Social-Engineering-Methoden, unabhängig von ihrer Grösse oder ihrem Geschäftsbereich.

  ► Aktuelle Lage Schweiz: Kapitel 3.1
  ► Aktuelle Lage International: Kapitel 4.6
  ► Tendenzen / Ausblick: Kapitel 5.1

- **Phishing-Versuche – zugeschnitten auf die Schweiz**
  Im ersten Halbjahr 2014 gab es wieder auffallend viele Phishing-Versuche. Neben den eher international anmutenden E-Mails im ersten Halbjahr 2014 wurden auch einige auf die Schweiz zugeschnittenen Phishing-E-Mails beobachtet. Die Kriminellen haben es dabei vor allem auf die Kreditkartendaten der Opfer abgesehen.

  ► Aktuelle Lage Schweiz: Kapitel 3.2

- **Entwicklungen im Internet nach Snowden**
  Die «Privatsphäre im Internet» hat nach den ersten Veröffentlichungen Snowdens stark gelitten. Der einzelne Nutzer steht dieser Entwicklung eher hilflos gegenüber. Doch welche Entwicklungen im Internet änderten sich durch die aufgrund der Snowden-Affäre gewonnen Erkenntnisse? Diese Frage, die im letzten Halbjahresbericht generell diskutiert wurde, soll in diesem Bericht vertieft und anhand konkreter Beispielen illustriert werden.

  ► Aktuelle Lage International: Kapitel 4.5
  ► Tendenzen / Ausblick: Kapitel 5.3

  **Angriff auf westliche Industrieanlagen**
  Ende Juni 2014 wurde eine Spionage- und Sabotage(vorbereitungs)-Kampagne publik, die sich gegen westliche Industrieanlagen und Energieversorger richtet. Die Angreifergruppe, die von Sicherheitsunternehmen «Dragonfly», «Energetic Bear» oder «Crouching Yeti» getauft wurde, könnte gemäss Hinweisen bereits seit 2010 aktiv sein. Die nun aufgedeckten Angriffe erfolgten ab Frühjahr 2013 in verschiedenen Phasen und über mehrere Wege.

  ► Aktuelle Lage International: Kapitel 4.3

# 2 Einleitung

Der 19 Halbjahresbericht (Januar – Juli 2014) der Melde- und Analysestelle Informationssicherung (MELANI) erläutert die wichtigsten Tendenzen rund um die Gefahren und Risiken, die mit den Informations- und Kommunikationstechnologien (IKT) einhergehen. Er gibt eine Übersicht über Ereignisse im In- und Ausland, beleuchtet Themen im Bereich der Prävention und fasst Aktivitäten staatlicher und privater Akteure zusammen. Erläuterungen zu Begriffen technischer oder fachlicher Art (*Wörter in kursiv*) sind in einem **Glossar (Kapitel 6)** am Ende dieses Berichts zu finden. Die Beurteilungen von MELANI sind jeweils farblich hervorgehoben.

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

**Kapitel 3 und 4** befassen sich mit Pannen und Ausfällen, Angriffen, Kriminalität und Terrorismus, die einen Zusammenhang mit IKT-Infrastrukturen aufweisen. Anhand ausgewählter Beispiele werden wichtige Ereignisse der ersten Hälfte des Jahres 2014 aufgezeigt. Kapitel 3 behandelt dabei nationale Themen, Kapitel 4 internationale Themen.

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

**Kapitel 5.5** enthält ausgewählte parlamentarische Geschäfte mit Bezug zu Themen im Bereich Informationssicherung.

# 3 Aktuelle Lage IKT-Infrastruktur national

## 3.1 Betrugsversuche bei Schweizer Unternehmen

MELANI hat im ersten Halbjahr 2014 mehrfach Meldungen über Betrugsversuche gegen Schweizer Firmen erhalten, die Social Engineering Methoden verwenden. Im Vorfeld eines solchen Angriffs werden typischerweise Informationen über das Unternehmen zusammengetragen, mit denen sich die Betrüger ein Bild von der Zielumgebung machen. Dies kann den Tätigkeitsbereich, die Schlüsselpositionen oder das Format der E-Mail-Adressen umfassen. Anschliessend wird in der Regel ein gefälschtes Mail vom Konto eines Kadermitglieds an einen Mitarbeiter in der Buchhaltung geschickt, das diesen über ein vertrauliches Geschäft informiert und als Kontakt eine «juristische Abteilung der Firma» nennt, welche die Angaben für die Zahlung liefern soll. In einem weiteren Schritt geben sich die Betrüger dann als diese Abteilung aus. Dieses E-Mail mit gefälschtem Absender weist vor allem auf die Dringlichkeit, sowie die ausserordentliche Natur des Auftrags hin, welche absolute Diskretion erfordert. Parallel dazu oder im Vorfeld werden zum Teil auch Telefonanrufe getätigt, um das inszenierte Szenario zu bestätigen und das Opfer dazu zu bringen, eine Überweisung auf das Konto eines Betrügers vorzunehmen.

Ein spezifischer Betrugstyp ebenfalls unter zu Hilfenahme von Social Engineering hat 2014 Finanzinstitute in der Schweiz getroffen. Es handelt sich dabei um einen möglichen Verwendungszweck von mittels Phishing gestohlenen E-Mailzugangsdaten. Bei diesem Modus Operandi suchen die Betrüger in den gehackten Mailkonten nach Korrespondenz eines Kontoinhabers mit seiner Bank. Die Betrüger schreiben dann den entsprechenden Bankangestellten mit der gefälschten Adresse des Kunden an und geben eine Überweisung auf ein Konto im Ausland in Auftrag.[1]

Die Grundregel bezüglich solcher Angriffe auf Firmen lautet, dass bei zweifelhaften oder ungewöhnlichen Kontaktaufnahmen keinerlei Informationen erteilt und keine Aktionen ausgeführt werden dürfen. In solchen Fällen wird dringend empfohlen, allfällige Aufträge oder Kontaktaufnahmen vorgängig telefonisch zu überprüfen. Die Abläufe im Unternehmen namentlich für den Geldtransfer müssen klar definiert und in jedem Fall eingehalten werden. MELANI empfiehlt, das Personal insbesondere in Schlüsselfunktionen für diese Art von Angriffen zu sensibilisieren.

## 3.2 Phishing – auf die Schweiz zugeschnitten

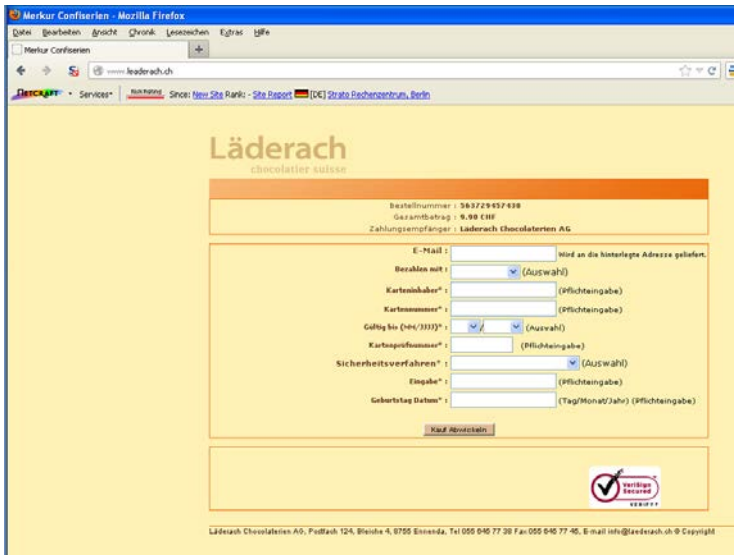
Im ersten Halbjahr 2014 gab es erneut auffallend viele *Phishing-V*ersuche. Neben den eher international anmutenden E-Mails wurden auch einige auf die Schweiz zugeschnittene Phishing-E-Mails beobachtet. Die Kriminellen hatten es dabei vor allem auf die Kreditkartendaten der Opfer abgesehen.

*Das Sonderangebot für Schokolade*

Ein äusserst auf die Schweiz zugeschnittener Angriff erfolgte im Februar dieses Jahres. In einer E-Mail, welche an eine grosse Zahl Empfänger versendet worden war, wurde

[1] http://www.tio.ch/News/Ticino/803356/Pirata-informatico-preleva-un-milione-di-franchi-da-un-conto-luganese/ (Stand: 1. September 2014).

behauptet, dass der Schokoladehersteller Läderach ein Aktionsangebot für Pralinen habe. Bezahlen konnte man direkt und bequem auf der Webseite mit Kreditkarte. Erst ein genauer Blick auf die Webadresse zeigte, dass diese nicht korrekt war: Statt l**ae**derach.ch lautete die Webadresse l**ea**derach.ch. Zusätzlich fehlte die Verschlüsselung der Webseite, auf welcher man seine Kreditkartendaten eingeben sollte.

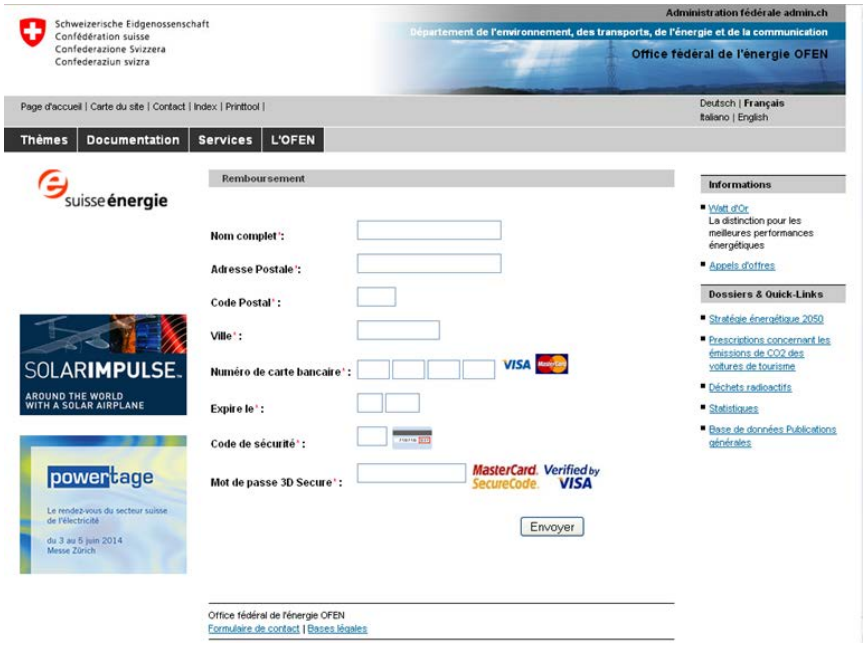



Figur 1: Die Phishingseite gibt vor, vom Schokoladenhersteller Läderach zu stammen

Die Firma Läderach schaltete umgehend eine Information auf ihrer Webseite. MELANI versuchte ihrerseits die gefälschte Webseite vom Netz zu nehmen. Dennoch folgten noch mehrere weitere Angriffe des gleichen Typs. Danach hörten diese aber plötzlich auf. Anscheinend waren zu wenige Opfer auf den Betrug hereingefallen, als dass es sich für die Betrüger gelohnt hätte.

*Logo der Bundesverwaltung für Phishing missbraucht*

Eine andere Phishing-Welle, welche 2014 das erste Mal auftrat, war entschieden hartnäckiger. Die Betrüger versuchten wiederholt, als Bundesamt für Energie (BFE) oder als Energie Schweiz getarnt, per E-Mail an Kreditkartendaten von Internet-Nutzern zu gelangen. Die Empfänger wurden dabei mit einer angeblichen Rückerstattung über CHF 165.00 geködert, die ihnen noch zustehen würde. Um die Auszahlung zu ermöglichen, sollte man sich auf die angegebene Internetseite begeben. Auf der täuschend echt aussehenden Internetseite wurde jedoch nicht nur Name und Adresse verlangt, sondern auch die Kreditkartennummer inklusive Verfallsdatum und Prüfziffer.



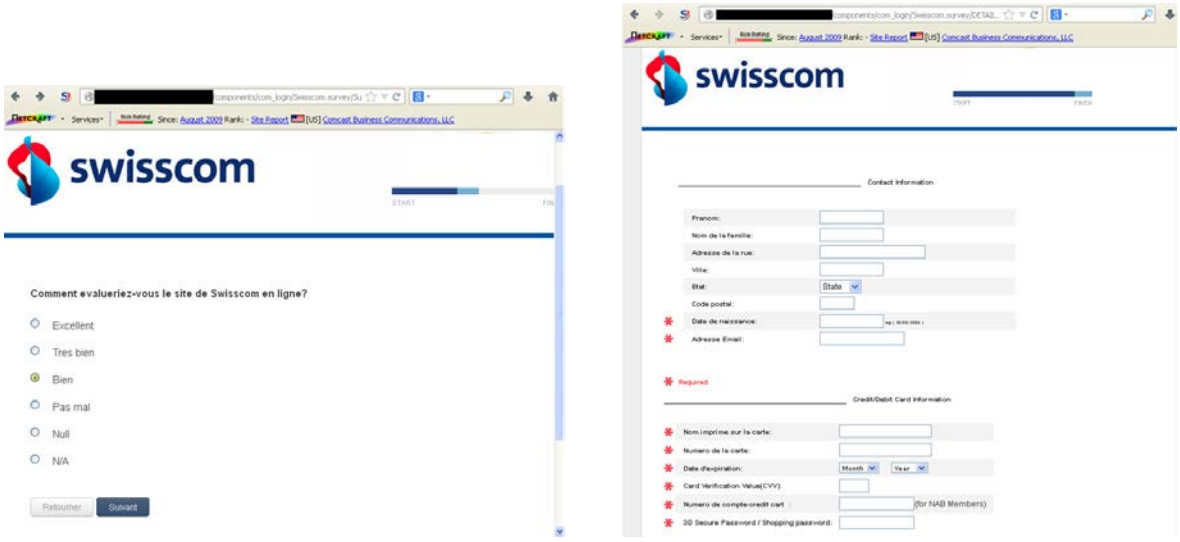
Figur 2: Phishingseite, die vorgibt vom Bundesamt für Energie zu stammen

Auch in diesem Fall wurde vom BFE, zudem von der Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK sowie von MELANI, eine Warnmeldung veröffentlicht. Zusätzlich wurde versucht, die Phishing-Seiten schnell zu deaktivieren. Dies gelang am Anfang nicht optimal, obschon die Webseiten immer auf dem gleichen (tschechischen) Server lagen. Kaum war eine Webseite deaktiviert, wurde auch schon wieder die nächste publiziert. Mittlerweile wurde der Deaktivierungsprozess optimiert, so dass bei Vorfällen innert weniger Minuten eine Deaktivierung erreicht werden kann. Trotzdem werden regelmässig weitere Phishing-Wellen dieses Typs beobachtet.

Die beiden Beispiele zeigen, wie wichtig eine schnelle Reaktion gerade bei den ersten Versuchen einer neuen Variante ist. Kann man bereits die ersten Wellen im Keim ersticken und den Erfolg bei den Angreifern minimieren, hören die Angriffe in der Regel schnell auf. Gelingt dies aber nicht, dann sind die Angriffswellen nur noch schwierig zu stoppen, auch wenn man den Prozess der Webseiten-Deaktivierung beschleunigt und so den Erfolg der Angreifer erheblich einschränkt.

*Phishing-Versuch als Umfrage getarnt*

Bei einem Phishing-Versuch, welcher das Logo der Swisscom missbraucht hatte, kam eine andere Vorgehensweise zum Einsatz. Hierbei köderte man das Opfer mit einer Umfrage. Zuerst wurden zehn Fragen zu Produkten und zur Qualität der Dienstleistungen der Firma gestellt. Am Ende der Umfrage wurde dann Name und Adresse verlangt, aber auch Kreditkartendaten waren Teil der obligatorischen Angabe. Die Absicht der Angreifer war klar: Durch die zehn durchaus sinnvollen Fragen wurde versucht, die Bedenken der Opfer zu zerstreuen. Wieso sollte ein Betrüger auch eine Kundenumfrage machen?




Figur 3: links: eine der 10 Fragen; rechts: am Ende erscheint ein Formular, auf dem man Kreditkartendaten angeben muss: „Dieses Feld ist obligatorisch".

Die aktuellen Phishing-Versuche zeigen, dass es für E-Mail-Empfänger stets schwieriger wird, Phishing-Versuche als solche zu erkennen. Bei E-Mails, in denen die Angabe persönlicher Daten verlangt wird, ist generell Vorsicht geboten. Wird unaufgefordert per E-Mail nach Passwörtern oder Kreditkartendaten gefragt, handelt es sich höchstwahrscheinlich um einen Betrugsversuch. MELANI weist deshalb regelmässig in ihren Warnungen darauf hin: «Keine seriöse Firma wird Sie jemals per E-Mail nach Login, Passwörtern und Kreditkartendaten fragen.»
Diese Aussage, die zunächst einfach klingt, stellt allerdings die Firmen im Zeitalter der elektronischen Kundenkommunikation vor gewisse Herausforderungen. Wie soll eine Firma mit den Kunden kommunizieren, damit diese die Nachricht nicht als betrügerische E-Mail auffassen? Und noch wichtiger: Eine allzu sorglose Kundenkommunikation durch eine Firma kann auch das Kundenverhalten bezüglich betrügerischer E-Mails negativ beeinflussen.

Dass dies ein ernstzunehmendes Thema ist, zeigen angebliche Phishing-Meldungen aus der Bevölkerung, die in Wirklichkeit aber tatsächlich von einer seriösen Firma stammen. Das anschaulichste Beispiel, das MELANI im ersten Halbjahr gemeldet worden ist, stammt von PayPal. Hierbei wurde der Empfänger aufgefordert, die Kreditkartendaten zu aktualisieren. Der Link auf die Webseite war dabei hinter einem Button versteckt, so dass dieser nicht ohne weiteres überprüft und festgestellt werden konnte, unter welcher *URL* die Webseite gespeichert war. Die E-Mail stammte tatsächlich von PayPal.


Figur 4: Gemeldete Phishing E-Mail, die keine ist. Diese E-Mail stammte tatsächlich von Paypal

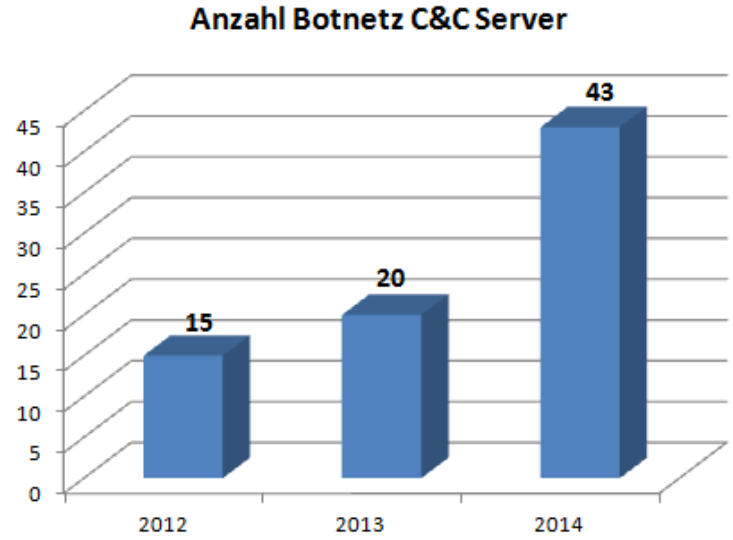
In solchen Fällen ist es empfehlenswert, den Link in der E-Mail trotzdem NICHT anzuklicken, sondern die *URL* der Firma manuell in die *Adresszeile* des Browsers einzugeben und dann zu der entsprechenden Seite zu navigieren. Im Zweifelsfalle sollte man direkt bei der Firma nachfragen.

Firmen sollten folgende Punkte beim Versand von Newslettern beachten:

- Mails wenn möglich im Textformat versenden.
- Newsletter-E-Mails möglichst regelmässig versenden.
- Mit Links in der E-Mail sparsam umgehen und nur auf die eigene Domäne verlinken.
- Wenn möglich Links auf *verschlüsselte Seiten (https://...) b*enutzen und dies dem Empfänger auch mitteilen.
- Nicht auf Webseiten verlinken, die Benutzernamen und Passwort oder andere Daten verlangen.
- Auf der Startseite des Webauftrittes auf den Newsletter hinweisen.
- Kunden, mit Vor- und Nachnamen anschreiben, sofern diese Information vorhanden ist.

## 3.3 Mehr C&C Server in der CH – ein Trend?

Die meisten infizierten Computer werden von einem oder mehreren Kontrollservern überwacht und gesteuert. Diese als *«Botnet Command & Control Server» (kurz «C&C»)* bezeichneten Server kontrollieren die Funktionen der zugehörigen Schadsoftware. Meldungen über solche C&C, welche in der Schweiz lokalisiert sind, sind im vergangenen Halbjahr massiv angestiegen. Auch MELANI konnte vermehrt C&C Server identifizieren und unschädlich machen. Verglichen mit den beiden Vorjahren 2012 / 2013 hat sich die Anzahl gemeldeter bzw. detektierter Botnetz C&C-Server in der Schweiz mehr als verdoppelt.




Figur 5: Anzahl detektierter Botnetz C&C Server in der Schweiz

Bei einem Grossteil der detektierten Infrastrukturen handelt es sich um C&C-Server, welche zum Steuern von mit E-Banking-Trojanern - wie z. B. ZeuS, Citadel oder KINS - infizierten Computern verwendet werden. Neben solcher Schadsoftware, welche üblicherweise eine breite Masse von Internet-Benutzer attackiert, wurde MELANI aber auch auf solche Infrastrukturen aufmerksam, welche für gezielte Angriffe auf Regierungsorganisationen

verwendet werden. Im Fachjargon spricht man bei solchen Angriffen von einem «*Advanced Persistent Threat (APT)».* In vielen dieser Fälle liegt der Verdacht nahe, dass es sich um Spionageversuche von ausländischen Akteuren handelt.

Die Frage stellt sich, wieso Internetkriminelle, welche in der Regel vom Ausland aus operieren, und andere ausländische Akteure den Schweizer Internetplatz für solche Handlungen missbrauchen. Neben dem Fakt, dass die Schweiz hochwertige Infrastruktur bietet, welche sehr gut an das Internet angebunden ist, gibt es auf der anderen Seite sicherlich auch zu berücksichtigen, dass der Datenschutz in der Schweiz gut ausgebaut ist. Polizei und Nachrichtendienst haben einen strengen gesetzlichen Rahmen, den sie beachten müssen, wenn sie im Internet operieren. Dies ist im Licht der Snowden Affäre ein (Standort-) Vorteil, welcher auf Datenschutz und Privatsphäre sensibilisierte Unternehmen wie auch Privatpersonen anzieht. Zudem machen die genannten Umstände den Schweizer Internetplatz attraktiv für ausländische Bürger und Organisationen, welche sich den teilweise scharfen Internetkontrollen in ihrem Land entziehen möchten. Leider wissen dies aber auch Internetkriminelle für sich auszunutzen.

Von der günstigen Lage in der Schweiz haben auch gewisse ausländische Hosting Provider Kenntnis genommen, welche ihr Angebot unlängst auf die Schweiz ausgeweitet haben und versuchen Kunden mit «Offshore Hosting mit Schweizer Qualität» anzulocken. Oftmals drücken diese Hosting Provider dabei beide Augen zu, wenn es um zweifelhafte Inhalte respektive Infrastruktur geht, welche auf Servern in der Schweiz gehostet werden.

MELANI geht Meldungen von Bürgern und Partnern über solche kriminellen Infrastrukturen nach und involviert, falls nötig, die entsprechenden Stellen auf Bundes- und Kantonsebene.

## 3.4 E-Mail gehackt – Kantonsrätin betroffen

E-Mails, worin behauptet wird, dass eine Person im Ausland festsitzt und alles Geld verloren hat, sind bereits seit mehreren Jahren bekannt. Dabei wird jeweils mit gestohlenen Zugangsdaten auf das E-Mail-Konto des Absenders zugegriffen. Danach werden alle oder einzelne Kontakte aus dem Konto angeschrieben. Meist handelt es sich bei diesen E-Mails um gefälschte Hilferufe, dass der Sender irgendwo im Ausland festsitze und das Mobiltelefon, alles Geld sowie der Pass gestohlen worden sei. Schliesslich wird um die Überweisung von Geld gebeten. Immer noch gehen einige dieser Meldungen bei MELANI ein. Auch Politiker sind davor nicht gefeit. Nachdem vor zwei Jahren Kantonsrat Josef Brägger[2] betroffen war, hat es im April 2014 die FDP-Kantonsrätin und Gemeindepräsidentin von Gänsbrunnen, Rosmarie Heiniger, erwischt[3]. Die Hacker verschickten in ihrem Namen ein E-Mail an alle Kontakte, dass sie sich in einer Notlage in den Ferien in Südafrika befände und dringend finanzielle Hilfe benötige. In einem solchen Fall kann es hilfreich sein, alle potenziellen Adressaten der betrügerischen E-Mails, die sich in ihrem Adressbuch befunden haben, auf die Situation hinzuweisen. Das geschieht am besten über eine alternative E-Mail-Adresse oder via Telefon/*SMS*. Allerdings haben sich die Betrüger auch auf diese Massnahme, welche die Erfolgschancen doch erheblich schmälert, eingestellt und löschen kurzerhand das Adressbuch und alle E-Mails. Zu den ganzen Umtrieben und Rückfragen der Empfänger kommt dann noch der Verlust aller Kontakte und der E-Mail-Korrespondenz dazu.

[2] http://www.tagblatt.ch/ostschweiz/thurgau/kantonthurgau/tz-tg/Kantonsrat-von-Unbekannten-gehackt;art123841,2977642 (Stand: 1. September 2014).

[3] http://www.oltnertagblatt.ch/solothurn/thal-gaeu-niederamt/kantonsraetin-rosmarie-heiniger-wird-opfer-eines-hacker-angriffs-127848961 (Stand: 1. September 2014).

Da heute E-Mails meist nicht mehr auf einen Computer heruntergeladen und dort gespeichert werden, sondern via *Webmail* und somit in einer *Cloud* bearbeitet werden, halten die Benutzer häufig ein *Backup* für überflüssig. Diese Pflicht wird von den meisten Benutzern unbewusst an den E-Mail-Provider delegiert. Sie gehen davon aus, dass der Provider für die Backups sorgt. Dies ist zwar insofern korrekt, als dass der Provider für technische Probleme seinerseits (wie zum Beispiel Serverabstürze) ein Backup erstellt. Wenn aber unbefugt auf ein Konto zugegriffen wird und mutwillig – aber über den regulären benutzergesteuerten Prozess – Daten gelöscht werden, hilft ein Backup des Providers in der Regel nur bedingt. Es ist also dringend zu empfehlen, von den Kontakten und auch den E-Mails regelmässig ein eigenes Backup zu erstellen.

Betrüger kommen meist mittels Phishing an die Daten. Viele Phishing-Versuche zielen mittlerweile direkt oder indirekt auf E-Mail-Logindaten. Eine Variante, die schon längere Zeit im Umlauf ist, gibt vor, dass man ein vertrauliches Dokument bekommen haben soll. Zum Abholen dieses Dokumentes solle man auf den Link klicken. Anschliessend wird man gebeten, den E-Mail-Provider auszuwählen und dann Benutzername und Passwort anzugeben. Diese werden dann die Betrüger gesendet.


Figur 6: Phishingseite, um an E-Mail Logindaten zu gelangen

## 3.5 Moderne Alarmierungsmethoden – Chancen und Limiten

Einmal im Jahr werden in der Schweiz die Sirenen getestet, so auch am 5. Februar 2014. Die Information wird in einem solchen Falle über die örtlichen Behörden und die nationalen Radiosender verbreitet. Über die gleichen Kanäle würde bei einer echten Katastrophe auch die Krisenkommunikation geführt. Die SRG/SSR-Radiosender sind denn auch besonders gegen Ausfälle geschützt (siehe hierzu auch den MELANI Halbjahresbericht 2010/2[4]). Allerdings informieren sich heute immer mehr Leute auch über das Internet, beispielsweise auf den Seiten des Bundesamtes für Bevölkerungsschutz (BABS). Genau diese war zum Zeitpunkt des Tests am 5. Februar 2014 allerdings kurzzeitig nicht verfügbar, und es war die Fehlermeldung «Service Unavailable» zu lesen. Die Seite war dem grossen Ansturm nicht gewachsen.

[4] MELANI Halbjahresbericht 2010/2, Kapitel 3.7: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 1. September 2014).

Ein solches Ereignis wirft die Frage auf, unter welchen Bedingungen im digitalen Zeitalter moderne Kommunikationstechnologien für die Alarmierung verwendet werden können. So ist die Ausfallsicherheit der BABS-Website nach dem diesjährigen Sirenentest stark verbessert worden. Darüber hinaus laufen verschiedene Projekte zum Einsatz von neuen Kommunikationstechnologien in diesem Bereich. Die Bewohner des Berner Mattequartiers beispielsweise werden bereits heute bei Hochwassergefahr zusätzlich von der Berufsfeuerwehr Bern via *SMS* über die aktuelle Situation informiert. In Basel gibt es seit 2012 einen SMS-Abo-Service für Menschen, die den Sirenenalarm akustisch nicht wahrnehmen können.[5] Auch das BABS prüft zur Zeit die Einführung eines SMS-Alarmsystems. Konkret strebt das BABS an, künftig einen SMS-Alarm im Sinne des «Cell-Broadcasting» einzusetzen. Dabei wird eine Nachricht an alle Mobiltelefone geschickt, die diesen Dienst aktiviert haben und sich in derselben Mobilfunkzelle befinden. Bei all diesen Projekten geht es nicht um einen Ersatz der bestehenden Alarmierung, sondern um eine Ergänzung der bestehenden Systeme. Damit werden einerseits neue Bedürfnisse der Bevölkerung aufgenommen, andererseits wird die Reichweite der Alarmierung weiter optimiert. Darüber hinaus prüft das BABS auch den Einsatz von weiteren Kommunikationskanälen für die Alarmierung und die Information der Bevölkerung, beispielsweise über bestehende Informationssysteme im öffentlichen Verkehr oder über soziale Netzwerke.

Moderne IKT-Systeme wecken immer neue Begehrlichkeiten auch in Bereichen, in denen die Sicherheit oberstes Gebot ist. Ein Beispiel ist der Einsatz von GPS bei der Flugsicherung[6]. Dabei geht es in vielen Fällen um den Einsatz von Systemen, die kostengünstiger betrieben werden können. Diese Effizienz sollte man sich aber nicht durch Sicherheitseinbussen erkaufen. Im Gegensatz dazu können aber IKT-Systeme eine wertvolle Ergänzung zu den älteren und stabileren Sicherheitssystemen bieten, wie das Beispiel der SMS-Nachrichten im Katastrophenfall zeigt.

## 3.6 Sensible Daten einsehbar

Am 31. März 2014 veröffentlichte die NZZ einen Bericht, dass an der Universität Basel über einen längeren Zeitraum Dokumente im Zusammenhang mit Berufungsverfahren ohne besonderen Schutz auf Servern abgelegt waren, welche direkt mit dem Internet verbunden waren und über eine Suchmaschine gefunden werden konnten.[7]

Insgesamt waren über 1500 Dokumente frei zugänglich. Darunter befanden sich unter anderem Bewerbungsschreiben, Zeugnisse, Empfehlungsschreiben und Diplome. Gerade Bewerbungsunterlagen können zahlreiche Informationen enthalten, welche man nicht jedermann zur Verfügung stellen möchte, insbesondere nicht dem aktuellen Arbeitgeber.

Informiert wurde die Universität Basel durch einen Betroffenen. Das Datenleck wurde umgehend geschlossen und die Betroffenen informiert. Grund für diese Panne war anscheinend ein Fehler bei der Migration von Servern auf eine aktuelle Software. Die Zugriffsrechte von Ordnern wurden bei der Migration nicht korrekt übernommen. Dokumente, die bislang in geschützten Verzeichnissen lagen, wurden so für jedermann einsehbar. Die Universität geht zurzeit davon aus, dass die Daten im Zeitraum vom 27. Februar 2014 bis 15. März 2014 zugänglich waren.

---

5 http://www.polizei.bs.ch/aktuell/gehoerlose-hoerbehinderte.html (Stand: 1. September 2014).

6 MELANI Halbjahresbericht 2011/1, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (Stand: 1. September 2014).

7 http://www.nzz.ch/aktuell/startseite/heikles-datenleck-an-der-universitaet-basel-1.18273869 (Stand: 1. September 2014).

Nach Bekanntwerden dieses Fehlers wurde der Zugang zu den betroffenen Verzeichnissen sofort gelöscht. Zusätzlich wurde für jedes einzelne Dokument bei Google ein Antrag gestellt, dieses auch im Google *Cache* zu löschen. Dieser aufwändige Prozess ist nötig, da das Löschen der Dokumente auf dem Server allein nicht genügt. Veröffentlichte Dokumente werden von Suchmaschinen für eine gewisse Zeit zwischengespeichert.

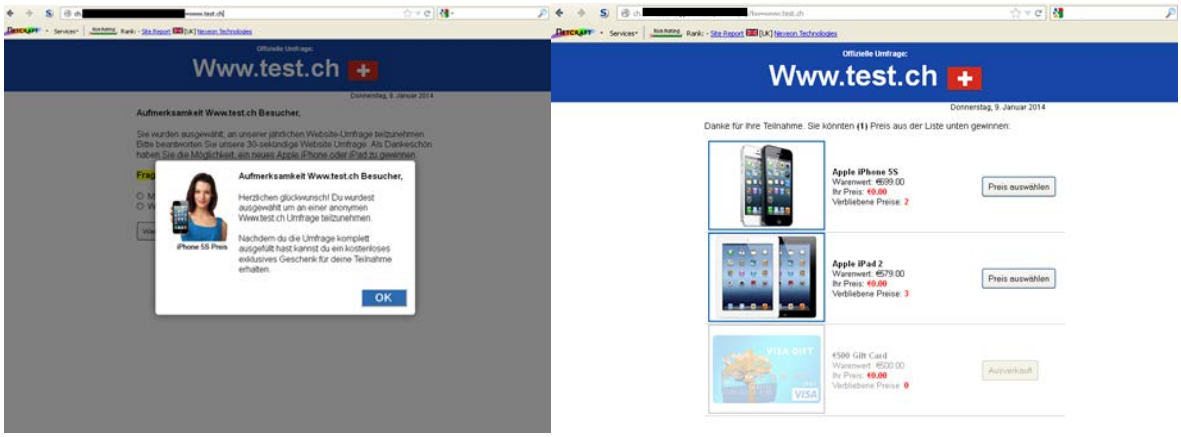
Solche versehentlichen Veröffentlichungen kommen immer wieder[8] vor und können nie gänzlich verhindert werden. Trotzdem gibt es gewisse Leitregeln, die MELANI seit mehreren Jahren propagiert, um solchen Pannen vorzubeugen. Bei der Sicherung von Daten wird sehr viel Gewicht auf die technischen Massnahmen gelegt. Dies alleine genügt jedoch nicht. Informationssicherung besteht zu einem grossen Teil auch aus organisatorischen Massnahmen. Hierzu muss jeder Datei eine bestimmte Relevanz zugeordnet werden. Je nach Relevanz muss diese anders gespeichert und geschützt werden. Im vorliegenden Fall muss man sich deshalb die Frage stellen, wieso solche Daten überhaupt auf einem Server gespeichert waren, auf dem man aus dem Internet zugreifen konnte. Eine fehlerhafte Einstellung der Zugriffsechte kann so erhebliche Probleme verursachen.

## 3.7 Seltsame Fenster während E-Banking Sessions

Im ersten Halbjahr wurden MELANI mehrere Vorfälle gemeldet, bei denen sich während einer E-Banking Sitzung ein Fenster mit einer Umfrage öffnete. Diese Umfrage bestand aus simplen Fragen, wie beispielsweise die Frage nach Geschlecht, Alter und Vorlieben. Anschliessend wurde dem Benutzer vorgegaukelt, dass er ein iPad oder iPhone gewonnen habe. Das gewünschte Geschenk konnte sofort ausgewählt und angeklickt werden. Anschliessend wurde man auf eine Webseite mit dem Namen «Bogabids» geleitet, die anscheinend von Flamingo Intervest betrieben wird und zu der auch die Firma «Ziinga» gehört. Ziinga wurde bereits im Zusammenhang mit einem ähnlichen, früher stattgefundenen Vorfall erwähnt[9]. Tatsächlich geht es wohl um vermeintliche Gratisangebote, welche eine Abonnementsgebühr nach sich ziehen. So steht im Kleingedruckten, dass das Geschenk nur erlangt werden kann, wenn ein Mitgliederbeitrag von mindestens einem Monat bezahlt wird. Je nach Typ des gewählten Abonnements schlägt diese Gebühr mit bis zu 100 Dollar zu Buche. Ein Zusammenhang mit dem E-Banking konnte in keinem Falle nachgewiesen werden. Ebenfalls konnte keine Verbreitung von Malware über diese Seiten festgestellt werden.

[8] MELANI Halbjahresbericht 2008/1, Kapitel 4.1: http://www.melani.admin.ch/dokumentation/00123/00124/01065/index.html?lang=de (Stand: 1. September 2014).

[9] MELANI Halbjahresbericht 2012/2, Kapitel 3.7: http://www.melani.admin.ch/dokumentation/00123/00124/01535/index.html?lang=de (Stand: 1. September 2014).




Figur 7: Popup, welches während einer E-Banking Session erschien

Die Schweizerfahne auf der Website in Figur 7 suggeriert, dass diese Webseite aus der Schweiz stammt, was Vertrauen erwecken soll. Bei einer genaueren Analyse der Webseite stellte sich aber heraus, dass die Flaggen von insgesamt 19 Ländern hinterlegt sind und eingeblendet werden können – je nach Ziel des Angriffs. Diese Liste geht von Australien, Belgien, Brasilien, Finnland bis hin zu den USA. Die Angriffe richten sich also nicht nur gegen die Schweiz, sondern gegen eine Vielzahl von Ländern. Ebenfalls variabel ist die Einblendung des Firmentextes oder der Webadresse links von der Flagge (www.test.ch). Dieser Text kann beliebig durch das Setzen einer Variable in der Webadresse generiert werden. Die Einblendungen dürften durch sogenannte *Adware* generiert werden, welche sich auf dem Computer befindet. Solche Programme werden häufig als Zusatz an Gratisprogramme, *Gratistreiber* oder *VideoCodecs* eingebunden und manipulieren den Computer in der Art und Weise, dass er beim Surfen Werbung einblendet.

# 4 Aktuelle Lage IKT-Infrastruktur international

## 4.1 Heartbleed bei OpenSSL

Eine am 7. April 2014 publik gewordene Lücke in *OpenSSL* - eine der wichtigsten Verschlüsselungsbiblitotheken - betraf unzählige Internetbenutzer direkt oder indirekt. OpenSSL ist standardmässig auf vielen Webservern und Internetdiensten installiert, um die Kommunikation zu sichern. Eine Analyse des IT-Dienstleisters Netcraft zeigt, dass 17.5% aller SSL-Sites, welche Zertifikate eines (vertrauenswürdigen) Zertifikatsaussteller verwenden, die verwundbare Funktion implementiert hatten.[10]

Ursache war eine Sicherheitslücke bei der Funktion «Heartbeat». Eigentlich sorgt diese dafür, dass eine gesicherte Verbindung über eine bestimmte Zeit bestehen bleibt und nicht immer wieder neu initialisiert werden muss. Durch diese Lücke konnten die Angreifer einen Teil, nämlich die letzten 64 *Kilobyte*, des Arbeitsspeichers eines betroffenen Servers einsehen, in dem sich die von Benutzern übertragenen Daten während eines kurzen Zeitraums befinden. Auf diese Weise konnten Passwörter, Transaktionsdaten, aber auch Daten des Servers, wie zum Beispiel *private Schlüssel*, ausgelesen werden.

[10] http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html (Stand: 1. September 2014).

Von dieser Lücke waren nicht nur Mail-Provider oder Finanzinstitute betroffen, sondern generell Webdienste, die ein verschlüsseltes Login anboten und eine verwundbare Software einsetzten. Aber auch nicht-webbasierte Internetdienste wie beispielsweise *Smartphone*-Apps, *Chat*dienste, *Cloud*speicher, *Streaming*dienste, Maildienste und *VPN*-Zugänge waren von der Schwachstelle betroffen.

Während es eher schwierig war, einen kompletten Datensatz abzugreifen, war es jedoch sehr gut möglich, dass dabei Schlüsselmaterial und Zugangsdaten in die Hände von Angreifern fielen und diese erst zu einem späteren Zeitpunkt eingesetzt werden. Deshalb mussten die betroffenen Provider neben dem Schliessen der Sicherheitslücke auch zwingend neue Zertifikate installieren.

MELANI hat sowohl alle Betreiber kritischer Informationsinfrastrukturen als auch die Öffentlichkeit über die zu treffenden Massnahmen informiert.[11] Insgesamt kann festgestellt werden, dass die Umsetzung innerhalb der Schweiz schnell und effizient durchgeführt worden ist. Schwierigkeiten wurden allerdings bei der Bestellung der Zertifikate geortet. Die Menge an neu auszustellenden Zertifikaten brachte die Zertifikatsaussteller an die Kapazitätsgrenze, und es dauerte mitunter mehrere Tage, bis ein neues *Zertifikat* geliefert werden konnte.

*Technische Aspekte und* «*Lessons Learned*»

Durch die Sicherheitslücke in OpenSSL wurde wieder vermehrt der Einsatz von Perfect Forward Secrecy (PFS) thematisiert. Hintergrund ist, dass Angreifer, welche einen verschlüsselten Datenstrom abgegriffen haben, diesen zwar in diesem Moment nicht entschlüsseln können. Aber es besteht die Gefahr, dass dies trotzdem möglich ist, wenn der Schlüssel den Angreifern irgendwann in die Hände fällt. «Heartbleed» ist das Paradebeispiel, wie man zu einem späteren Zeitpunkt an Schlüssel und Zertifikate kommen kann.

Genau hier setzt Perfect Forward Secrecy an: Normalerweise werden Sitzungsschlüssel verwendet, welche jeweils in kurzen Abständen neu ausgehandelt werden. Es ist deshalb einem Angreifer nicht möglich, den gesamten Verkehr zu entschlüsseln, sondern nur einen Teil davon. Ohne PFS werden diese Kurzzeitschlüssel durch einen einzigen Langzeitschlüssel generiert. Wird dieser gestohlen, ist es anschliessend möglich, alle Sitzungsschlüssel zu erhalten und somit auch den gesamten Datenverkehr zu entschlüsseln. Bei PFS ist es trotz Kenntnis des Langzeitschlüssels auch im Nachhinein nicht möglich, Rückschlüsse auf die Kurzzeitschlüssel zu erhalten. Dies wird dadurch erreicht, dass der Langzeitschlüssel nur benutzt wird, um Kurzzeitschlüssel zu signieren. Mit diesen wird jeweils durch einen «*Diffie-Hellman*»-Schlüsselaustausch ein Sitzungsschlüssel ausgehandelt. Wird ein Server kompromittiert, erfährt der Angreifer nur den langfristigen Signaturschlüssel und die Sitzungsschlüssel gerade aktiver Verbindungen. Die Sitzungsschlüssel zurückliegender Verbindungen sind bereits gelöscht und lassen sich nicht mehr rekonstruieren.[12]

In der Folge der OpenSSL-Problematik rückten verschiedene *SSL*-Varianten in den Fokus, welche versuchen, die Probleme der OpenSSL-Library (historisch gewachsen, viele nur selten benötigte Funktionen) zu lösen. In der folgenden Tabelle sind die verschiedenen quelloffenen SSL-Bibliotheken kurz aufgeführt:

[11] http://www.melani.admin.ch/dienstleistungen/archiv/01564/index.html?lang=de (Stand: 1. September 2014).

[12] http://de.wikipedia.org/wiki/Perfect_Forward_Secrecy (Stand: 1. September 2014).

| Bibliothek | Beschreibung | Bemerkungen |
|---|---|---|
| **OpenSSL** | Die nach wie vor am häufigsten verwendete Bibliothek. | OpenSSL wird momentan einem intensiven *Code Review* unterzogen. So sollen weitere Fehler entdeckt und behoben werden. |
| **LibreSSL** | Eine Weiterentwicklung von OpenSSL, die nicht benötigte Funktionen beseitigt und gleichzeitig versucht, möglichst nahe bei OpenSSL zu bleiben und Migrationen einfach zu halten. | Stammt von den Entwicklern um OpenBSD, welche sich einen ausgezeichneten Namen im Bereich sicherer Software gemacht haben. |
| **PolarSSL** | PolarSSL wurde entwickelt, weil OpenSSL zu gross und komplex geworden war und fokussiert sich auf die für TLS-Verbindungen notwendigen Funktionen. | PolarSSL ist dual-licensed, einerseits unter GPL v2, andererseits auch als kommerzielle Lizenz erhältlich. |
| **GnuTLS** | GnuTLS ist ähnlich umfangreich in Bezug auf die Funktionalität wie OpenSSL. Immer wieder tauchten Sicherheitslücken auf. | GnuTLS wurde seit längerer Zeit als Alternative zu OpenSSL entwickelt und ist Teil des GNU Projekts. |

MELANI empfiehlt generell, kryptographische Verbindungen so zu konfigurieren, dass eine möglichst hohe Sicherheit erreicht werden kann[13].

In Bezug auf SSL/TLS bedeutet dies:

- nur sichere Ciphers zu verwenden, wie z.B.
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  oder
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- Perfect Forward Secrecy zu ermöglichen, damit bei einer Kompromittierung eines privaten Schlüssels allfällig aufgezeichneter Verkehr nicht später entschlüsselt werden kann. Dies wird mit den oben erwähnten Algorithmen erreicht.
- Dennoch müssen die Privaten Schlüssel so sicher wie möglich aufbewahrt werden, idealerweise auf einem *Hardware Security Module (HSM)*.
- Einsatz von *HSTS (HTTP Strict Transport Security)*. Der Server teilt mit HSTS dem Browser mit, wie dieser mit den verschlüsselten Verbindungen umgehen soll. So ist sichergestellt, dass ein Browser nur verschlüsselt und mit gültigen Zertifikaten mit diesem Server kommuniziert.
- Mixed Content vermeiden (ein Teil des Inhalts wird verschlüsselt übertragen, der andere Teil bleibt unverschlüsselt). Wenn verschlüsselte und unverschlüsselte Inhalte gemixt werden, können Angreifer beispielsweise über unverschlüsselte Inhalte möglicherweise Session-Informationen manipulieren.
- Verwenden einer vertrauenswürdigen *Certificate Authority (CA)*. Allgemein und im Speziellen bei einem Vorfall hat es Vorteile, wenn eine CA im gleichen Rechtssprechungsraum liegt. Je nach Ausrichtung der Firma und je nach

[13] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report/at_download/fullReport (Stand: 1. September 2014).

Bedrohungslage sollte deshalb darauf geachtet werden, dass die entsprechende CA ihren Sitz in der Schweiz hat.

«Heartbleed» hat aufgezeigt, dass es sich aus Architektursicht lohnen kann, einen zentralen Eintrittspunkt für sämtliche SSL-Verbindungen zu haben, der entsprechend überwacht wird und bei einer Sicherheitslücke sehr rasch *gepatched* werden kann.

## 4.2 Spionagevorfälle

Auch im ersten Halbjahr 2014 machten einige Spionagevorfälle Schlagzeilen. So publizierte das russische IKT-Sicherheitsunternehmen Kaspersky am 10. Februar 2014 einen Spionagefall mit dem spanischen Namen «Careto» oder zu Deutsch «die Maske».[14]

*Careto / The Mask*

Die Operation «Careto» soll bereits seit 2007 laufen, jedoch blieb sie während mehr als sechs Jahren unentdeckt. Diese Spionagekampagne zeichnet sich durch ihre Universalität und ihre Anpassungsfähigkeit aus. Die Schadsoftware kann nicht nur verschiedene Betriebssysteme wie Windows, Mac, Linux usw. befallen, Kaspersky vermutete auch die Existenz einer Version für Smartphones. Die Infektion fand über den Versand von *Spearphishing*-E-Mails statt. Diese E-Mails enthielten Links zu Websites, welche verschiedene auf das Opfer zugeschnittene *Exploits* bereitstellten. Die *Exploits* waren in Unterordnern von Websites versteckt, so dass diese nur über den direkten Link, nicht aber über einen zufälligen Besuch der Website erreichbar waren. Um die Links legitim erscheinen zu lassen, verwendeten die Angreifer URLs, welche die Domänen der wichtigsten Tageszeitungen Spaniens, aber auch internationaler Zeitungen wie «The Guardian» und der «Washington Post» imitierten.

Sobald die *Schadsoftware* installiert ist, befällt sie verschiedene Kommunikationskanäle, wie zum Beispiel Skype, und versucht, möglichst viele Dokumente unterschiedlichsten Typs zu sammeln. Kaspersky machte in 31 Ländern mehr als 380 Opfer aus, darunter auch in der Schweiz. Betroffen waren verschiedenste Sektoren im öffentlichen Bereich (Regierungen, diplomatische Vertretungen) sowie in der Privatwirtschaft (Energie, Forschung, Finanzen). Bei solch komplexen Angriffen wird jeweils ein staatlicher Akteur als Täterschaft vermutet. Der in der Schadsoftware enthaltene spanische Text, der auf eine Urheberschaft im spanischsprachigen Raum schliessen lässt, ist in diesem Zusammenhang aber eher überraschend. Es kann sich dabei natürlich auch um eine bewusst gelegte falsche Spur handeln.

*Uroburos/ Turla/ Snake/ Epic*

Im ersten Halbjahr 2014 erschienen Berichte von diversen Sicherheitsdienstleistern[15] über einen Spionagekomplex mit den Namen «Epic», «Turla», «Uroburos» und «Snake». Der deutsche IKT-Sicherheitsdienstleister G-Data[16] hat im März 2014 einen Bericht über die Spionagesoftware Uroburos publiziert. Die komplexe Malware besitzt unter anderem eine «*Peer to Peer*»-Funktionalität. Das heisst, dass die Verbreitung und Kommunikation auch in einem internen Netzwerk funktioniert, in dem nicht unbedingt alle Computer am Internet angeschlossen sein müssen. Als Ziele genannt werden staatliche Einrichtungen, Nachrichtendienste und Grossunternehmen. G-Data sieht den Beginn der Kampagne im

[14] http://securelist.com/blog/research/58254/the-caretomask-apt-frequently-asked-questions/ (Stand: 1. September 2014).

[15] http://securelist.com/analysis/publications/65545/the-epic-turla-operation/ (Stand: 1. September 2014).

[16] https://blog.gdata.de/artikel/uroburos-hochkomplexe-spionagesoftware-mit-russischen-wurzeln/ (Stand: 1. September 2014).

Jahr 2011, weil die ältesten gefundenen Treiber damals kompiliert worden sind. Ein Report von «BAE Systems Applied Intelligence» sieht die Entwicklung der Schadsoftware allerdings sogar schon im Jahr 2005.[17] Auch beim im Mai bekannt gewordenen Spionageangriff gegen das Belgische Aussenministerium soll die Spionagesoftware Uroburos eingesetzt worden sein. Dies meldete die belgische Tageszeitung «De Standaard» unter Berufung auf eine vertrauenswürdige Quelle[18]. Die Angreifer sollen es in diesem Fall vor allem auf Dokumente, Analysen und Berichte zur «Ukraine-Krise» abgesehen haben.

*Operation Newscaster*

Ein gezielter *Spearphishing*-Angriff gelang einer iranischen Hackergruppe, welche während drei Jahren über 2000 Computer infizieren konnte.[19] Für die Operation mit dem Namen «Newscaster» kreierte die Gruppe dutzende gefälschte Profile auf allen grösseren sozialen Netzwerken. Die Personen hinter diesen Profilen gaben vor, im Bereich Journalismus, Rüstung oder bei der Regierung zu arbeiten. Dies alles mit dem Zweck, möglichst viele Opfer zu überzeugen, den Angreifer als «Freund» zu akzeptieren. Sogar eine falsche Newsseite, bei der die vermeintlichen Journalisten arbeiteten, wurde für die Operation aufgesetzt. «Newsonair.org» kopierte hierzu Inhalte von anderen Newsportalen und publizierte diese unter ihrem eigenen Namen. In einem ersten Schritt wurden nur ungefährliche E-Mails mit einfacher Korrespondenz verschickt. Es ging vor allem darum, Vertrauen bei den gezielt ausgewählten Opfern zu schaffen. War das Vertrauen aufgebaut, wurden mit Schadsoftware präparierte E-Mails versendet. Zielpersonen waren vor allem militärische und politische Kader in den USA und Israel.

*Symbolische Aktion gegen mutmassliche chinesische Spione?*

Das US-Justizministerium hat gegen fünf chinesische Militärangehörige Anklage wegen Cyberspionage erhoben.[20] Die Angriffe sollen im Zeitraum zwischen 2006 und 2014 stattgefunden haben.[21] Die Angeklagten gehören zur chinesischen Volksbefreiungsarmee. Da diese Personen wohl nie in die USA oder in Staaten mit einem Auslieferungsabkommen einreisen werden, ist diese Anklage eher symbolischer Natur.

Gezielte Spionageangriffe sind längst keine Einzelereignisse mehr. Es besteht ein ständiges Interesse und demzufolge ein ständiger Druck auf sensible Daten. Davon ist auch die Schweiz nicht ausgenommen, da gerade hier sehr viele Spitzenunternehmen ansässig sind, die über Know-how oder Informationen mit grossem Wert verfügen.

## 4.3 Angriff auf westliche Industrieanlagen

Ende Juni 2014 wurde eine Spionage- und Sabotage(vorbereitungs)-Kampagne publik, die sich gegen westliche Industrieanlagen und Energieversorger richtet. Die Angreifergruppe, die

---

17 http://www.baesystems.com/what-we-do-rai/the-snake-campaign? (Stand: 1. September 2014).

18 http://www.standaard.be/cnt/dmf20140512_01103164 (Stand: 1. September 2014).

19 http://www.isightpartners.com/2014/05/newscaster-iranian-threat-inside-social-media/ (Stand: 1. September 2014).

20 http://www.spiegel.de/netzwelt/netzpolitik/cyberspionage-usa-klagen-chinesische-regierungsbeamte-an-a-970259.html (Stand: 1. September 2014).

21 MELANI Halbjahresbericht 2013/1, Kapitel 4.2: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 1. September 2014).

von Sicherheitsunternehmen «Dragonfly[22]», «Energetic Bear[23]» oder «Crouching Yeti[24]» getauft wurde, könnte gemäss Hinweisen bereits seit 2010 aktiv sein. Die nun aufgedeckten Angriffe erfolgten ab Frühjahr 2013 in verschiedenen Phasen und über mehrere Wege. In einem ersten Schritt wurden E-Mails mit einer Schadsoftware im Anhang an ausgesuchte Mitarbeiter in den Zielunternehmen gesendet (*Spear-Phishing*). Weiter infiltrierten die Angreifer mehrere Webseiten, die sich thematisch mit Energieversorgung beschäftigen und platzierten dort *Drive-by-Infektionen* (*Watering hole-Angriffe*). Schliesslich gelang es der Gruppe auch, legitime Softwarepakete auf Webseiten von Herstellern *speicherprogrammierbarer* Steuerungen durch manipulierte Versionen zu ersetzen.

Die Angreifer setzen verschiedene Malwaretypen für das Erreichen ihrer Zwecke ein:

- *Trojanische Pferde* (Havex und Sysmain)
- *Hintertüren* (Karagany und Oldrea)
- Weitere Werkzeuge für den jeweiligen Einsatzzweck (Verankerung im Netz, Datendiebstahl).

Für die Angriffe wurden nur bereits bekannte Sicherheitslücken ausgenutzt. Bei den Opfern handelt es sich hauptsächlich um westeuropäische und US-amerikanische Firmen.

Interessant ist dabei die automatisierte Suche nach *OPC-Servern* lokal und im Netzwerk. Durch Manipulationen an OPC-Servern lassen sich die damit gesteuerten physischen Prozesse stören. Dazu verfügt die Malware über die Fähigkeit, OPC-Systeme mit Hilfe von *Fingerprints* zu identifizieren und überträgt Informationen bezüglich gefundenen Systemen zum *Command and Control Server (C&C-Server).*

Die Kampagne ist primär auf Spionage ausgelegt. Es sollte jedoch gleichwohl eine nachhaltige Präsenz in den Zielsystemen und –netzwerken etabliert und die Möglichkeit für allfällige spätere Sabotageakte bereitgestellt werden.

Durch die Trojanisierung von Herstellersoftware konnten Sicherheitsvorkehrungen auf Seiten der Anwender komplett ausgehebelt werden – solche Softwarepakete sollen ja explizit installiert werden, damit ein Gerät verwendet oder ein Dienst genutzt werden kann.

Diese Kampagne illustriert eindrücklich, wie Angriffe auf kritische Infrastrukturen ablaufen: Durch fokussierte Massnahmen werden Einfallstore in Netzwerke von Betreibern gesucht, um eine Präsenz nahe der Zielsysteme zu etablieren. In der Folge werden möglichst viele Informationen gesammelt (Reconnaissance). Die Angreifer sichern ihren Zugriff, um zu einem späteren Zeitpunkt weiterhin Informationen sammeln und bei Bedarf auch Manipulationen durchführen zu können.

Zur Absicherung der OPC-Schnittstelle gibt es verschiedene Ansätze:

- Einführen und regelmässige Aktualisierung von *ACLs (Access Control Lists*) zwischen den OPC-Clients und -Servern unter Berücksichtigung von *Least Privilege*.

[22] http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat (Stand: 1. September 2014).

[23] http://www.crowdstrike.com/sites/all/themes/crowdstrike2/css/imgs/platform/CrowdStrike_Global_Threat_Report_2013.pdf (Stand: 1. September 2014).

[24] http://www.kaspersky.com/about/news/virus/2014/crouching-yeti-an-ongoing-spying-campaign-with-2800-highly-valuable-targets-worldwide (Stand: 1. September 2014).

- Abschotten von *RPC-Kommunikation* in separaten Netzen und mit Punkt-Punkt Verbindungen.
- *Tunneling* von solchen Verbindungen.
- Überwachung von Zugriffen (zentrales Logging und regelmässige Überwachung der Zugriffslogs).
- Wenn die Software digital signiert ist, sollten auch die Signaturen vor einer Installation geprüft werden.

Generell empfiehlt MELANI, Industriesteuerungen von der üblichen IKT-Infrastruktur möglichst stark abzuschotten und auch vor direkten Angriffen zu härten, siehe auch MELANI-Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS).[25]

## 4.4 Konflikte im Cyberspace

Neben dem Nahostkonflikt, in welchem Israel von arabischen Hacktivisten angegangen wird, und dem andauernden Auftreten der «Syrian Electronic Army» zur Unterstützung des Assad-Regimes, gibt nun auch die Ukrainekrise verschiedenen Akteuren Anlass für Operationen im Cyberspace. Vor und während dem Einmarsch von bewaffneten Truppen auf der Krim, Ende Februar 2014, wurden die Mobiltelefonie und der Internetzugang auf der Halbinsel durch physische Eingriffe in die Telekommunikationsinfrastruktur und möglicherweise auch durch Cyberangriffe gestört. Kurz darauf waren auch Webseiten der ukrainischen Regierung temporär nicht mehr verfügbar und verschiedene Parlamentarier beklagten sich über Probleme bei der Verwendung ihrer Mobiltelefone. Nachdem in Russland Anfang März Webauftritte von Regierungskritikern abgeschaltet wurden, griffen Hacktivisten Webseiten des Kremls an, so dass diese zeitweise nicht mehr erreichbar waren. Gleiches haben (andere) Hacktivisten mit Webseiten der NATO gemacht.

Darüber, inwiefern auch die im vorigen Kapitel beschriebenen Angriffe auf westliche Industrieanlagen unter diese Thematik fallen, kann zum aktuellen Zeitpunkt nur spekuliert werden. In den Vereinigten Staaten wird seit einiger Zeit ein Szenario bearbeitet, in welchem eine fremde Macht die amerikanische Energieversorgung infiltrieren könnte, um den USA bei Bedarf den Strom abzuschalten.

Wie bereits in früheren Halbjahresberichten aufgezeigt, bewirken Konflikte in der physischen Welt immer häufiger auch Aktionen und Reaktionen im Cyberspace. Insbesondere dann, wenn eine Konfliktpartei nicht oder nur schwerlich mit konventionellen Mitteln angreifbar ist – sei dies, weil ein physischer Angriff zur Eskalation der Situation führen würde oder weil der «Gegner» sich nicht in Reichweite für eine solche Aktion befindet oder schlicht weil die Ausübung physischer Angriffe an der Asymmetrie des Gewaltpotenzials scheitert – ist ein Cyberangriff ein naheliegendes Mittel, um dem Kontrahenten zu schaden oder zumindest um Missfallen auszudrücken.

Staaten, deren Wirtschaft und/oder kritische Infrastrukturen stark von der funktionierenden IKT abhängig und deshalb in diesem Bereich verletzlich sind, können durch Cyberangriffe auch von kleinen Personengruppen oder gar Einzeltätern massiv geschädigt werden.

Schliesslich ist bei Aktionen im Cyberspace auch der Aspekt der Informationsverbreitung (Propaganda) durch die beteiligten Parteien und weitere Interessenvertreter zu

[25] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=de (Stand: 1. September 2014).

berücksichtigen, denn in jedem Konflikt hat einen Vorteil, wer die Informationssphäre dominiert oder gar kontrolliert.

## 4.5 NSA – die weiteren Veröffentlichungen

Die Berichterstattung rund um Snowden und die NSA-Affäre ging auch im ersten Halbjahr 2014 auf kleinerer Stufe weiter. Dennoch möchten wir an dieser Stelle die wichtigsten Veröffentlichungen kurz zusammenfassen. Die ersten Auswirkungen der veröffentlichten Dokumente auf die Entwicklungen im Internet sind in Kapitel 5.3 aufgeführt

*USA halten Sicherheitslücken in Computersystemen geheim*

In einer Publikation aus dem Snowden-Fundus wurde behauptet, dass die NSA gefundene Sicherheitslücken in Software oftmals für ihre Zwecke ausnutzt. Ein Berater von US-Präsident Obama erklärte hierzu, dass es durchaus Kriterien gebe, ob eine Sicherheitslücke öffentlich gemacht werde oder nicht. Durch deren Ausnutzung könnten auch wichtige Informationen gewonnen werden. Kriterien, ob eine Sicherheitslücke für Spionagezwecke verwendet wird oder nicht, sind beispielsweise, wie weit verbreitet die Technologie ist und ob jemand anderes die Schwachstelle entdecken und ausnützen kann. Es gebe auch die Möglichkeit, eine Lücke zuerst auszunutzen und anschliessend publik zu machen.[26]

Diese Erkenntnis ist nicht neu. Bereits 2005 wurde eine Spionagekampagne beobachtet, die systematisch Schwachstellen in Microsoft-Produkten ausnutzte. Als Ursprung wurde damals China vermutet.[27]

*NSA soll per Post verschickte US-Netzwerktechnik manipuliert haben*

Eine weitere Veröffentlichung der beiden Journalisten und Anwälte, Glenn Greenwald und Jacob Appelbaum, machte publik, dass die NSA «teilweise» per Post verschickte Netzwerkgeräte und Peripheriegeräte abfange, um darauf Spionagesoftware zu installieren. Mitarbeiter der «Tailored Access Operations (TAO)» würden dann in diese Geräte spezielle Technik einbauen, die Spionagemöglichkeiten erlaubt. Danach würden diese wieder verpackt und an den Empfänger verschickt. Betroffen sind Greenwald zufolge auch Router und Server von Cisco, einer US-Firma, welche einen grossen Teil der weltweit verwendeten Netzwerkkomponenten herstellt und einsetzt.[28] Erwähnenswert ist, dass in den letzten Jahren die USA verlauten liessen, den chinesischen Firmen Huawei und ZTE, welche ebenfalls Netzwerkkomponenten produzieren, sei nicht zu trauen.[29] Konkret ging es um die Gefahr, dass die Technologie der beiden Firmen eingesetzt werden könnte, um US-amerikanische Netzwerke auszuspionieren.

---

[26] http://www.tagesanzeiger.ch/digital/internet/USA-halten-Sicherheitsluecken-in-Computersystemen-geheim/story/12638578 (Stand: 1. September 2014).

[27] MELANI Halbjahresbericht 2006/1, Kapitel 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/00162/index.html?lang=de (Stand: 1. September 2014).

[28] http://www.droemer-knaur.de/buch/7943698/die-globale-ueberwachung (Stand: 1. September 2014). http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html (Stand: 1. September 2014).

[29] http://www.spiegel.de/netzwelt/netzpolitik/us-kongress-will-chinas-telekom-firmen-huawei-und-zte-aussperren-a-860014.html (Stand: 1. September 2014).

Das US-Repräsentantenhaus hat im Juni 2014 einem Gesetzesentwurf zugestimmt, der es der NSA und der CIA verbieten würde, Sicherheitslücken oder Hintertüren in inländischen IT-Produkten oder Dienstleistungen zwecks Überwachung zu finanzieren.[30] Ebenfalls verboten würde laut dem Entwurf die gängige und publik gewordene Praxis, dass bereits gesammelte und erhaltene Daten im Nachhinein auch nach US-Bürgern durchsucht werden dürfen. Das Geschäft muss aber zuerst noch durch den Senat.

*Landesweite Aufzeichnung von Telefondaten*

Bekannt wurde ebenfalls, dass unter dem Codenamen «Somalget» Mobilfunkgespräche von ganz Bahamas abgehört werden. Mindestens bei einem anderen Land sollen ebenfalls flächendeckend Telefongespräche abgehört werden. «Somalget» gehört zum Programm «Mystic», bei dem Informationen über Telefonanrufe in Mexico, den Philippinen und Kenia gesammelt werden.[31] Der Unterschied ist allerdings, dass bei «Mystic» nur Metadaten aufgezeichnet werden, bei «Somalget» auch Inhalte. Anscheinend wurde eine Kooperation zwischen den Behörden Bahamas und der US-amerikanischen «Drug Enforcement Administration (DEA)», welche zwecks Drogenbekämpfung bei der Überwachung einzelner Anschlüsse zusammenarbeiten, von der NSA für einen Komplettzugriff auf das Mobilfunknetz genutzt.

*Beeinflussung des Standard bei Gesprächsverschlüsselung*

Im ersten Halbjahr 2014 wurden Dokumente veröffentlicht, wonach das Government Communications Headquarters (GCHQ), das britische Pendant zur NSA, beim Mobilfunkstandard A5/1 von Anfang an kurze Schlüssel durchgesetzt haben soll. Während zuerst Schlüssel von 128-*Bit* Länge vorgeschlagen wurden, habe das GCHQ in den achtziger Jahren auf einen Schlüssel von 48-Bit gedrängt. Schliesslich einigte man sich auf einen Kompromiss und verwendete einen 64-Bit-Schlüssel bei dem zehn Stellen immer Null sind. Damit soll der Algorithmus A5/1 von Anfang an leicht zu knacken gewesen sein.[32] Die ersten Angriffe wurden bereits im Jahre 2000 bekannt.[33] Der 25 Jährige Standard wird noch heute verwendet und wird erst langsam durch den Nachfolger A5/3 ersetzt.

Im letzten Jahr machte in diesem Zusammenhang vor allem der Standard «Dual_EC_DRBG» Schlagzeilen, ein von der NSA entwickelter Zufallszahlengenerator, der die Zahlen nicht so zufällig liefert, wie er es eigentlich sollte.

*NSA und GCHQ haben angeblich Zugriff auf Userdaten von Apps*

Dass diverse Daten von Smartphone-Applikationen, so genannten Apps, an deren Betreiber weitergeleitet werden, ist nichts Neues. Wir haben bereits im MELANI-Halbjahresbericht 2011/2[34] darauf hingewiesen, dass die Rechte, die eine App durch den Benutzer wissentlich oder unwissentlich erhält, mitunter über das hinaus geht, was die App auch wirklich für ein reibungsloses Funktionieren benötigt. Neu dazu gekommen ist nun laut einem Bericht in der «New York Times», dem «Guardian» und der «ProPublica», dass auch NSA und GCHQ

---

30 http://thehill.com/blogs/floor-action/house/210027-house-votes-to-limit-nsa-spying (Stand: 1. September 2014).

31 https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (Stand: 1. September 2014).

32 http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html#.UtFDAvZuTGK (Stand: 1. September 2014).

33 http://de.wikipedia.org/wiki/A5_%28Algorithmus%29 (Stand: 1. September 2014).

34 MELANI Halbjahresbericht 2011/2, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01141/index.html?lang=de (Stand: 1. September 2014).

diese Daten abfangen, welche die Smartphone-Apps über ihre Nutzer sammeln. Neben einfachen Daten über Alter, Geschlecht und Aufenthaltsort eines Nutzers können so unter Umständen auch komplexe Profildaten enthalten werden. Der Wert solcher Daten ist entsprechend hoch, so dass die NSA anscheinend mehr als eine Milliarde US-Dollar für dieses Programm ausgegeben haben soll. Zudem bezeichnet die NSA in einer der veröffentlichten Folien den vermehrten Gebrauch von Smartphones als Glücksfall.

*WLAN im Flughafen – Kanadischer Geheimdienst soll Netz überwachen*

Im Zeitalter der Mobilkommunikation ist eine der ersten Handlungen nach Verlassen des Flugzeuges, das Mobiltelefon zu starten und seine E-Mails zu checken oder andere Informationen herunterzuladen - dies vorzugsweise über ein vom Flughafen zur Verfügung gestelltes *WLAN*. Genau hier setzte anscheinend der kanadischen Geheimdienst Communications Security Establishment Canada (CSEC) an und verwendete das WLAN in einem kanadischen Grossflughafen, um Personen im Land zu lokalisieren. Bei jedem Verbinden auf ein öffentliches Netzwerk werden *Metadaten* übermittelt, welche es erlauben, das Gerät zu einem späteren Zeitpunkt wieder zu identifizieren. Die am Flughafen erhaltenen Daten können so verwendet werden, um Zielpersonen digital zu verfolgen.[35]

*NSA ist in der Lage, Internetverbindungen umzuleiten*

Gemäss den Veröffentlichungen aus dem Snowden-Fundus soll die NSA im Rahmen des Programms «Qfire» in der Lage sein, beliebige Internetverbindungen zu unterbrechen und umzuleiten. Bei diesen dezentral durchgeführten Angriffen auf Internet-Verbindungen soll die NSA Daten möglichst nahe bei den Zielen abfangen und manipulieren können.[36]

*Auch OSZE soll unter den Zielen der NSA sein*

Gerade internationale Organisationen sind besonders interessant für Spionageangriffe. Auf kleinem Raum sind Mitarbeiter vieler Länder vertreten und es werden zahlreiche elektronische Kommunikationsmittel benutzt. Schon im August 2013 wurde bekannt, dass die Zentrale der Vereinten Nationen in New York durch die NSA abgehört worden sei.[37] Nun wurde von der österreichischen Tageszeitung «Die Presse» publiziert, dass auch die OSZE in Wien auf der Zielliste der US-Nachrichtendienste aufgeführt gewesen sein soll.[38] Dies unter Berufung auf einen deutschen Journalisten, welcher Einblick in die Unterlagen von Snowden hatte. Vor allem «aussenpolitische Ziele» und «Waffenkontrolle und Waffenhandel» sollen in dem Dokument erwähnt sein.

## 4.6 Wie Betrüger aktuelle Ereignisse für ihre Zwecke missbrauchen

Vorschussbetrug ist ein allgemein bekanntes und gut dokumentiertes Phänomen. Die Betrüger bereiten ein Szenario vor, bei dem das Opfer angeblich eine grosse Summe

---

35 http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881 (Stand: 1. September 2014).

36 http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigng-der-nsa-fotostrecke-105358.html (Stand: 1. September 2014).

37 http://www.spiegel.de/politik/ausland/nsa-hoerte-zentrale-der-vereinte-nationen-in-new-york-ab-a-918421.html (Stand: 1. September 2014).

38 http://diepresse.com/home/politik/aussenpolitik/3809719/NSAAffaere_Obama-laesst-OSZE-ausspionieren (Stand: 1. September 2014).

erhalten soll, beispielsweise durch eine Erbschaft, ein nachrichtenloses Konto oder einen Lottogewinn. Wenn auf den Erstkontakt eine Antwort erfolgt, müssen dann erst einmal verschiedene Anzahlungen getätigt werden, natürlich ohne dass die versprochene Summe jemals ausbezahlt wird. Ein Merkmal, welche diese Betrugsart auszeichnet, ist die grosse Anpassungsfähigkeit der Betrüger gegenüber dem Opfer oder die Umgebung und die Art, wie sie sich die Aktualität zunutze machen, um ihre Opfer besser zu täuschen. Sehr beliebt war dieses Jahr bei Betrügern beispielsweise das Thema Fussballweltmeisterschaft in Brasilien. Die begehrten Tickets und das besondere Ereignis boten ein fruchtbares Terrain für Szenarien, bei denen die Angreifer den Opfern beispielsweise gefälschte Tickets über das Internet anboten, natürlich erst nach einer vorgängigen Überweisung. Auch hier ging es darum, Geld zu ergaunern und persönliche Angaben auszuspionieren.

Das Flugzeugunglück der Malaysia Airlines Maschine im Frühjahr 2014 und die Verwirrung nach deren Verschwinden boten ebenfalls Anlass für verschiedene Betrügereien. Verbreitet waren insbesondere Links in den sozialen Netzwerken auf ein Video mit dem angeblich gefundenen Flugzeug. Wer darauf klickte, riskierte seinen Computer zu infizieren, da er statt auf das Video auf eine Seite mit einem Virus gelangte. In einigen Fällen wurden die Opfer auch auf Phishingseiten gelotst, wo sie Angaben zu Bankzugangsdaten machen sollten, um an den gewünschten Inhalt zu kommen.

Betrüger, welche im Internet aktiv sind, zeichnen sich oft durch grosse Anpassungsfähigkeit aus. Insofern sind Ereignisse mit grossem medialem Echo weltweit für sie ein gefundenes Fressen. Sie nutzen diese für Szenarien, um das Interesse ihrer Opfer zu wecken. Internetnutzer müssen deshalb gegenüber spontanen Angeboten besonders vorsichtig sein. Bevor sie einem Link folgen, einen Anhang öffnen oder persönliche Informationen angeben, sollten sie sich immer vergewissern, dass die Nachricht sicher und der Absender vertrauenswürdig ist. Im Zweifelsfalle gilt es, das E-Mail zu löschen.

## 4.7 Störungen der Flugsicherung durch Militärübung?

Am 5. und 10. Juni 2014 kam es in Mittel- und Osteuropa stellenweise zu Ausfällen des Radarkontaktes der Zivilluftfahrt, die 20 respektive 25 Minuten lang dauerten. Betroffen war dabei der Sekundärradar, welcher Daten des Transponders des Flugzeugs, wie Kennung und Höhe, übermittelt. Die Position der Flugzeuge war hingegen sichtbar. Auch der Funk zu allen Flugzeugen war stets gewährleistet.

Kurz danach wurde die Vermutung laut, dass eine von der Nato abgehaltene Militärübung in Ungarn und Italien Schuld am Ausfall des Sekundärradars war. Die Nato bestätigte, dass sie das lokale Stören bestimmter Frequenzen geübt habe, dass es aber höchst unwahrscheinlich sei, dass die Störungen von den Nato-Übungen verursacht worden waren. Die bei der Übung gestörten Frequenzen unterscheiden sich von den Frequenzen der zivilen Luftfahrt. Die europäische Flugsicherungsbehörde Eurocontrol untersucht nun die Vorfälle.

Nach heutigen Erkenntnissen ist die Wahrscheinlichkeit einer soft- respektive hardwarebasierten Fehlfunktion oder sogar einer Manipulation der Radargeräte gering. Ansonsten wäre es schwierig zu erklären, wieso Flugsicherungen verschiedener Länder und mit diversen Gerätschaften das gleiche Phänomen beobachtet haben. Eine externe Störung dürfte hier sicherlich plausibler sein. Auch wenn ein vorläufiger Bericht von Eurocontrol

davon ausgehe, dass die Frequenzen zwischen Militär und Zivilluftfahrt genügend getrennt waren[39], ist die örtliche und auch zeitliche Korrelation der Ereignisse mit der Übung frappant.

## 4.8 Passwörter entdeckt und gestohlen

*Bundesamt für Sicherheit in der Informationstechnik entdeckt 34 Millionen gestohlene Passwörter*

Ende Januar 2014 publizierte das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI), dass bei der Analyse eines *Botnetzwerks* 16 Millionen Zugangsdaten, bestehend aus E-Mail-Adresse und Passwort, entdeckt worden sind.[40] Diese Zugangsdaten gehören zu allen Arten von Online-Konten, bei denen eine E-Mail-Adresse als Benutzername verwendet werden kann. Die Zugangsdaten wurden anscheinend über Computer erlangt, welche mit Schadsoftware infiziert worden sind. Jedes Mal, wenn eine E-Mail/Passwortkombination über einen solch kompromittierten Computer eingegeben wird, werden Zugangsdaten gestohlen und an einen zentralen Server unter der Kontrolle der Kriminellen übermittelt.

Anfang April 2014 hat das BSI die Öffentlichkeit über einen weiteren Passwortfund informiert. Diesmal waren 18 Millionen Benutzerdaten betroffen.[41] Nebst der bereits seit Januar 2014 installierten URL[42], auf welcher man die E-Mail-Adresse überprüfen konnte, wurden diesmal auch weitere Möglichkeiten der Benachrichtigung berücksichtigt. So wurden entsprechende Informationen auch an E-Mail-Provider wie GMX und Web.de weitergeleitet, die dann betroffene E-Mail-Konten mit einem Hinweis auf den Datenklau sperrten. Bei beiden Vorfällen waren auch Schweizer E-Mail-Konten betroffen.

*Datendiebstahl bei E-Bay*

Im vergangenen Mai räumte Ebay in einem Communiqué einen Angriff ein, bei dem Betrüger an eine Datenbank mit Kundendaten gelangen konnten. Die Angreifer sollen so Zugriff auf Mailadressen, verschlüsselte Passwörter , Postadressen und Telefonnummern erhalten haben, offenbar aber nicht auf Kreditkartendaten. Die Zahl der kompromittierten Daten wurde nicht bekanntgegeben. Auch wenn nichts dafür spricht, dass die Angreifer die Passwörter entschlüsseln konnten, empfahl Ebay den Kunden diese nicht mehr zu verwenden.

Eine zentrale Frage bei diesem Vorfall war der Eintrittspunkt des Angriffs. Ebay bestätigte bereits im Februar, dass Zugangsdaten bei Mitarbeitern des Unternehmens gestohlen worden waren. Mit diesen Daten gelangten die Angreifer dann ins Netzwerk des Unternehmens. Die Art, wie die Betrüger an die Mitarbeiterdaten gelangten, ist allerdings nicht bestätigt. Einige Experten gingen aber davon aus, dass der Angriff mindestens zum Teil mittels Social Engineering erfolgte. Dies scheint bisher die plausibelste Annahme zu sein. Auch da könnte *Spear Phishing* eingesetzt worden sein.

---

39 http://www.n24.de/n24/Nachrichten/Politik/d/5260064/militaeruebungen-koennten-radar-gestoert-haben.html (Stand: 1. September 2014).

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Mailtest_21012014.html (Stand: 1. September 2014).

41 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html (Stand: 1. September 2014).

42 https://www.sicherheitstest.bsi.de/ (Stand: 1. September 2014).

Der Vorfall zeigt, dass eine ursprüngliche Kompromittierung im kleinen Stil unter Umständen grosse Konsequenzen haben kann und die Angreifer sich so den Zugang zu einem ganzen Netzwerk und allem, was es enthält – vor allem zu den Datenbanken – verschaffen können. Es lohnt sich deshalb für Cyberkriminelle, grössere Ressourcen für das Ausspionieren einzelner Konten in einem Unternehmen zu investieren, über die sie dann Zugriff auf wichtigere Informationen bekommen. Für die Unternehmen bedeutet das, möglichst wenige Accounts mit erweiterten Privilegien auszustatten und diese auf ungewöhnliche Aktivitäten hin zu überwachen.

## 4.9 Neue DDoS Varianten

Denial-of-Service Attacken haben zum Ziel, bestimmte Dienste für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Solche *DDoS Angriffe* sind weit verbreitet und stellen eine ernst zu nehmende Bedrohung für viele IKT-Infrastrukturen dar. Nebst den bekannten «*DNS-Amplification/Reflection»-Angriffen*, bei denen für jedermann zugängliche *DNS-Server* für den Angriff missbraucht werden, sind in den letzten Monaten diverse neuere Techniken aufgetaucht. So werden andere offen zugängliche Dienste auf ähnliche Weise missbraucht. Beispiele sind das einfache Netzwerkverwaltungsprotokoll (Simple Network Management Protocol, *SNMP)*, das Network Time Protocol *NTP,* welches für die Zeitsynchronisation innerhalb eines Netzes verwendet wird oder das Character Generator Protocol (Chargen), welches zur Fehlersuche verwendet wird. Typisch für diese Angriffsarten ist, dass eine kleine Anfrage eine um ein Vielfaches grössere Antwort erzeugt, die dann auf das tatsächliche Angriffsziel gelenkt wird. Die Dienste basieren auf dem *User Datagram Protocol (UDP)* , welches für DDoS Angriffe sehr beliebt ist, da das Protokoll verbindungslos ist und keine Validierung der an der Kommunikation beteiligten *IP-Adressen* beinhaltet.

Der Missbrauch von NTP-Servern mit Hilfe des «monlist»-Befehls wurde bereits im MELANI Halbjahresbericht 2013/2[43] angesprochen, ist aber nach wie vor aktuell. Dieser Befehl gibt eine Liste mit den 600 *IP-Adressen* heraus, welche sich zuletzt auf den NTP-Server verbunden haben. Wird dieser Befehl mit einer gefälschten IP-Adresse abgesetzt, prasseln die Antworten auf das unschuldige Opfer ein, dessen IP-Adresse gefälscht worden ist. Bei den grössten DDoS-Angriffen im Frühjahr 2014 wurden Bandbreiten von mehr als 400Gb/s gemessen. SNMP bietet eine ähnliche hohe Amplifikationsmöglichkeit und wird bereits aktiv missbraucht.

Eine neue Variante von DDoS-Angriffen missbraucht eine Funktion in der weitverbreiteten *Blog/CMS Software* Wordpress. Diese verfügt über eine Funktion «*PingBack»*, welche es erlaubt eine Benachrichtigung einzufordern, sobald die eigene Seite verlinkt wird. Missbraucht ein Angreifer diese Funktion und sendet die Adresse seines Opfers an eine Vielzahl von Wordpress-Instanzen senden diese entsprechende *HTTP* Anfragen an die Opferseite, welche unter der Flut von Anfragen zusammenbricht. Der ursprüngliche Angreifer ist dabei für das Opfer praktisch unsichtbar, da es von vielen Tausend legitimen Wordpress-Installationen attackiert wird. Bei einem Angriff wurden dabei über 160'000 verschiedene Wordpress-Sites beobachtet, die für den DDoS-Angriff missbraucht worden sind.

Generell empfiehlt MELANI, die Systeme so zu schützen, dass sie nicht für DDoS-Angriffe missbraucht werden können. Dazu gibt es im Internet entsprechende Ressourcen, wie z. B.

[43] MELANI Halbjahresbericht 2013/2, Kapitel 3.10: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 1. September 2014).

von «Team Cymru» für das Absichern der DNS-Server oder von NTP-Servern.[44] Die Absicherung von Wordpress-Instanzen ist nicht einfach, da das «PingBack» prinzipiell ja ein erwünschtes Feature des Systems ist. Es gibt jedoch die Möglichkeit, ein entsprechendes Filterplugin zu erstellen, welches die Funktion ausschaltet.

Für *Internet Service Provider (ISP)* ist die Implementation von BCP 38[45] (Best Current Practice) ein zentrales Element, um die DDoS-Problematik mittel- bis langfristig lösen zu können. BCP 38 legt dabei fest, wie ein Netzwerk vor unerwünschtem eingehendem Verkehr (Pakete mit gefälschten oder fehlerhaften IP Adressen) geschützt wird (*Ingress Filtering*).

## 4.10 Angriffe auf virtuelle Währungen

Die dezentrale virtuelle Währung Bitcoin war bereits im letzten MELANI-Halbjahresbericht ein Thema[46]. Sicherheitsfragen rund um diese Währung wurden dort thematisiert: Diebstahl privater Schlüssel, Angriffe auf Handelsplattformen oder Malware, die Bitcoins beim Nutzer stehlen oder dessen Rechner für das Mining missbrauchen.

Bitcoin bleibt auch 2014 aktuell, insbesondere auch in Bezug auf solche Sicherheitsfragen. So waren Android-Nutzer Ziel entsprechender Malwareattacken und Google musste mehrere Apps vom Play-Store zurückziehen, die vom Smartphonebesitzer unbemerkt Bitcoins und andere ähnliche Währungen «schürften». Die steigenden Nutzerzahlen und der entsprechend höhere Bedarf an Miningressourcen sind der Grund, dass Kriminelle vermehrt versuchen, an zusätzliche Rechenkapazitäten zu kommen. Dies geschieht vor allem über Mobiltelefone. Für den Nutzer sind Leistungsverluste des Geräts und rasch leere Akkus Hinweise darauf, dass die Ressourcen abgezapft sein könnten. Dieser Modus Operandi wird jedoch von vielen Experten in Anbetracht der Zeit, die es für das Mining braucht, als bisher wenig rentabel eingeschätzt.

Plattformen, auf denen traditionelles Geld gegen Bitcoins getauscht wird, waren dieses Jahr ebenfalls weiter unter Druck. Wie im letzten Halbjahresbericht dargelegt, stellen diese Handelsplattformen ein beliebtes Ziel für Angriffe dar. Der Konkurs von Mt. Gox im ersten Halbjahr 2014 zeigt die Bedeutung und Verwundbarkeit dieser Börsen auf. Mt. Gox, eine der ersten und grössten Plattformen auf dem Markt, hat am 7. Februar 2014 die Tätigkeit eingestellt und Ende des Monats dann in Japan Konkurs angemeldet. Sie soll 750 000 Bitcoins von Kunden sowie 100 000 eigene Bitcoins verloren haben, was zum damaligen Zeitpunkt einem Wert von 620 Millionen Dollar entsprach. Ein Grund für den Verlust sollen Schwächen der Plattform und daraus folgend betrügerische Transaktionen gewesen sein. Einige Experten sind aber der Ansicht, dass dies nicht die einzige Erklärung für das Ende war. Fehlendes Management bei Mt. Gox sowie mögliche andere Hackermethoden, um an Bitcoins zu gelangen, sind weitere Möglichkeiten, die die Verluste erklären könnten.

Bitcoins und virtuelle Währungen stehen weiterhin im Fokus, vor allem hinsichtlich Sicherheit und Zuverlässigkeit. Neben dem Interesse der Strafverfolgungsbehörden auf internationaler Ebene, versuchen einzelnen Staaten, den Rechtsstatus virtueller Währungen zu klären. In der Schweiz enthält ein kürzlich erschienener Bericht des Bundesrats eine

[44] http://www.team-cymru.org/ReadingRoom/Tips/dns.html (Stand: 1. September 2014).

[45] http://tools.ietf.org/html/bcp38

[46] MELANI Halbjahresbericht 2013/2, Kapitel 5.2: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 1. September 2014).

Bestandsaufnahme der virtuellen Währungen, ihrer Funktionsweise und der Fragen und Probleme im Zusammenhang mit diesen[47].

## 4.11 Erfolge gegen Betrüger

Auch im ersten Halbjahr 2014 gab es einige Erfolge im Kampf gegen Betrüger und Hacker zu verzeichnen.

*Razzia gegen Besitzer der Schadsoftware Blackshades*

Am 20. Mai 2014 fand eine Razzia gegen die Besitzer der Spionagesoftware «Blackshades» statt. Bei der vom Federal Bureau of Investigation (FBI) initiierten Aktion gab es in 19 Ländern bei mehr als 300 angeblichen Besitzern dieser Schadsoftware eine Hausdurchsuchung.[48] Gegen 100 Personen wurden verhaftet, darunter auch der mutmassliche Drahtzieher Alex Yucel. Bei der Schadsoftware Blackshades können Windows-Rechner fast unbeschränkt aus der Ferne kontrolliert werden. Deren Nutzer dürften die Spionagesoftware für verschiedenste Zwecke eingesetzt haben. Die Malware wurde auch bei Oppositionsmitgliedern in Syrien und Libyen entdeckt.

*Spiel aus für GameOver Zeus*

Am 2. Juni 2014 teilte das US. Department of Justice (DOJ) und das FBI die Deaktivierung der beiden *Botnetzwerke* «GameOver ZeuS (GOZ)» und «CryptoLocker» mit.[49] GOZ ist eine Weiterentwicklung der Schadsoftware ZeuS / Zbot, seit vier Jahren auch in der Schweiz aktiv und eines der wenigen Botnetzwerke, das auf Peer2Peer-Technik basiert. Ziel der Botnetzwerke war es E-Banking-Betrug zu betreiben oder Computernutzer zu erpressen (*Ransomware*). Bereits seit Juli 2013 hat MELANI zusammen mit den Schweizer *Internetprovidern* Massnahmen gegen die Bedrohung ausgehend von Cryptolocker ergriffen.

Die IT-Sicherheitsdienstleister FireEye und Fox-IT haben nach der Deaktivierung des Cryptolocker Botnetzwerks einen Gratis Service zur Verfügung gestellt, der es Opfern ermöglicht, die durch die Schadsoftware verschlüsselten Daten wieder zurückzuerlangen.[50]

*Verhaftung mit Schweizer Hilfe*

Anfang März 2014 verhaftete die thailändische Polizei mit Schweizer Hilfe den mutmasslichen Hacker «Diab10» in Bangkok, welcher 2005 unter anderem den Computerwurm «Zotob» in Umlauf gebracht haben soll.[51] Dieser legte damals zahlreiche Rechner lahm. Der gebürtige Marokkaner mit russischem Pass wurde in der Schweiz wegen «betrügerischen Missbrauchs einer Datenverarbeitungsanlage» gesucht. Der Verhaftete, gegen den in der Schweiz ein Haftbefehl vorliegt, wird an die Schweiz ausgeliefert.

---

47 http://www.admin.ch/aktuell/00089/?lang=fr&msg-id=53513 (Stand: 1. September 2014).

48 http://www.fbi.gov/news/stories/2014/may/international-blackshades-malware-takedown/international-blackshades-malware-takedown (Stand: 1. September 2014).

49 http://www.abuse.ch/?p=7822 (Stand: 1. September 2014).

50 http://www.melani.admin.ch/dienstleistungen/archiv/01583/index.html?lang=de (Stand: 1. September 2014).

51 http://www.nzz.ch/aktuell/panorama/hacker-diab10-in-thailand-verhaftet-1.18265704 (Stand: 1. September 2014).

# 4.12 Verwundbarkeiten von cyber-physischen Systemen

*Schadsoftware in japanischem Kernkraftwerk*

Auf einem Computer im Kontrollraum des japanischen Kernkraftwerks Monju wurde Anfang 2014 eine Schadsoftware festgestellt. Infiziert wurde die Maschine vermeintlich durch das Update von Gratis-Videosoftware, welches ein Mitarbeiter vorgenommen hatte. In der Folge sind rund 42‘000 E-Mails sowie Unterlagen von Mitarbeitertrainings nach respektive via Südkorea abgeflossen. Entdeckt wurde die Infektion durch das Netzwerk-Monitoring, bei welchem Verbindungen zu einer unbekannten Webseite auffielen.

Aus der Berichterstattung ist nicht ersichtlich, ob der betroffene Computer nur für administrative Zwecke gebraucht wurde oder ob er auch für die Steuerung kritischer Prozesse des Kraftwerks gedacht war. Zudem ist nicht klar, ob der Computer auch bei regulärem Betrieb des Reaktors – das Kraftwerk war zu diesem Zeitpunkt nicht in Betrieb – über einen Internet-Anschluss verfügt hätte und wie er in diesem Fall von den operativen Systemen des Kontrollraums getrennt ist. Laut dem Betreiber war die Reaktorsicherheit durch diesen Zwischenfall zu keiner Zeit gefährdet.

Der Reaktor vom Typ «schneller Brüter» musste bereits 1995 kurz nach seiner Inbetriebnahme wegen eines Brandes wieder abgeschaltet werden. Im Frühling 2010 wurde der Testbetrieb wieder aufgenommen. Ein Unfall bei der Brennstoffbefüllung führte weniger als vier Monate später schliesslich zur erneuten und wohl definitiven Abschaltung.

Auch wenn es sich bei diesem Vorfall nicht um einen gezielten Angriff auf ein Kernkraftwerk handeln dürfte, sondern um eine zufällige Infektion, ist doch bedenklich, dass ein Computer im Kontrollraum, in welchem der Betrieb des Reaktors gesteuert wird, mit Schadsoftware infiziert werden kann. Operative und administrative Netzwerke sollten so stark wie möglich voneinander abgeschottet sein – insbesondere wenn die Prozesse, die gesteuert werden, ein so hohes Gefährdungspotenzial haben wie bei der nuklearen Energiegewinnung.

*Computerbasierte Medizintechnik und Sicherheitslücken*

Der Sicherheitsforscher Scott Erven hat während zwei Jahren elektronische medizinische Geräte in amerikanischen Spitälern überprüft und stellte dabei zum Teil verheerende Mängel fest. Diese betrafen hauptsächlich eingebettete Webdienste, welche den Geräten erlauben, miteinander zu kommunizieren und Daten direkt in Patientendossiers zu senden. Dabei waren die Probleme weniger bei der grundsätzlichen Programmierung von Software zu suchen, sondern eher bei der Implementierung der Systeme. Häufig waren Geräte nur durch schwache oder unveränderbare Standardpasswörter geschützt, übermittelten Patientendaten unverschlüsselt im Netzwerk oder liessen sich durch das Senden von sinnlosen, das heisst dem Gerät unbekannten Befehlen aus dem Konzept bringen.

Man mag sich nicht ausmalen, was passieren könnte, wenn ein Operationsroboter während eines Eingriffs plötzlich seinen Dienst versagt, eine Infusionspumpe die mehrfache (oder eine zu geringe) Menge eines Medikaments abgibt oder ein Herzschrittmacher dem Träger im falschen Moment Elektroschocks versetzt. Auch Manipulationen an Röntgengeräten oder Computertomographen, welche die Abgabe einer zu hohen Strahlendosis zur Folge haben, könnten vorgenommen werden. Neben direkter Einflussnahme auf medizintechnische Geräte ist auch im Spitalumfeld die zunehmende Vernetzung der Hausautomation ein Risiko: Wenn bei Kühlsystemen für Blutkonserven oder Medikamenten die Temperatur ferngesteuert reguliert werden kann, ist es möglich, die entsprechenden Vorräte verderben zu lassen.

Im Gesundheitsbereich gibt es wie in traditionellen industriellen Anlagen cyber-physische Systeme – Geräte, die einen physischen Prozess über Software steuern. Die

dahinterliegende Administration wird häufig mit gewöhnlichen Computern geführt, welche in ein (zumindest internes) Netzwerk eingebunden sind. Es muss entsprechend auch in Spitälern darauf geachtet werden, dass diese Systeme effektiv vom Internet abgeschirmt sind und weder gezielt noch zufällig mit Schadsoftware infiziert werden können. Bei gezielten Angriffen können normale Computer als Einfallstor ins interne Netzwerk dienen, wenn sie Zugang zum Internet haben.

*Städtische Stromversorgung verwundbar*

Die Stadtwerke einer mittelgrossen deutschen Stadt liessen ein Hacker-Team auf ihre Anlagen los, um die Sicherheit der Strom- und Wasserversorgung zu prüfen.[52] Die Angreifer testeten das ganze Spektrum von Infiltrationsmethoden. Dieses umfasst neben direkten Hacking-Versuchen übers Internet auch das physische Einstecken eines Hotspots an einer relativ einfach zugänglichen Netzwerksteckdose auf dem Betriebsgelände – zum Beispiel im Empfangsbereich oder in Konferenzräumen – über welche man direkt Anschluss ins interne Netz hat. Der einfachste Weg war aber auch hier, mit Social Engineering Methoden einen Mitarbeiter dazu zu bringen, einen präparierten E-Mail-Anhang zu öffnen, wodurch eine Software installiert wurde, welche den Angreifern ein Einfallstor ins interne Netzwerk bietet. Den beauftragten Hackern gelang es schliesslich, die Steuersoftware in der Leitstelle des Stromversorgers soweit zu infiltrieren, dass ihnen die Übernahme der Kontroll- und Steuerfunktionen möglich gewesen wäre. Fazit der Sicherheitsexperten ist, dass die Übernahme der Kontrolle zwar machbar ist – diese aber zu behalten sehr schwierig, da der Verteidiger physischen Zugang zu allen Geräten und deshalb gegenüber dem Angreifer einen entscheidenden Vorteil habe. Auch sind bei den herkömmlichen Versorgungssystemen nach wie vor viele elektro-mechanische Schutzelemente und analoge Anzeigen im Einsatz, welche sich der Kontrolle eines Cyber-Angreifers entziehen. Ein ausgelöster Stromausfall wäre entsprechend wohl nur von kurzer Dauer.

Ein Angreifer, der eine starke Motivation und viel Zeit hat, also genügend Persistenz an den Tag legt, kann in fast jedes System eindringen. Der erste Schritt ist dabei immer die Beschaffung möglichst vieler Informationen über das Unternehmen, seine Mitarbeiter und allenfalls bereits aus öffentlichen Quellen erhältlichen Angaben zum Zielsystem.

Ein System vollständig abzusichern ist leider praktisch nicht möglich. Deshalb sollte man seine Netzwerke effektiv überwachen, damit man Ereignisse umgehend erkennt, schnell eingreifen und den Normalzustand wieder herstellen kann.

## 4.13 Angriffspunkt Router

Wie bereits im letzten Halbjahresbericht (2/2013) berichtet, geraten *Router* immer mehr in den Fokus der Cyberkriminellen. Auch in der aktuellen Berichtsperiode wurden diverse Angriffe auf Router und deren Schwachstellen beobachtet:

Anfang des Jahres bestätigten die Hersteller «Cisco», «Netgear» und «Linksys», dass über eine Sicherheitslücke Konfigurationsdateien des Routers ausgelesen und auch manipuliert werden können.[53] Zudem konnten Passwörter und Zertifikate für *VPN*s bei einigen Geräten

[52] http://heise.de/-2165153; siehe auch die TV-Dokumentation http://www.arte.tv/guide/de/048364-000/netwars-krieg-im-netz (deutsch), http://www.arte.tv/guide/fr/048364-000/netwars-la-guerre-sur-le-net (français) sowie die interaktive Webdoc unter http://netwars-project.com/de/ (deutsch) oder http://netwars-project.com (englisch).

[53] http://www.heise.de/security/meldung/Mysterioese-Router-Backdoor-Viele-tausend-Router-in-Deutschland-haben-eine-Hintertuer-jetzt-testen-2080913.html (Stand: 1. September 2014).

abgegriffen werden. Auf den betroffenen Geräten läuft ein Dienst auf dem *Port* 32764. Unklar war, ob diese Sicherheitslücke nur vom lokalen Netz aus oder auch über das Internet ausgenutzt werden konnte. Erstaunlich ist, dass diese Lücke in diversen Produkten und seit mehreren Jahren existieren soll.

Anfang Februar wurde bekannt, dass Angreifer über Sicherheitslücken im Router der Firma «AVM-Fritzbox» für das Opfer kostenpflichtige Telefonanrufe tätigen konnten. Nachdem zuerst gestohlene Passwörter für diesen Hack im Verdacht standen, wurde später eine Sicherheitslücke vermutet. Nahezu alle Geräte, ob mit oder ohne *Fernzugang*, waren davon betroffen.[54]

Im März warnte der Hersteller «D-Link» seine Benutzer vor einer Sicherheitslücke im Modem DSL-321B und stellte ein entsprechendes Update bereit.[55] Angreifer konnten unter Ausnutzung der Sicherheitslücke über das Internet auf das Gerät zugreifen. Bei den beobachteten Angriffen wurden *DNS-Servereinträge* verändert.[56] So können beispielsweise Opfer beim Aufruf einer Webseite durch den Angreifer auf eine von ihm definierte Webseite umgeleitet werden. Solche Manipulationen können Kriminelle zum Beispiel für das Umleiten von Online-Banking-Sessions nutzen.

Auch ein Fall mit veränderten DNS-Einstellungen machte das «Team Cymru» Anfang März publik. Bei rund 300‘000 Routern wurden laut eigenen Angaben veränderte DNS-Einstellungen entdeckt. Vor allem Router der Firmen D-Link, TP-Link und Zyxel, aber auch Geräte speziell für kleine Büros (SOHO, Small Office, Home Office) standen im Fokus. Auch in diesen Fällen sollen Schwachstellen die Manipulationen ermöglicht haben.

Router werden sowohl automatisiert, von Hand wie auch mit Malware angegriffen. Aus diesem Grund gibt es verschiedene Würmer, welche sich via Infektion von Routern weiterverbreiten. So befällt z. B. der «Moon Wurm» Geräte der Hersteller Linksys und Netgear, indem er eine Verwundbarkeit ausnutzt.

Router stehen immer häufiger im Fokus der Angreifer, da diese oftmals unsichere Konfigurationen oder Sicherheitslücken enthalten. Auf der anderen Seite ist die Sensibilität der Benutzer bezüglich der Sicherheit von Routern noch nicht so gross. Meist wird ein Gerät angeschlossen und dann während der gesamten Lebenszeit nicht mehr gewartet und aktualisiert. Erschwerend kommt hinzu, dass gerade bei älteren Geräten Updates nicht automatisch eingespielt werden können.

MELANI empfiehlt, den Zugang auf die Wartungsinterfaces der Router so stark als möglich einzuschränken. Viele Geräte unterstützen eine Restriktion auf eine *IP-Adresse* aus dem internen Netz. Werden nicht vom Provider gewartete Geräte verwendet, muss der Benutzer selber regelmässig überprüfen, ob Updates für seinen Router vorhanden sind und gegebenenfalls die Aktualisierungen einspielen. Zudem sollten nicht benötigte Dienste deaktiviert werden.

---

http://www.golem.de/news/port-32764-cisco-bestaetigt-backdoor-in-routern-1401-103882.html (Stand: 1. September 2014).
http://www.golem.de/news/dsl-router-netgear-schliesst-endlich-hintertuer-zu-port-32764-1404-105705.html (Stand: 1. September 2014).

54 http://www.heise.de/security/meldung/Hack-gegen-AVM-Router-Fritzbox-Luecke-offengelegt-Millionen-Router-in-Gefahr-2136784.html (Stand: 1. September 2014).

55 http://www.dlink.com/de/de/press-centre/press-releases/2014/march/10/ma_sicherheitspatch-modem-dsl-321b-revision-z1 (Stand: 1. September 2014).

56 http://www.heise.de/security/meldung/Akute-Angriffsserie-auf-D-Link-Modems-2135158.html (Stand: 1. September 2014).

# 4.14 Vorratsdatenspeicherung verstösst gegen EU-Recht

Unter Vorratsdatenspeicherung versteht man die Speicherung von Telekommunikations-Verbindungsdaten durch oder für öffentliche Stellen, ohne dass die Daten aktuell benötigt werden. So kann beispielsweise im Rahmen eines Strafverfahrens zu einem späteren Zeitpunkt herausgefunden werden, welcher Person eine bei einer Tat verwendete IP-Adresse zugeordnet war. Damit die Zuordnung von Informationen im Internet funktioniert benötigt jeder ans Netz angeschlossene Computer lediglich eine unpersönliche IP-Adresse. Unter Vorratsdatenspeicherung fallen zudem Angaben über Telefonanrufe und SMS sowie Standortdaten, wo sich eine Person zum Zeitpunkt der Telefonbenutzung aufgehalten hat.

Gemäss dem Entscheid des Europäischen Gerichtshofs (EuGH) vom 8. April 2014 verstösst das umstrittene EU-Gesetz zur Vorratsdatenspeicherung gegen europäisches Recht und ist ungültig. Die EU-Richtlinie wurde vom EuGH auf die Vereinbarkeit mit dem Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union überprüft. Der EuGH sieht in der Vorratsdatenspeicherung einen besonders schwerwiegenden Eingriff in die Grundrechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten. Gemäss Urteil des EuGH können sehr genaue Schlüsse auf das Privatleben der Personen gezogen werden, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld. Dies löse beim Bürger möglicherweise ein ständiges Gefühl der Überwachung aus.

Zwar anerkennt der EuGH, dass die Bekämpfung schwerer Kriminalität, insbesondere der organisierten Kriminalität und des Terrorismus, von grösster Bedeutung für die Gewährleistung der öffentlichen Sicherheit ist und dass ihre Wirksamkeit in hohem Mass von der Nutzung moderner Ermittlungstechniken abhängt. Das Gericht kommt jedoch gleichzeitig zum Schluss, dass eine dem Gemeinwohl dienende Zielsetzung, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Vorratsdatenspeicherung, wie in der Europäischen Richtlinie 2006/24 vorgesehen, für die Kriminalitätsbekämpfung nicht gerechtfertigt ist. Der Schutz des Grundrechts auf Achtung des Privatlebens verlange, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen. Aufgrund der Formulierung der europäischen Richtlinie führe dies jedoch zu einem Eingriff in die Grundrechte fast der gesamten europäischen Bevölkerung, da sie sich generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie auf sämtliche Verkehrsdaten erstrecke, ohne eine Differenzierung, Einschränkung oder Ausnahme vorzusehen. Weitere Argumentationspunkte waren die fehlende Information der Teilnehmer über die Vorratsdatenspeicherung, sowie das fehlende objektive Kriterium, welches den Zugang der nationalen Behörde zu den Daten beschränke.

Hervorzuheben ist, dass der EuGH zwar die Unverhältnismässigkeit der in der Richtlinie statuierten Vorratsdatenspeicherung festhält, dieser jedoch in seinem Urteil nicht zum Schluss kommt, dass die Vorratsdatenspeicherung überhaupt nicht möglich ist.

Die Reaktionen der EU-Mitgliedstaaten fielen unterschiedlich aus. Es gibt etliche Bestrebungen, um einen Lösungsansatz für eine verfassungskonforme Vorratsdatenspeicherung zu finden, eine wirkliche Alternative besteht jedoch noch nicht. Die EU-Kommission scheint keine neue Richtlinie in dieser Frage anzustreben, so dass wohl einige Mitgliedstaaten ihre Regelungskompetenz in diesem Punkt zurücknehmen werden.

Das EuGH Urteil wirkt sich jedoch nicht nur auf die Zukunft aus, sondern erfordert seit dem Inkrafttreten am 30. Juni 2014 auch eine vollständige Bereinigung der bisher gesammelten Daten. Die Löschung dieser Daten stellt die Provider vor technisch nicht ganz triviale Herausforderungen, da in grosse Datenbanken eingegriffen werden muss.

Die Entscheidung des EuGH wird voraussichtlich zu tiefgreifenden Änderungen in der europäischen Handhabung der Vorratsdatenspeicherung führen. Für die Schweiz hat das Urteil des EuGH keine direkten innerstaatlichen Auswirkungen. Allerdings wird die klare Absage an die bisherige Vorratsdatenspeicherung eine negative Auswirkung auf die europäische und internationale Zusammenarbeit im Bereich der Strafverfolgung haben und vorerst nicht zur kontinentaleuropäischen Rechtssicherheit in der Verbrechensbekämpfung beitragen. Ob das EuGH Urteil und die damit verbundenen Änderungen im EU-Raum auch Signalwirkung auf die anstehenden Gesetzesrevisionen der Schweiz und das Bestreben nach Verlängerung der Vorratsdatenhaltung von sechs Monaten auf ein Jahr haben, kann zu diesem Zeitpunkt nicht beurteilt werden.

Wichtig für die Zukunft der Vorratsdatenspeicherung in der Schweiz scheint auch die weitere Entwicklung der Beschwerde der Digitalen Gesellschaft – ein Zusammenschluss netzpolitisch interessierter Kreise – zu sein. Die Digitale Gesellschaft hat mittels Beschwerde an den zuständigen Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF) die Unterlassung der Vorratsdatenspeicherung gefordert mit der Begründung, diese sei grundrechtswidrig und unverhältnismässig. Mit Antwort vom 30. Juni 2014 hat der Dienst ÜPF die Beschwerde abgelehnt. Die Digitale Gesellschaft hält jedoch an ihrer Beschwerde fest und zieht die Verfügung an das Bundesverwaltungsgericht und nötigenfalls an den Europäischen Gerichtshof für Menschenrechte in Strassburg weiter.

# 5 Tendenzen / Ausblick

## 5.1 Social Engineering: Eine Bedrohung mit vielen Gesichtern

Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen. Um dies zu erreichen, nutzt der Angreifer menschliche Schwächen und gewinnt das Vertrauen seines Gegenübers durch verschiedene Tricks (falsche Identität, Dreistigkeit, Einschüchterung usw.) um das zu bekommen, was er will[57].

Beispiele, in denen solche Methoden zum Einsatz kommen, sind zahlreich und in den MELANI-Halbjahresberichten immer wieder erwähnt. Social Engineering spielt vor allem bei Betrügereien eine grosse Rolle. Ein aktuelles Beispiel sind die Angriffe auf Firmen wie sie in Kapitel 3.1 beschrieben sind: Zurzeit sind alle in der Schweiz tätigen Unternehmen potenzielle Angriffsziele für Attacken mit Social-Engineering-Methoden, unabhängig von ihrer Grösse oder ihrem Geschäftsbereich. In solchen Fällen dienen Social-Engineering-Methoden dazu, direkt und ohne fortgeschrittene Technologie zum eigentlichen Ziel des Angriffs zu gelangen, nämlich zur Überweisung von Geld. Es wäre aber falsch, das Phänomen auf derartige Art Attacken zu reduzieren. Social Engineering hat viele Gesichter und ist oft auch ein Werkzeug, das im Rahmen komplexerer Angriffe, verwendet wird. Unabhängig von Herkunft und Ziel haben solch komplexere Angriffe oft das Ziel, in bestimmte geschützte (Firmen-)Netzwerke zu gelangen. Dabei kommt häufig Social Engineering zur Anwendung. Meist wird ein gefälschtes, teils sehr gezieltes Mail an einen Mitarbeiter der Opferfirma

[57] Siehe auch Definition im Referenzwerk von Kevin Mitnick «The Art of Deception» (2002): «Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology».

verschickt (*Spear Phishing*). Damit wird versucht den Mitarbeiter zu täuschen, damit er Zugangsdaten preisgibt, auf einen Link klickt oder einen Anhang öffnet, mit dem dann sein Computer infiziert wird. Diese Methode spielt häufig bei komplexen Spionageangriffen eine Rolle (Advanced Persistent Threats, APT). Im Fall von Careto/The Mask (s. Kapitel 4.2) wurden die Opfer beispielsweise mit falschen Links auf bekannte Zeitungstitel getäuscht. Auch die Operation «Newscaster» (s. Kapitel 4.2) hat Social Engineering unter zu Hilfenahme von falschen Identitäten zur Erreichung des Zieles verwendet.

Komplexe Angriffe mit finanziellem Ziel verlaufen bei der initialen Infektion ebenfalls häufig nach diesem Muster. So wurde der Angriff gegen die Ladenkette Target[58] mit einem Diebstahl von Zugangsdaten bei einem Lieferanten über ein gezieltes E-Mail gestartet. Dazu haben die Kriminellen einen Lieferanten ausfindig gemacht, der einen umfassenden Zugang zum Netz des Unternehmens Target hatte, und dann gezielt an einen dortigen Mitarbeiter ein gefälschtes E-Mail mit verseuchtem Anhang geschickt. Der Angriff wurde mit Informationen vorbereitet, welche online verfügbar waren. Auch beim Datendiebstahl bei Ebay im ersten Halbjahr 2014 (s. Kapitel 4.8) ist die Verwendung von Social-Engineering-Methoden wahrscheinlich.

Die technologischen Werkzeuge über die Cyberkriminelle verfügen, sind zunehmend ausgefeilter. Neue Lücken werden entdeckt, neue Protokolle verwendet und immer komplexere *Malware-Codes* geschaffen. Etwas bleibt bei aller Veränderung aber gleich: Nämlich, dass die Kriminellen menschliche Schwächen ausnutzen. Die Art und Weise, wie sie das tun, mag je nach Erfindungsgeist und Anpassungsfähigkeit anders sein, die Angreifer setzen bei ihren Opfern aber immer am gleichen Hebel an, nämlich bei deren Neugier, Leichtgläubigkeit, Lust auf Gewinn, Angst und Gutmütigkeit usw. Das Phänomen darf deshalb nicht als einzelner Angriffstyp behandelt werden, sondern ist als Ganzes zu betrachten. Diese Methoden werden auch in Zukunft verbreitet sein, solange man mit ihnen an Informationen und Geld gelangt oder den Zugriff auf ein Netzwerk bekommt, die mit technischen Mitteln allein nicht oder nur mit deutlich mehr Aufwand zu erreichen sind. Deshalb hat die Sensibilisierung des Nutzers gegenüber solchen Bedrohungen nach wie vor die oberste Priorität. Die Nutzer müssen lernen, vorsichtig respektive misstrauisch zu sein, wenn jemand Informationen verlangt oder Links oder Anhänge anbietet, auf die man klicken soll. Das Überprüfen solcher Anfragen und ihrer Echtheit ist ein Muss und sollte, für alle Nutzer zur Routine werden. Gerade in Unternehmen müssen die internen Abläufe klar definiert und jederzeit eingehalten werden, insbesondere in Bezug auf Finanztransaktionen. Auch die Möglichkeit, dass Angreifer durch Infizieren eines Accounts Zugriff zu einem gesamten Netzwerk bekommen, muss beachtet werden. Erweiterter Zugriff und Privilegien sollten nur erteilt werden, wo dies wirklich nötig ist. Schliesslich müssen auch die Informationen, welche ins Internet oder in ein soziales Netz gestellt werden, im Hinblick auf möglichen Missbrauch überprüft werden. Social Engineers nutzen all diese Informationen, um ihr Vorgehen zu verfeinern und damit die Erfolgschancen ihrer Angriffe zu erhöhen.

## 5.2 Medien und Journalisten: attraktive Ziele

Informationen sind ein zentraler Wert, auf die es Angreifer abgesehen haben, vor allem in den drei Bereichen Vertraulichkeit, Verfügbarkeit und Integrität. In diesem Sinne sind Stellen, die über grosse Mengen an Informationen verfügen und die beruflich Informationen verbreiten, natürlich besonders interessante Ziele. Dazu gehören zweifelsfrei die Medien und Journalisten: Durch ihre Tätigkeit verarbeiten sie (sensible) Informationen, die bei ihrer

[58] Siehe MELANI Halbjahresbericht 2013/2, Kapitel 4.4: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 1. September 2014).

Verbreitung grosse Wirkung und Multiplikationseffekte haben können. So werden Medien und Journalisten regelmässig Ziel unterschiedlicher Angriffe, wobei dies nicht nur professionelle, sondern auch andere Journalisten («Bürgerjournalisten», Blogger) betrifft. Zahlreiche Quellen bestätigen, dass dieser Trend im Steigen begriffen ist.

*Angriffe auf Vertraulichkeit der Daten*

Stellen, die eine grosse Menge an Informationen handhaben, sind ein interessantes Ziel. Es ist deshalb logisch, dass verschiedenste Akteure an den diversen Informationen bei Medien und ihren Mitarbeitern interessiert sind, darunter auch staatliche. Zudem steigt mit der Mobilität (Smartphone, Laptop) der Journalisten die Zahl denkbarer Angriffspunkte.

Die Art des Angriffs hängt von der Natur und den Möglichkeiten des Angreifers und seinem Verhältnis zum Opfer ab. Ein staatlicher Akteur kann einen privilegierten Zugriff zu einer IT-Infrastruktur nutzen, um an die Informationen zu kommen. Dieser Zugang kann beispielsweise in totalitären Staaten eine praktisch systematische Überwachung durch die Kontrolle der IT- und Kommunikationssysteme im eigenen Hoheitsgebiet umfassen. Hierbei sind Journalisten ein bevorzugtes Ziel, die auch über andere als die offizielle Meinungen berichten. Auch deren Netz an Informanten ist ein interessantes Ziel.

Akteure, die nicht über einen privilegierten Zugang verfügen, aber Informationen beschaffen wollen und die Mittel dafür aufwenden können, greifen zu Computernetzwerkoperationen (C*omputer Network Operation*s, CNO). Das sind vor allem Operationen des Typs *APT*, über die MELANI schon oft berichtet hat, aber auch Attacken von geringerer Komplexität können Journalisten ins Visier nehmen. Dabei kann es sich um «klassisches» Phishing zum Ausspionieren der Identifikationsdaten handeln oder es kann auch Malware zum Einsatz kommen, welche direkt auf dem Gerät des Ziels installiert wird. Einige dieser Angriffe sind in der Öffentlichkeit bekannt, wie zum Beispiel die Angriffe auf die Mailkonten von Journalisten grosser amerikanischer Medien (New York Times, Wall Street Journal, Bloomberg, Washington Post), gefolgt von der Publikation des APT1-Berichts von Mandiant. Viele Opfer wollen einen Angriff aber lieber nicht öffentlich machen.

*Angriffe auf die Verfügbarkeit oder Integrität der Daten*

Als Herausgeber von Informationen mit mehr oder weniger grossem Multiplikationseffekt sind Webseiten von Zeitungen oder Presseagenturen ebenso wie deren Accounts in sozialen Netzwerken ein bevorzugtes Angriffsziel. Sie erfolgen vor allem durch Akteure, die eine religiöse oder politische Botschaft übermitteln, ihre Bekanntheit erhöhen und zum Teil die öffentliche Meinung mit Falschinformationen beeinflussen wollen. Ein Akteur, der diese Methoden in den letzten Jahren oft benutzte, ist die Syrian Electronic Army (SEA). Eine ihrer bekanntesten Angriffe ist das Hacken des Twitter-Accounts von *Associated Press* (AP) und der anschliessende Tweet, dass es im Weissen Haus eine Explosion gegeben habe, bei der Präsident Obama verletzt worden sei. Das Echo war aufgrund der vielen Follower, die die Information weiterverbreitet haben, gross, und die Meldung wirkte sich sogar auf die amerikanischen Märkte aus. Zugriff auf den Twitter Account von AP verschaffte sich die SEA durch verschiedene Diebstähle von Zugriffsdaten bei AP-Mitarbeitern mittels Phishing. Neben den Angriffen auf die sozialen Netzwerke ist auch das *Defacement* von Webseiten eine Möglichkeit für diese Art von Akteuren.

Die Entwicklung des Internets hat nicht nur zu einer Vervielfachung der Anbieter von Informationen (klassische Medien, Blogs, Bürgerjournalisten), sondern auch der verwendeten Technologien und Plattformen (soziale Netze, Webseiten, Foren usw.) geführt. Einige Akteure sehen das als ebensolche Zunahme der Möglichkeiten, auf diese Information zuzugreifen oder eine Botschaft effizient zu verbreiten. Der Druck auf die Information und ihre Verbreitungskanäle nimmt daher laufend zu. Entsprechend muss das Risiko der

betroffenen Berufsgruppen neu beurteilt werden. Bei der Risikoanalyse sind verschiedene Elemente zu berücksichtigen. Auch hier braucht es eine Sensibilisierung der Mitarbeiter, damit diese die Methoden, mit denen sich Angreifer Zutritt zu den Systemen oder Konten der Opfer verschaffen, erkennen können (Spear Phishing und Social Engineering allgemein). Der Gebrauch mobiler Geräte ist ein zusätzlicher Angriffsfaktor, der die potenziellen Angriffsflächen erhöht und berücksichtigt werden muss. Die Frage der Überwachung durch Akteure mit privilegiertem Zugriff auf eine Infrastruktur in bestimmten Situationen und geeigneter Lösungen im Umgang damit sind ein weiterer Aspekt, den es zu berücksichtigen gilt. Weiterhin im Zentrum stehen, muss deshalb die Verwendung bestehender Möglichkeiten, die eine sichere Kommunikation gewährleisten. Schliesslich muss bei der Wahl des Providers insbesondere für Mail- oder Archivierungsdienste ebenfalls geprüft werden, ob die Vertraulichkeit der Daten sichergestellt ist.

## 5.3 Entwicklungen im Internet nach Snowden

Die «Privatsphäre im Internet» hat nach den ersten Veröffentlichungen Snowdens stark gelitten. Die veröffentlichten Dokumente legten den Schluss nahe, dass die meisten Datenströme überwacht werden und auch Daten bei US-Firmen alles andere als vor Zugriffen des amerikanischen Staates geschützt sind. Der einzelne Nutzer steht dieser Entwicklung eher hilflos gegenüber. Dieser kann zwar bis zu einem gewissen Punkt sein Verhalten anpassen, beispielsweise durch die Wahl seiner IKT-Dienstleistungsanbieter oder zusätzlicher Verschlüsselungsmethoden. (So verzeichnete die Schweizer WhatsApp-Alternative «Threema» in letzter Zeit einen regen Zulauf[59]). Trotzdem ist er in vielen Fällen auf die standardisierten Hard- und Softwarekomponenten angewiesen. Doch wurden die Entwicklungen im Internet durch die aufgrund der Snowden-Affäre gewonnen Erkenntnisse im letzten Jahr überhaupt schon beeinflusst? Es ist sicherlich zu früh, hier bereits irgendwelche nachhaltigen Veränderungen ausmachen zu wollen. Trotzdem gibt es staatliche und private Initiativen, die wenigstens teilweise auf den neuesten Snowden-Erkenntnissen beruhen.

Momentan sind zwei Tendenzen erkennbar: Auf der einen Seite setzen sich Staaten dafür ein, gewisse Teile des Internets von den USA unabhängiger zu machen. Dies beinhaltet den Bau eigener Netze oder den Einsatz eigener Komponenten. Auf der anderen Seite versuchen US-Firmen, mit besseren Verschlüsselungstechniken und anderen Massnahmen das Vertrauen in das System Internet wieder zurückzugewinnen.

*Vorstösse für unabhängigere Netze*

Angela Merkel hat einen Vorstoss für einen innereuropäischen Datenverkehr lanciert. Die EU-Kommission hat diesbezüglich Unterstützung signalisiert.[60] Seit Beginn der Veröffentlichungen der NSA-Dokumente gab es Vorschläge für ein Netzwerk, das einen rein innereuropäischen Datenverkehr erlauben würde. Es geht dabei um die Idee, dass Datenpakete zwischen Internet-Nutzern im Schengen-Raum auch wirklich innerhalb dieser Grenzen bleiben. Heute sucht sich ein Datenpaket den günstigsten Weg, und der kann auch über die USA gehen. Inwiefern sich so etwas allerdings umsetzen lässt, ist noch offen. Dass

[59] http://www.handelsblatt.com/unternehmen/it-medien/instant-messenger-whatsapp-alternative-threema-waechst-rasant/9519942.html (Stand: 1. September 2014).

[60] http://www.heise.de/newsticker/meldung/Bruessel-unterstuetzt-Merkels-Vorstoss-fuer-Schengen-Netz-2116663.html (Stand: 1. September 2014).

bei solchen Plänen ebenfalls wirtschaftspolitische oder staatspolitische Gründe mitspielen können, ist ebenfalls zu berücksichtigen.[61]

Schon im Herbst 2013 hat die brasilianische Präsidentin, Dilma Rousseff, bekannt gegeben, dass Brasilien die Zahl der unabhängigen Internetverbindungen mit anderen Ländern erhöhen will.[62]

Auch in der Schweiz hatten die veröffentlichten Informationen erste Auswirkungen. Anfang Februar 2014 hat der Bundesrat beschlossen, dass kritische Infrastrukturen, wie die Kommunikationsnetze der Verwaltung, wenn möglich selbst gebaut werden sollen und Aufträge darüber hinaus möglichst an inländische Unternehmen vergeben werden müssen. In erster Linie geht es hier um die IKT-Infrastrukturen des Bundes, bei denen Vertraulichkeit eine Rolle spielt. Dies beinhaltet unter anderem Telefone, Mobiltelefone, Computer und Netzwerke, sowie militärische Anlagen.[63]

Für die «Internet Corporation for Assigned Names and Numbers (ICANN)» soll bis September 2015 eine internationale Struktur erarbeitet werden. Dies unter Einbezug der Privatwirtschaft, von Regierungen und der Öffentlichkeit. Die als Non-Profit Organisation registrierte ICANN koordiniert die Vergabe von einmaligen Namen und Adressen im Internet und unterliegt der Aufsicht des US-Handelsministeriums. Der aktuelle Vertrag mit der US-Regierung läuft 2015 aus. Schon seit längerer Zeit gab es vor allem aus Russland und China solche Vorstösse, die aber bislang nach Druck der Internet-Wirtschaft nicht angepackt wurden. Zwar wird ein Zusammenhang mit den aktuellen Snowden-Veröffentlichungen seitens USA dementiert, trotzdem will die USA nun die Kontrolle über die Internet-Verwaltung ICANN abgeben.[64]

*Investitionen von US- und nicht-US-Firmen in IT- und Rechtssicherheit*

Gleich mehrere E-Mail-Provider stellten im ersten Halbjahr 2014 auf *Transportverschlüsselung* um. Yahoo gab bereits im November 2013 bekannt, dass man die Sicherheit der Nutzer schrittweise erhöhen will. So wurde am Anfang des Jahres Webverkehr standardmässig auf *HTTPS* umgestellt. Anfang April wurde dann auch der gesamte Verkehr zwischen Yahoo-Diensten und den Datenzentren verschlüsselt. Eine neue verschlüsselte Version des Yahoo Messengers wurde ebenfalls angekündigt.[65] Auch die deutschen E-Mail-Provider «Freenet», «GMX», «Web.de» und die deutsche Telekom erlauben seit Ende April nur noch verschlüsselte Kommunikation zwischen Nutzer und Datencenter.[66]

Die oben erwähnte Transportverschlüsselung bezieht sich allerdings nur auf den Weg zwischen dem Nutzer und seinem E-Mail Provider. Der Transport von Daten zwischen den Providern muss gesondert betrachtet werden. Akzeptiert der Provider des Empfängers beispielsweise keine verschlüsselten Daten, werden die E-Mail Daten weiterhin

[61] http://www.welt.de/politik/ausland/article126925318/Schengen-Cloud-koennte-zum-Handelskrieg-fuehren.html (Stand: 1. September 2014).

[62] http://www.theguardian.com/world/2013/sep/20/brazil-dilma-rousseff-internet-us-control (Stand: 1. September 2014).

[63] http://www.nzz.ch/wirtschaft/newsticker/chus-geheimdienstaffaere-br-will-mehr-sicherheit-fuer-telekom-und-informatik-1.18236385 (Stand: 1. September 2014).

[64] http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/amerika-gibt-aufsicht-ueber-internet-verwaltung-auf-12849181.html (Stand: 1. September 2014).

[65] http://yahoo.tumblr.com/post/81529518520/status-update-encryption-at-yahoo (Stand: 1. September 2014).

[66] http://www.computerbild.de/artikel/cb-Aktuell-Sicherheit-E-Mail-made-in-Germany-Telekom-GMX-Web.de-Freenet-SSL-8593819.html (Stand: 1. September 2014).

unverschlüsselt übermittelt. Google hat hierzu einen ersten Transparenzbericht herausgegeben und listet auch die Provider auf, welche keine Verschlüsselung akzeptieren. Laut diesem Bericht werden 75% der von Gmail ausgehenden Nachrichten verschlüsselt, bei den eingehenden Nachrichten ist der Wert mit 57% kleiner.[67] Beide Werte sind im letzten Halbjahr gestiegen. Generell hat der verschlüsselte Datenverkehr in den letzten Monaten stark zugenommen, wie eine Studie im Mai 2014 veröffentlicht hat. Der verschlüsselte Datenverkehr hat sich innerhalb eines Jahres verdoppelt, in Europa sogar verdreifacht.[68]

Ein Fall, der Microsoft momentan beschäftigt, könnte weitereichende Folgen für die Datenhaltung, speziell von Cloud-Diensten, haben. Es geht darum, ob Kundendaten von US-Firmen, welche in Europa gespeichert sind, ebenfalls an die USA geliefert werden müssen. Dieser Rechtsstreit wird gerade im Hinblick auf die Snowden-Veröffentlichungen weltweit mit Interesse verfolgt. Konkret fordert ein US-Bezirksgericht von Microsoft, E-Mails und andere gespeicherten Daten eines Kunden herauszugeben, welche in einem Datenzentrum in Dublin gespeichert sind. Microsoft stellt sich hier auf den Standpunkt, dass die US-Justiz nicht das Recht habe, Daten zu fordern, welche ausserhalb der USA gespeichert sind. Die Symbolkraft dieses Urteils ist enorm: Es geht hier nicht nur um das langfristige Vertrauen von Kunden in US-Firmen, sondern auch um die Jurisdiktion von Daten in einer Cloud.

Auch seitens USA gibt es Zeichen, dass die Datenbeschaffung durch die NSA stärker reglementiert wird. So hat Präsident Obama Änderungen in der Praxis der Datenbeschaffung der NSA angeordnet. Beispielsweise wollen die USA die Kommunikation der Staats- und Regierungschefs von «Freunden und Verbündeten» im Ausland nicht mehr ausspähen, solange es nicht einen zwingenden Grund der nationalen Sicherheit dafür gebe. Nicht-US-Bürger sollen künftig in den Genuss eines Teils der Schutzvorschriften kommen, die bislang nur für US-Bürger gegolten haben.[69] Trotzdem sind diese Aussagen noch wenig konkret und stark interpretierbar.

## 5.4 Zwei-Faktor-Authentisierung für alle Dienste

In der aktuellen Bedrohungslage bieten Passwörter oder generell Authentisierungen, welche nur auf einem Faktor beruhen, nicht mehr genügend Sicherheit. Aus diesem Grund empfiehlt MELANI immer einen zweiten Faktor zur Authentisierung zu nutzen. Generell gibt es folgende Authentisierungsfaktoren:

- Wissen: «Ich beweise meine Identität durch Wissen», z. B. einem Passwort
- Haben: «Ich beweise meine Identität durch einen Besitz»; z. B. eine Smartcard
- Sein: «Ich beweise meine Identität durch eine Eigenschaft», z. B. ein Fingerabdruck

Werden zwei dieser Faktoren kombiniert, spricht man von einer Zwei-Faktor-Authentisierung. Sehr oft werden dabei Wissen und Haben miteinander kombiniert. Dies ist beim E-Banking seit einiger Zeit Standard, viele Anwendungen von grossen Internetprovidern ziehen langsam nach. Oft wird dabei die Technik verwendet, eine *SMS* mit einem Code an eine vorgängig definierte Telefonnummer zu senden. Ein Teil der Dienste löst das Problem so, dass dieser Schritt nur das erste Mal notwendig ist, wenn man sich mit einem Gerät

[67] http://www.google.com/transparencyreport/saferemail/ (Stand: September 2014).

[68] https://www.sandvine.com/trends/global-internet-phenomena/ (Stand: 1. September 2014).

[69] http://www.nzz.ch/aktuell/startseite/obama-setzt-geheimdiensten-engere-grenzen-1.18223803 (Stand: 1. September 2014).

verbindet und dass dann dieses Gerät dauerhaft als vertrauenswürdig gespeichert ist. Andere verwenden ein *One Time Password–Verfahren* (OTP), basierend auf einer App, welche zufällig Zahlen generiert, die während einer kurzen Zeit gültig sind (z.B. Google Authenticator).

Einige Provider, welche eine Zwei-Faktor-Authentisierung unterstützen:

- Google Anwendungen (gmail, google+, etc.)
- Outlook.com
- Dropbox
- …..

Diese Art von Authentisierung sollte ebenfalls für die Verwaltung von *CMS-Systemen* sowie generell von Administrationsinterfaces, die vom Internet her zugänglich sind, verwendet werden: ein Verlust des Passwortes in diesem Bereich kann besonders viel Schaden, auch für Drittpersonen, verursachen. Die meisten CMS-Systeme unterstützen eine Zwei-Faktor-Authentisierung, sei dies direkt wie z. B. in Joomla oder durch Plugins wie zum Beispiel in Wordpress mit dem Plugin von Henrik Schak[70]. Auch der oft mit *Bruteforce* angegriffene *SSH-Dienst* unter Linux, welcher einen verschlüsselten Datentransfer zur Verfügung stellt, kann beispielsweise benutzerfreundlich mit Google Authenticator oder mit einem *Privatekey/Publickey*-Verfahren abgesichert werden.

Für besonders heikle Zugriffe oder für grössere Firmen sollten als Authentisierungsverfahren Technologien wie Zertifikate auf Smartcards oder isolierte Einmalpasswortverfahren geprüft werden, da das Smartphone selbst mit dem Internet verbunden ist und somit ebenfalls angreifbar ist.

## 5.5 Politische Geschäfte

| Geschäft | Nummer | Titel | Eingereicht von | Datum Einreichung | Rat | Amt | Stand Beratung & Link |
|---|---|---|---|---|---|---|---|
| Ip | 14.3019 | Beschaffungswesen. ICT-Projekte | Noser Ruedi / FDP-Liberale Fraktion | 03.03.2014 | NR | EFD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143019 |
| Fr | 14.5063 | Telefonabhörsystem ISS | Balthasar Glättli | 05.03.2014 | NR | EJPD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143193 |
| Kt. Iv | 14.305 | Fertig mit den anonymen Aufrufen zu Demonstrationen und Grossanlässen ohne Übernahme von Verantwortung | Kanton Bern | 19.03.2014 | | | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20140305 |
| Ip | 14.3204 | Konsens der Arbeitsgruppe Agur 12. Weiteres Vorgehen | Felix Gutzwiller | 20.03.2014 | SR | EJPD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143204 |
| Po | 14.3193 | Verbesserung der polizeilichen Ermittlungen in sozialen Netzwerken | Karl Vogler | 20.03.2014 | NR | EJPD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143193 |
| Mo | 14.3288 | Identitätsmissbrauch. Eine strafbare Handlung für sich | Raphaël Comte | 21.03.2014 | SR | EJPD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143288 |
| Ip | 14.3240 | Globale Internetverwaltung. Eine einmalige Gelegenheit für das internationale Genf | Carlo Sommaruga | 21.03.2014 | NR | EDA | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143240 |
| Mo | 14.3236 | Anpassung der Grundversorgung mit Breitbandinternet | Martin Candinas | 21.03.2014 | NR | UVEK | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143236 |
| Mo | 14.3011 | Kostenreduktion dank elektronischen Zollverfahrens | Kommission für Wirtschaft und Abgaben NR | 24.03.2014 | NR | EFD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143011 |
| Mo | 14.3293 | Abgabe auf leeren Datenträgern | Kommission für Wirtschaft und Abgaben NR | 08.04.2014 | NR | EJPD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143293 |
| Ip | 14.3379 | Schweizer Internetseiten durch Schweizer Unternehmen absichern | Derder Fathi | 08.05.2014 | NR | EFD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143379 |
| Ip | 14.3351 | Personalizierte Medizin. Nationale Biobank statt ausländische private Datenbanken über Schweizer Patientinnen und Patienten | Barbara Schmid-Federer | 08.05.2014 | NR | EDI | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143351 |

[70] https://wordpress.org/plugins/google-authenticator/ (Stand: September 2014).

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ip | 14.3341 | Geplante Umstellung der Swisscom von analoger auf Internet-Telefonie für alle Festnetzanschlüsse | Glättli Balthasar | 08.05.2014 | NR | UVEK | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143341 |
| Ip | 14.3409 | Minimalrecht auf digitalen Zugang | Luc Recordon | 05.06.2014 | SR | UVEK | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143409 |
| Mo | 14.3423 | Positionierung der Schweiz als internationale Plattform im Bereich Internet | Noser Ruedi / FDP-Liberale Fraktion | 10.06.2014 | NR | EDA | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143423 |
| Po | 14.3532 | Standortbestimmung und Ausblick Open Source in der Bundesverwaltung | Edith Graf-Lischer | 19.06.2014 | NR | EFD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143532 |
| Po | 14.3658 | Internetplattformen zum Austausch von Dienstleistungen zwischen Internetnutzerinnen und -nutzern insbesondere in den Bereichen Unterkunft und Transport. Bericht über Konsequenzen und zu treffende Massnahmen | Carlo Sommaruga | 20.06.2014 | NR | EFD | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143658 |
| Ip | 14.3630 | Werbevorschriften. Automatische Übernahme von EU-Recht | Thomas Müller | 20.06.2014 | NR | EDA | http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143630 |

# 6 Glossar

| | |
|---|---|
| Access Control Lists (ACL) | Eine Access Control List (ACL), deutsch Zugriffssteuerungsliste, ist eine Software-Technik, mit der Betriebssysteme und Anwendungsprogramme Zugriffe auf Daten und Funktionen eingrenzen können. |
| Adresszeile | Durch Angabe der URL in der Adresszeile des Browsers wird die entsprechende Internetseite aufgerufen. |
| Advanced Persistent Threat (APT) | Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen. |
| Backup | Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können. |
| Bit/Byte | Das Byte ist eine Masseinheit für die Datenmenge digital gespeicherter und übertragener Daten. Ein Byte besteht aus 8 Bit. |
| Botnet | Eine Ansammlung von Computern, die mit Malicious Bots infiziert sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen kompromittierter Rechner bestehen. |
| Bruteforce | Die Bruteforce-Methode ist eine Lösungsmethode für Probleme, die auf dem Ausprobieren aller oder zumindest möglichst vieler möglichen Fälle beruht. |
| Cache | Cache bezeichnet in der EDV einen Speicher, der wiederholte Zugriffe auf ein langsames Hintergrundmedium oder aufwändige Neuberechnungen zu vermeiden hilft. |
| Chat | Chat bezeichnet die elektronische Kommunikation in Echtzeit, meist über das Internet. |
| Cloud Computing | Cloud Computing (Synonym: Cloud IT, deutsch etwa Rechnen in der Wolke) ist ein Begriff aus der Informationstechnik (IT). Die IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben/bereitgestellt, sondern über einen oder mehrere Anbieter bezogen. Die Anwendungen und Daten befinden sich nicht mehr auf dem lokalen |

| | |
|---|---|
| | Rechner oder im Firmenrechenzentrum, sondern in der Wolke (Cloud). Der Zugriff auf diese entfernten Systeme erfolgt über ein Netzwerk. |
| Code Review | Mit dem Review werden Arbeitsergebnisse der Softwareentwicklung manuell geprüft. |
| Command and Control Server | Die meisten Bots können von einem Botmaster über einen Kommunikationskanal überwacht werden und Befehle empfangen. Dieser wird als Command and Control-Server bezeichnet. |
| Computer Network Operation (CNO) | Unter Computer-Netzwerk-Operationen versteht man bei der Kriegsführung Massnahmen, um die Informationsüberlegenheit gegenüber einem Gegner zu gewinnen respektive diese beim Feind einzuschränken. |
| Content Management System (CMS) | Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet. |
| DDoS | Denial-of-Service Attacke. Hat zum Ziel, einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. |
| Defacement | Verunstaltung von Webseiten. |
| Diffie-Hellmann | Der Diffie-Hellman-Schlüsselaustausch oder Diffie-Hellman-Merkle-Schlüsselaustausch ist ein Schlüsselaustauschprotokoll. Mit ihm erzeugen zwei Kommunikationspartner einen geheimen Schlüssel, den nur diese beiden kennen. |
| DNS Amplification/Reflection Angriff | Denial of Service (DoS)-Angriff, der öffentlich zugängliche DNS-Server missbraucht und als Amplifier (Verstärker) benutzt. |
| DNS-Server | Domain Name System. Mit Hilfe von DNS lassen sich das Internet und deren Dienste benutzerfreundlich nutzen, da die Benutzer anstelle von IP-Adressen Namen verwenden können (z.B. www.melani.admin.ch). |
| Drive By Infektion | Infektion eines Computers mit Malware allein durch Besuch einer Web-Seite. Vielfach beinhalten die betroffenen Web-Seiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Die |

| | |
|---|---|
| | Infektion erfolgt meistens durch das Ausprobieren von Exploits für vom Besucher noch nicht geschlossene Sicherheitslücken. |
| Exploit | (kurz: Exploit) Ein Programm, ein Script oder eine Codezeile, mit der sich Schwachstellen in Computersystemen ausnutzen lassen. |
| Fernwartungssoftware | Die Fernwartungssoftware (englisch: Remote Administration Tool) stellt eine Anwendung des Konzeptes Fernwartung für beliebige Rechner oder Rechnersysteme dar. |
| Fingerprint | In der Informatik sind Fingerprints häufig Hashfunktionen, um eine Datei zu identifizieren |
| Hardware Security Module (HSM) | Der Begriff Hardware-Sicherheitsmodul (HSM) oder englisch Hardware Security Module bezeichnet ein (internes oder externes) Peripheriegerät für die effiziente und sichere Ausführung kryptographischer Operationen oder Applikationen. |
| Hintertür/Backdoor | Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen. |
| HTTP Strict Transport Security | HTTP Strict Transport Security (HSTS) ist eine Webserver Einstellung, die eine verschlüsselte Verbindung zwischen Webserver und Nutzer erzwingt. |
| HTTP-Request | HyperText Transfer Protocol Standard zur Übertragung von HTML-Dokumenten (z.B. im Internet). |
| Ingress-Filtering | Mit einem Ingress-Filter werden, allgemein formuliert, Netze vor unerwünschtem Eingangsdatenverkehr geschützt. |
| Internet Service Provider (ISP) | Internet Service Provider. Internet-Dienstanbieter, die meist gegen Entgelt verschiedene Leistungen erbringen, die für die Nutzung oder den Betrieb von Internet-Diensten erforderlich sind. |
| IP-Adresse | Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87). |
| Least Privilege | Das Konzept der geringsten Rechte besagt, dass einer Unterklasse kein Zugriff auf eine Komponente gewährt werden sollte, wenn dies nicht unbedingt erforderlich ist. |

| | |
|---|---|
| Metadaten | Metadaten oder Metainformationen sind Daten, die Informationen über andere Daten enthalten. |
| NTP | Das Network Time Protocol (NTP) ist ein Standard zur Synchronisierung von Uhren in Computersystemen über paketbasierte Kommunikationsnetze. |
| Privater Schlüssel / Öffentlicher Schlüssel | Das Public Key Verfahren ist ein asymmetrisches, kryptographisches Verfahren, bei dem ein Schlüsselpaar zum Einsatz kommt. Dieses kryptografisches Schlüsselpaar besteht aus einem öffentlichen und einem privaten Schlüssel. |
| OPC Server | OLE for Process Control (OPC) war der ursprüngliche Name für standardisierte Software-Schnittstellen, die den Datenaustausch zwischen Anwendungen unterschiedlichster Hersteller in der Automatisierungstechnik ermöglichen sollten. |
| OpenSSL | OpenSSL, ursprünglich SSLeay, ist eine freie Software für Transport Layer Security, ursprünglich Secure Sockets Layer (SSL). |
| OTP | Ein One Time Passwort (OTC) (oder zu Deutsch: Einmalpasswort) ist ein Kennwort zur Authentifizierung oder auch Autorisierung. Jedes Einmalkennwort ist nur für eine einmalige Verwendung gültig und kann kein zweites Mal benutzt werden. |
| Patch | Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z.B. eine Sicherheitslücke behebt |
| Peer To Peer | Peer to Peer (P2P). Eine Netzwerkarchitektur, bei der die beteiligten Systeme gleiche Funktionen übernehmen können (im Gegensatz zu Client-Server Architekturen). P2P wird häufig zum Austausch von Daten genutzt. |
| 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. |
| PingBack | Pingback ist eine Methode, die es Web-Autoren erlaubt, eine Benachrichtigung anzufordern, sobald jemand ihre Dokumente oder Seiten |

| | |
|---|---|
| | verlinkt. |
| Port | Ein Port ist der Teil einer Netzwerk-Adresse, der die Zuordnung von TCP- und UDP-Verbindungen und -Datenpaketen zu Server- und Client-Programmen durch Betriebssysteme bewirkt. |
| Ransomware | Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt. |
| 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. |
| Remote Procedure Call (RPC) | Der Remote Procedure Call (RPC) ist eine Technik zur Realisierung von Interprozesskommunikation. Sie ermöglicht den Aufruf von Funktionen in anderen Adressräumen. |
| Schadsoftware | Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). |
| Smartphone | Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt. |
| SMS | Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer. |
| SNMP | Das Simple Network Management Protocol (SNMP) ist ein Netzwerkprotokoll, das von der IETF entwickelt wurde, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können. |
| Social Engineering | Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen. |
| Spearphishing | Gezielte Phishing Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren. |

| | |
|---|---|
| Speicherprogrammierbare Steuerung (SPS) | Eine (SPS) ist ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt wird und auf digitaler Basis programmiert wird. |
| SSL | Secure Sockets Layer Ein Protokoll, um im Internet sicher zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen. |
| SSH FileTransfer Protocol | Das SSH File Transfer Protocol oder Secure File Transfer Protocol (SFTP) ist eine für die Secure Shell (SSH) entworfene Alternative zum File Transfer Protocol (FTP), die Verschlüsselung ermöglicht. |
| Streamingdienst | Streaming Media bezeichnet die gleichzeitige Übertragung und Wiedergabe von Video- und Audiodaten über ein Netzwerk. |
| Transportverschlüsselung | Verschlüsselung von Daten zwischen zwei Servern. Im Speziellen bei E-Mail-Diensten zwischen Nutzer und E-Mail-Provider. |
| Treiber | Ein Gerätetreiber, häufig kurz nur Treiber genannt, ist ein Computerprogramm oder Softwaremodul, das die Interaktion mit angeschlossenen Geräten steuert. |
| Trojanisches Pferd | Trojanische Pferde (häufig als Trojaner bezeichnet) sind Programme, die im Verborgenen schädliche Aktionen ausführen und sich dabei für den Benutzer als nützliche Anwendung oder Datei tarnen. |
| Tunneling | Tunnel bzw. Tunneling bezeichnet in einem Netzwerk die Konvertierung und Übertragung eines Kommunikationsprotokolls, das für den Transport in ein anderes Kommunikationsprotokoll eingebettet wird. |
| URL | Uniform Resource Locator Die Web-Adresse eines Dokuments bestehend aus Protokoll, Server-Name, sowie Dateiname mit Pfad (Beispiel: http://www.melani.admin.ch/test.html). |
| User Datagram Protocol (UDP) | UDP ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört. Aufgabe von UDP ist es, Daten, die über das Internet übertragen werden, der richtigen Anwendung zukommen zu lassen. |
| Verschlüsselte Seite (https) | Protokoll zur sicheren, d.h. verschlüsselten Übertragung von HTML-Dokumenten (z.B. Internet). Siehe auch HTTP. |
| VideoCodec | Ein VideoCodec bezeichnet ein Algorithmenpaar, das die Kodierung und Dekodierung von |

| | |
|---|---|
| | digitalem Videomaterial beschreibt. |
| Virus | Ein selbstreplizierbares, mit schädlichen Funktionen versehenes Computerprogramm, welches sich zur Verbreitung an ein Wirteprogramm oder eine Wirtedatei hängt. |
| VPN | Virtual Private Network Ermöglicht durch Verschlüsselung des Datenverkehrs eine sichere Kommunikation zwischen Rechnern über öffentliche Netzwerke (z.B. das Internet). |
| Watering-Hole Angriffe | Gezielte Infektion durch Schadsoftware über Webseiten, welche bevorzugt nur von einer spezifischen Benutzergruppe besucht werden. |
| Webmail | Webmail werden Dienste im World Wide Web bezeichnet, die die Verwaltung von E-Mails mit einem Webbrowser ermöglichen. |
| WLAN | WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk. |
| Zertifikat | Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. |
| Zertifizierungsstelle | Eine Zertifizierungsstelle ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht. |