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 2015/I (Januar – Juni)

29. OKTOBER 2015

MELDE- UND ANALYSESTELLE INFORMATIONSSICHERUNG MELANI
http://www.melani.admin.ch

1 Übersicht / Inhalt

1 Übersicht / Inhalt 2

2 Editorial 5

3 Schwerpunktthema: Website-Sicherheit 6

4 Lage national 9

4.1 Spionage 9

4.1.1 Duqu reloaded: ausgeklügelte Spionagesoftware gegen Teilnehmer der iranischen Atomgespräche 9

4.1.2 Swisscom-Leitungen angeblich von BND und NSA abgehört 10

4.2 Datenabflüsse 11

4.2.1 Rex Mundi 11

4.3 Industrielle Kontrollsysteme 12

4.3.1 Honeypot Wasserkraftwerk – 31 Attacken 12

4.3.2 Offene Systemsteuerung von Wasserversorgungssystemen 13

4.4 Angriffe (DDoS, Defacements) 15

4.4.1 DDoS und Erpressung: Angriffswelle DD4BC 15

4.4.2 Defacements von Westschweizer Webseiten 15

4.5 Social Engineering, Phishing 16

4.5.1 Phishing – Angriffe auf Kantonalbanken, Kreditkartendaten, Verbesserung der Phishing-E-Mails 17

4.5.2 Phishing nach Defacements und manchmal auch umgekehrt 18

4.5.3 Gefälschte Steuerformulare 19

4.6 Crimeware 20

4.7 Präventive Massnahmen 25

4.7.1 Antiphishing.ch 25

5 Lage International 26

5.1 Spionage 26

5.1.1 Hacker-Angriff auf den deutschen Bundestag 26

5.1.2 Carbanak – der elektronische Banküberfall 27

5.1.3 SIM-Karten angeblich im Visier von NSA und GCHQ 27

5.1.4 Spionage im Profisport 28

5.2 Datenabflüsse 28

5.2.1 Über 21 Millionen Datensätze beim US-Personalamt entwendet 28

5.2.2 AdultfriendFinder, British Airways und Krankenversicherung - Datenabflüsse in verschiedensten Branchen 29

5.3 Industrielle Kontrollsysteme 30

5.3.1 Sicherheit in der Automobilbranche 31

5.3.2 Reboot bei Boeing 787 Dreamliner 32

5.3.3 Infotainmentsysteme im Flugzeug ... 32
5.3.4 Stromausfälle – Cyberhintergrund vermutet aber nicht bestätigt ... 33
5.3.5 US-Tankstellen aus dem Internet angreifbar ... 33
5.4 Angriffe (DDoS, Defacements) ... 34
5.4.1 Kein Signal bei TV5 Monde ... 34
5.4.2 Cyberangriff: Flüge von Polish Airlines gestrichen ... 36
5.4.3 Cyberangriffe im Nachgang von Charlie Hebdo ... 37
5.4.4 Hacker legen Website der US-Armee lahm ... 38
5.4.5 Superfish/Lenovo ... 38
5.4.6 Exploit Kits ... 39
5.4.7 Log Jam und FREAK-Lücken ... 41
5.5 Präventive Massnahmen ... 41
5.5.1 Neues Patch-Management von Microsoft ... 41
5.6 Weitere Themen ... 42
5.6.1 Einfache, aber folgenschwere Diebstähle ... 42
6 Tendenzen und Ausblick ... 43
6.1 Wenn Daten in ein anderes Leben führen ... 43
6.2 Auf Leben und Tod - IKT im Gesundheitswesen ... 44
7 Politik, Forschung, Policy ... 46
7.1 Parlamentarische Vorstösse ... 46
7.2 Weitere Themen ... 47
7.2.1 Nationales Forschungsprogramm Big Data ... 47
7.2.2 Neuorganisation Domainvergabe ... 48
8 Publizierte MELANI Produkte ... 49
8.1 GovCERT.ch Blog ... 49
8.1.1 Joining the DNSSEC Day in Germany (nur in Englisch verfügbar) ... 49
8.1.2 Outdate WordPress: Thousands of websites in Switzerland are vulnerable (nur in Englisch verfügbar) ... 49
8.1.3 Increase in DDoS extortion (DD4BC) (nur in Englisch verfügbar) ... 49
8.1.4 e-Banking Trojan Retefe still spreading in Switzerland (nur in Englisch verfügbar) ... 50
8.1.5 Critical vulnerability in Magento: Many Swiss websites are still vulnerable (nur in Englisch verfügbar) ... 50
8.2 MELANI Newsletter ... 50
8.2.1 Meldeportal gegen Phishing ... 50
8.2.2 DDoS Angriffe und Erpressung : eine äusserst aktuelle Kombination ... 50
8.2.3 E-Banking Trojaner «Dyre»: Lawinenartige Verbreitung ... 51
8.2.4 10 Jahre MELANI: Ein Blick zurück und auf die aktuellen Bedrohungen in der Cyberwelt im 20. Halbjahresbericht ... 51
8.2.5 Kunden von Schweizer KMUs: Ziel von massgeschneiderten Phishing-Angriffen ... 51

8.2.6 E-Banking Trojaner hat Schweizer KMU im Visier 52
8.3 Checklisten und Anleitungen 52
8.3.1 Massnahmen gegen DDoS-Attacken 52
8.3.2 Merkblatt IKT-Sicherheit für KMU 52
9 Glossar 53

2 Editorial

Pascal Lamia, 48, ist seit 2008 Leiter der Melde- und Analysestelle Informationssicherung MELANI

Liebe Leserinnen, liebe Leser

Die Melde- und Analysestelle Informationssicherung MELANI hat am 1. Oktober 2014 ihr zehnjähriges Bestehen gefeiert. Unzählige Fälle wurden uns in den letzten zehn Jahren gemeldet. Vom normalen Betrugsversuch bis hin zu Spionageangriffen kann MELANI unterdessen eine breite Erfahrung vorweisen. Zahlreiche Betreiber kritischer Infrastrukturen konnten seit 2004 von unserer Unterstützung in den Bereichen Prävention und Bewältigung von Cyberangriffen profitieren.

MELANI hat ihren Erfolg in erster Linie der Privatwirtschaft zu verdanken. Ohne das sehr gut funktionierende «Public Private Partnership», also die erfolgreiche Zusammenarbeit zwischen Bund und Privatwirtschaft, hätte MELANI niemals den heutigen Stellenwert erreicht. Ich bedanke mich ganz herzlich bei allen Personen aus Verwaltung und Privatwirtschaft, die in den letzten zehn Jahren MELANI zu dem gemacht haben, was sie heute ist.

Den Beginn der zweiten Dekade des Bestehens von MELANI haben wir zum Anlass genommen, ein neues Emblem erstellen zu lassen.

Das Emblem symbolisiert einerseits die weltweiten digitalen Datenströme. Andererseits bildet sie aber auch die internationale Vernetzung ab. Ohne ein persönliches Netzwerk zu Partnerorganisationen auf der ganzen Welt wäre es heute ein Ding der Unmöglichkeit, Cyberbedrohungen erfolgreich entgegen zu treten.

Der vorliegende Halbjahresbericht ist ebenfalls ein Schritt in das zweite MELANI-Jahrzehnt: Er wurde strukturell komplett überarbeitet und soll Ihnen das Lesen noch einfacher und angenehmer gestalten.

Ich wünsche Ihnen viel Freude beim Lesen

Pascal Lamia

3 Schwerpunktthema: Website-Sicherheit

Das Internet ist in den letzten 15 Jahren sehr stark gewachsen. Tausende neuer Websites gehen jeden Tag online. Gemäss Netcraft[1] gibt es momentan mehr als 850 Millionen aktive Websites. Einer der Gründe, wieso die Anzahl Websites so stark gewachsen ist, liegt im Einsatz von *Content Management Systemen (CMS)* wie beispielsweise «WordPress, «Typo3», «Joomla!» und «Drupal». Mit einem CMS können Internet-Benutzer sehr einfach und ohne fundiertes IKT-Wissen Inhalte im Internet publizieren. Zusätzlich gibt es zahlreiche *Plug-Ins*, die zur Verfügung stehen und es erlauben, die Website nach den eigenen Wünschen anzupassen. Durch die einfache Bedienung von CMS werden diese auch gerne und oft von Hobby-Webmastern aber auch von kleineren und mittleren Unternehmen (KMU) verwendet, um ihre Informationen im Internet zu publizieren.

Während auf der einen Seite ein *CMS* sehr praktisch ist, bietet dieses andererseits ein wertvolles Ziel für Hacker. Ein Grossteil der *Phishing*-Seiten und *Drive-by-Infektionen* wird auf Webseiten platziert, welche mit einem nicht aktualisierten CMS betrieben werden. Wie in vielen Programmen tauchen auch bei CMS regelmässig Sicherheitslücken auf, für welche der jeweilige Hersteller in der Regel zeitnah entsprechende Sicherheits-Updates zur Verfügung stellt. Beispielsweise wurden im Jahr 2014 alleine in der CMS-Software Drupal 14 Schwachstellen entdeckt und behoben, in Joomla! deren neun und in Wordpress sogar 29[2]. Websites, die mit einer verwundbaren CMS-Version erstellt worden sind, können mit Tools automatisiert im Internet aufgefunden und angegriffen werden. Somit ist es für Kriminelle relativ einfach, auf diese Weise eine grosse Zahl von verwundbaren Webauftritten aufzuspüren und zu manipulieren. Ein regelmässiges Update (Patchen) der CMS-Software ist deshalb für jeden Betreiber von Websites essentiell – trotzdem wird in vielen Fällen gerade diesem Bereich zu wenig Beachtung geschenkt. Durch den Einsatz von veralteten (und unsicheren) CMS gefährden Website-Betreiber aber nicht nur andere Internet-Benutzer, sondern auch sich selber: Im ersten Halbjahr 2015 sind MELANI mehrere Fälle gemeldet worden, bei welchen veraltete CMS kompromittiert worden sind. Die Daten im CMS wurden kopiert und anschliessend die Besitzer mit diesen Daten erpresst. Besonders bei KMU besteht hier eine Gefährdung, da in vielen CMS auch Kundendaten hinterlegt sind.

Sicherheitsupdates für CMS werden in der Regel schnell durch die Hersteller zur Verfügung gestellt. Im Unterschied zu den meisten Betriebssystemen geschieht dies aber nicht automatisch, sondern muss oftmals vom Betreiber manuell initialisiert werden. Leider ist es so, dass ein Grossteil der Website-Betreiber, welche ein CMS für Ihren Webauftritt verwenden, dieses einmal installieren und über Jahre hinweg auf derselben (und somit in der Regel veralteten und unsicheren) Version des CMS betreiben. Folgende Beispiele von Verwundbarkeiten in Wordpress, welche auch auf alle anderen CMS erweitert werden können, visualisieren dieses Verhalten.

70% der Schweizer Wordpressinstallationen verwundbar

Im April 2015 wurde eine Schwachstelle in WordPress bekannt, welche einem Angreifer erlaubte, einen *Cross Site Scripting Angriff (XSS)* gegen jede verwundbare Webseite auszuführen, indem dieser einen Kommentar mit speziell präpariertem *JavaScript* auf der

[1] http://news.netcraft.com/archives/2015/08/13/august-2015-web-server-survey.html (Stand: 31. August 2015).

[2] https://cve.mitre.org (Stand: 31. August 2015).

verwundbaren Webseite verfasste (CVE-2015-3429). Noch am gleichen Tag hat Wordpress ein Sicherheits-Update veröffentlicht, um die Verwundbarkeit zu schliessen. Am 6. Mai 2015 wurde jedoch bereits die nächste Sicherheitslücke in Wordpress publik, welche es einem Angreifer erlaubte, einen weiteren Cross-Site-Scripting Angriff (XSS) gegen WordPress durchzuführen (CVE-2015-3440). Auch hier veröffentlichte Wordpress bereits am nächsten Tag ein Sicherheits-Update.

Die Reaktionsgeschwindigkeit der betroffenen Betreiber war jedoch erschreckend langsam. In der Schweiz werden beispielsweise rund 6% der Websites mit Wordpress betrieben. Obwohl die Sicherheits-Updates zur Verfügung standen, blieben über 70% der Websites verwundbar.[3]

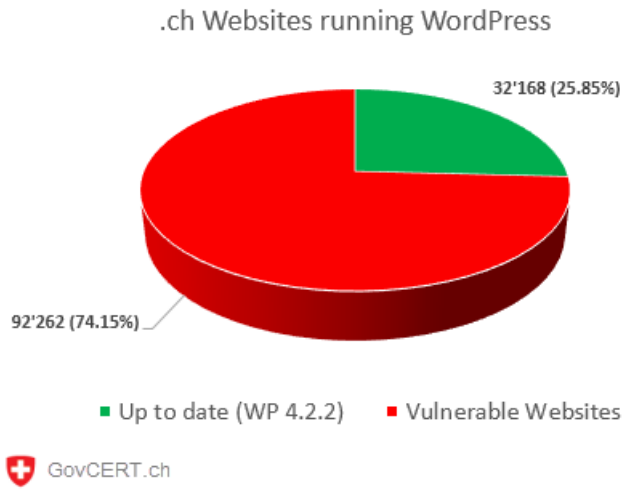


Abbildung 1: Wordpressnutzer, welche gegenüber den Schwachstellen CVE-2015-3440 und CVE-2015-3429 verwundbar sind (rot), zwei Monate nach Veröffentlichung des Patches.

Regelmässige Updates – notwendig, aber nicht genügend!

Die Erkenntnisse aus der von MELANI erstellten Analyse erschrecken und werfen die Frage auf, warum so viele Website-Betreiber verwundbare CMS-Versionen einsetzen. Eine Antwort dürfte neben fehlender Sensibilität und fehlender Zeit auch ein gewisses Stück an Bequemlichkeit beinhalten. Viele erkennen die Notwendigkeit nicht, ihr CMS zu patchen oder sind sich nicht bewusst, welche Auswirkungen verwundbare CMS-Installationen haben können. Der Betrieb eines CMS bringt aber immer eine gewisse Verantwortung mit sich. Diese gilt es wahrzunehmen. Neben dem *zeitnahen Patch-Management* gibt es auch noch andere Massnahmen, welche die Sicherheit von CMS-Systemen verbessern können:

- **Zwei-Faktor-Authentifizierung**
  Neben der normalen Authentifizierung (Benutzername und Passwort) für den Zugriff auf den Administrationsbereich empfiehlt MELANI den Einsatz einer Zwei-Faktor-

[3] GovCERT.ch Blog-Post: „Outdate WordPress: Thousands of websites in Switzerland are vulnerable" http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable (Stand: 31. August 2015).

Authentifizierung. Ein solches zusätzliches *One Time Passwort (OTP)* lässt sich z. B. mit dem Einsatz von Google Authenticator realisieren. Dabei wird eine App auf dem Mobile Phone (Android, iOS, Blackberry) installiert, welche alle 60 Sekunden ein neues OTP generiert. Auf dem Webserver (CMS) kann Google Authenticator mit einem entsprechenden *Plug-In* realisiert werden, die bereits für zahlreiche Content-Management Systeme wie z. B. Wordpress oder Typo3 angeboten werden.

- **Einschränkung der Administrator-Zugriffe auf bestimmte IP-Adressen**
  Eine Zugriffs-Limitierung kann auf *IP-Adressen*, IP-Adressbereiche oder auf der *Geolocation* einer IP-Adresse basieren. Entsprechende Erweiterungen (Plug-Ins) existieren bereits für eine Vielzahl verschiedener CMS.

- **Einschränkung der Administrator-Zugriffe mittels .htaccess-Datei unter dem Apache Webserver**
  Diese Variante bietet den Vorteil, dass nicht nur der IP-Adressbereich eingeschränkt werden kann, es lässt sich so auch eine zusätzliche Authentifizierung (Benutzername / Kennwort) implementieren (Basic Authentication).

- **Absichern des Webmaster-Computers**
  Oftmals werden Websites und CMS auch durch gestohlene *FTP*-Zugangsdaten kompromittiert. Dies geschieht in der Regel mit Hilfe eines Trojaners auf dem Computer des Webmasters. Der Webmaster sollte deshalb stets sicherstellen, dass der verwendete Computer frei von Malware und mit einem aktuellen Virenschutz ausgestattet ist. Zusätzlich sollte, wenn möglich, die FTP-Verbindung verschlüsselt werden (Verwendung von sFTP).

- **Web Application Firewall**
  Web basierte Angriffe auf Websites lassen sich mit Hilfe einer Web Application Firewall (WAF) bereits blockieren, bevor diese die Applikation erreichen. Es gibt eine Vielzahl verschiedener WAF-Lösungen. Die bekannteste OpenSource-Lösung ist «ModSecurity».

- **Frühzeitige Erkennung von Sicherheitslücken**
  Ziel ist es, eine potenzielle Sicherheitslücke auf der eigenen Website zu identifizieren, bevor dies Kriminelle tun. Auch hier gibt es verschiedene kostenlose und kostenpflichtige Angebote im Internet.

Die vollständige Anleitung und Checkliste ist auf der Website von www.melani.admin.ch abrufbar:

Massnahmen zum Schutz von Content Management Systemen (CMS):

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

Zudem finden Sie dort eine Anleitung und Checkliste, was zu tun ist, wenn bereits ein Angriff erfolgt ist:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/anleitung-webseitenbereinigung.html

4 Lage national

4.1 Spionage

Im ersten Halbjahr gab es vor allem zwei Spionagefälle, welche das öffentliche Interesse weckten und in denen direkt oder indirekt die Schweiz betroffen war. Dabei muss jeweils unterschieden werden, ob der Angriff einem bestimmten Ziel in der Schweiz gilt oder ob die Schweizer Infrastrukturen als Mittel für Spionage gegen Dritte verwendet wird. Dass gerade im Spionagebereich nicht alle Fälle publik werden, liegt auf der Hand. Wenn es um Wirtschaftsspionage geht, sind Firmen erfahrungsgemäss sehr zurückhaltend, weil diese einen Reputationsverlust befürchten. Generell lässt sich sagen, dass ein ständiges Interesse und demzufolge ein ständiger Druck auf sensible Daten besteht. Ein Fall, der im ersten Halbjahr 2015 grosse Aufmerksamkeit erregte, ist die Entdeckung und Veröffentlichung der Schadsoftware «Duqu2», welche vor allem im Umfeld der Atomgespräche mit dem Iran aktiv gewesen sein soll.

4.1.1 Duqu reloaded: ausgeklügelte Spionagesoftware gegen Teilnehmer der iranischen Atomgespräche

Im März 2015 berichtete das Wall Street Journal gestützt auf Quellen im Weissen Haus, dass vertrauliche US-interne Gespräche bezüglich dem Nuklearabkommen mit dem Iran abgehört worden sein sollen. Israel wurde in diesem Fall von den USA als möglicher Urheber vermutet.[4,5] Israelische Politiker haben eine Beteiligung Israels aber umgehend scharf dementiert. Am 10. Juni 2015 gab das Sicherheitsunternehmen Kaspersky in einem Bericht bekannt, dass sowohl der Sicherheitsdienstleister selbst, als auch diverse Orte wo die Gespräche zu den Nuklearverhandlungen mit dem Iran stattgefunden haben von einem Spionagevorfall unter Einsatz von Schadsoftware betroffen waren. Die Schadsoftware beinhaltet zu Teilen «sehr ähnliche bis fast identische»[6] Softwarepassagen wie die 2011 bekannt gewordene Schadsoftware Duqu und weist ebenfalls Ähnlichkeiten zur Schadsoftware Stuxnet auf. Deshalb taufte Kaspersky die Schadsoftware Duqu2. Wie bei Spionagevorfällen üblich, lassen die aus den technischen Analysen hervor gehenden Angriffsmuster allerdings keinen eindeutigen Schluss auf die Täterschaft zu.

Die Ziele waren in den nun aufgedeckten Fällen unter anderem die Feierlichkeiten zum 70. Jahrestag der Befreiung des Konzentrationslagers Auschwitz-Birkenau und die P5+1 Gespräche über das iranische Atomprogramm. An drei Orten, wo die P5+1 Verhandlungen stattfanden, haben Computerexperten die Schadsoftware entdeckt. Die letzten Verhandlungsrunden fanden in Lausanne, Montreux, Genf, München und Wien statt.[7]

In der Schweiz hat der Bundesrat die Bundesanwaltschaft aufgrund von Hinweisen des Nachrichtendienstes des Bundes (NDB) bereits am 6. Mai 2015 ermächtigt[8], in diesem Fall ein Strafverfahren gegen Unbekannt zu eröffnen. Bei einer Hausdurchsuchung Mitte Mai

---

4 http://www.wsj.com/articles/israel-spied-on-iran-talks-1427164201 (Stand: 31. August 2015).

5 http://www.theguardian.com/world/2015/mar/24/israel-spied-on-us-over-iran-nuclear-talks (Stand: 31. August 2015).

6 http://www.zeit.de/digital/internet/2015-06/duqu-2-kaspersky-labs (Stand: 31. August 2015).

7 http://www.kaspersky.com/about/news/virus/2015/Duqu-is-back (Stand: 31. August 2015).

8 http://www.heise.de/newsticker/meldung/Kaspersky-Trojaner-hatte-auch-Atomverhandlungen-im-Visier-2689929.html (Stand: 31. August 2015).

wurden in Genf verschiedene Geräte beschlagnahmt.[9] Auch in Österreich starteten die Behörden Ermittlungen wegen mutmasslicher Spionage in diesem Fall. Der Fokus lag hier auf dem Wiener Hotel Palais Coburg, in dem ebenfalls mehrere Treffen für Atomverhandlungen stattgefunden hatten.[10]

Dieser Spionagekomplex zeigt, dass nicht nur die eigentlichen Ziele, sondern auch direkt das Sicherheitsunternehmen Kaspersky angegriffen worden ist. Die Angreifer haben anscheinend das Firmennetzwerk durchforstet, um an Daten zu gelangen, welche einen Angriff auf die Ziele erleichtern sollten. IT-Sicherheitsunternehmen stellen einen fundamentalen Pfeiler für das Grundvertrauen in das Internet dar. Angriffe mit dem Ziel diese für weitere zu missbrauchen, schaden daher ganz grundsätzlich den Bestrebungen, das Internet als vertrauenswürdiges Medium u.a für geschäftliche Tätigkeiten weiterzubringen. Entsprechend sollte die Diskussion über Leitplanken weiter forciert werden.

Für weiterführende Informationen siehe MELANI Halbjahresbericht 2013/2 Kapitel 5.1

https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html

4.1.2 Swisscom-Leitungen angeblich von BND und NSA abgehört

Laut den Aussagen des österreichischen Abgeordneten Peter Pilz soll der deutsche Bundesnachrichtendienstes (BND) und die amerikanische National Security Agency (NSA) unter dem Namen «Operation Eikonal» angeblich Transit-Internetdaten am Internetknoten Frankfurt nach bestimmten Suchbegriffen durchforstet haben.[11] Ziel der Suche war, Informationen bezüglich Terrorverdächtigen und Waffenschmugglern zu erlangen. Die Suchbegriffe wurden dem BND jeweils von der NSA übermittelt. Allerdings seien hier im Laufe der Zeit aber immer wieder seltsame, nicht themenrelevante Suchbegriffe beobachtet worden, die allenfalls nur indirekt mit diesem Auftrag in Verbindung gebracht werden konnten.

Im Fokus der Operation standen 250 Transit-Leitungen. Darunter sollen sich gemäss der Liste von Herrn Pilz auch neun Leitungen befunden haben, deren Endpunkte in der Schweiz von der Swisscom betrieben wurden und nach Prag, Sydney, Tokio, Seoul, Luxemburg, Warschau oder Moskau führten. Die Schweiz wäre somit eines von 64 Ländern, die von den BND/NSA-Abhörmassnahmen betroffen gewesen sind. Die Aussagen stützen sich auf einen Vertrag zwischen BND und deutscher Telekom von 2004, welcher von Herrn Pilz veröffentlich wurde. Laut Aussagen von Swisscom sind diese Leitungen aktuell jedoch nicht mehr in deren Besitz.[12]

---

9 http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf (Stand: 31. August 2015).

10 http://www.tagesschau.de/ausland/duqu-103.html (Stand: 31. August 2015).

11 http://www.zeit.de/politik/deutschland/2015-04/bnd-nsa-kooperation-verantwortliche (Stand: 31. August 2015).

12 http://www.nzz.ch/schweiz/bnd-und-nsa-sollen-swisscom-kunden-ausspioniert-haben-1.18549890 (Stand: 31. August 2015).

Der Nachrichtendienst des Bundes hat unter anderem zum Themengebiet Wirtschaftsspionage die Broschüre «Prophylax» publiziert. Diese ist Bestandteil einer Präventions- und Sensibilisierungsaktion im Bereich der Nonproliferation und der Wirtschaftsspionage. Sie dient zur Sensibilisierung von Unternehmen und Bildungsinstitutionen und informiert darüber, wie Gefahren und illegale Geschäfte erkannt und verhindert werden können und was die Behörden zur Prävention und Bekämpfung unternehmen.

http://www.vbs.admin.ch/internet/vbs/de/home/documentation/publication/snd_publ.html

4.2 Datenabflüsse

Elektronischer Datendiebstahl kann die Tat von Akteuren mit unterschiedlichen Motiven sein: Staaten, die an den Daten selbst interessiert sind, die ihnen beispielsweise einen strategischen oder wirtschaftlichen Vorteil verschaffen oder Cyberkriminelle, die auf schnelles Geld aus sind. Eine der zur Zeit häufigsten Methoden, um an dieses schnelle Geld zu kommen, ist die Erpressung mit gestohlenen Daten, welche als Druckmittel verwendet werden, um das Opfer zu einer Zahlung zu bewegen. Wir haben diese Thematik bereits im letzten Halbjahresbericht[13] beschrieben.

4.2.1 Rex Mundi

Auf dieses Vorgehen hat sich die Gruppe Rex Mundi spezialisiert. Sie trat 2014 mit zahlreichen Opfern vor allem in Belgien in Erscheinung. Im Januar 2015 war auch die Schweiz betroffen. Der Vorfall, der ein Unternehmen in der Romandie betraf, war in allen Punkten identisch mit dem zuvor beobachteten Vorgehen. Zuerst erfolgte eine *SQL-Injection* für den Zugriff auf eine Datenbank. Diese enthielt Informationen aus einem Kontaktformular auf der Webseite der Firma unter anderem persönliche Angaben (Adresse, Telefonnummer usw.) und die Mitteilungen aus dem Formular. Die Täter verlangten anschliessend ein Lösegeld, ansonsten würden sie die Informationen veröffentlichen. Mit dem zu erwartenden Imageschaden, der beim Bekanntwerden des Angriffs droht, wird versucht eine Zahlung zu erzwingen. Um Druck auf das Unternehmen auszuüben, machte Rex Mundi wie gewohnt das Ereignis, seine Forderungen und die Reaktion des Unternehmens auf Twitter publik. Da sich die Firma nicht erpressen liess, wurden die Daten veröffentlicht. Die Firma hatte ihre Kundschaft im Vorfeld kontaktiert und über die Sicherheitslücke und die mögliche Verwendung der Daten informiert.

Neben dem Imageschaden für das Unternehmen können je nach Art und Wert der Daten bei einer Veröffentlichung auch andere Probleme auftreten. Dies trifft natürlich vor allem auf vertrauliche Informationen über das Unternehmen und seine Tätigkeit zu. Im Fall Rex Mundi liegt die Problematik allerdings eher darin, dass die veröffentlichten persönlichen Kundendaten für nachgelagerte Social Engineering Betrugsversuche missbraucht werden können. Der Wert der Daten bietet zusätzlich die Möglichkeit, diese zu Geld zu machen, im Speziellen, falls das Unternehmen nicht zahlt. Man denke hier vor allem an einen Weiterverkauf der Daten auf dem Untergrundmarkt. Diese Fälle werfen einmal mehr die

[13] MELANI Halbjahresbericht 2014/2, Kapitel 5.3: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (Stand: 31. August 2015)

Frage der Sicherheit von Webseiten auf, die oft als Vektoren für verschiedene Angriffsarten dienen.

MELANI hat diese Fragen bereits mehrfach thematisiert (siehe z.B. Halbjahresbericht 2014/2, Ziff. 3.5 «CMS-Schwachstellen und fehlende Sensibilität bei Web-Administratoren» und das Dokument

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

4.3 Industrielle Kontrollsysteme

Das Thema Industrielle Kontrollsysteme wird stets wichtiger, da heute immer mehr Prozesse mittels IKT gesteuert werden. In diesen Themenbereich gehört auch die *Industrie 4.0*, die vierte industrielle Revolution. Allerdings wird der Begriff industrielle Kontrollsysteme sehr weit gefasst und kann von der Steuerung eines Kernkraftwerkes bis hin zum Gebäude-Management so ziemlich alles umfassen. Dies kann unter Umständen zu einer Vermischung verschiedener Problematiken führen. In den nachfolgenden Kapiteln beleuchten wir vor allem kritische Systeme. Zu Systemen, mit hoher Kritikalität gehören sicherlich diejenigen, welche zur Elektrizitätsversorgung beitragen.

4.3.1 Honeypot Wasserkraftwerk – 31 Attacken

Eine Möglichkeit herauszufinden, wie real Angriffsrisiken sind, ist die Verwendung von so genannten *Honeypots*. Hierbei werden kontrolliert Systeme ins Internet gestellt, welche die richtigen Ziel-Systeme imitieren und so Angriffe anziehen, ohne dass ein Schaden angerichtet wird.

Die Sonntagszeitung[14] präsentierte im Februar 2015 eine solche Studie, die sich mit Wasserkraftwerken befasste. Dazu wurde ein System aufgesetzt, das sich drei Wochen lang als Wasserkraftwerk ausgegeben hat. Das Ergebnis waren 31 Angriffe, unter denen sich auch drei Angriffe von Hackern befanden, welche versuchten, einen Fehler im System zu provozieren, respektive das System zum Absturz zu bringen. Wenn es auch ein Modellversuch ist und sicherlich nicht vollständig auf im Einsatz befindliche Systeme übertragen werden kann, zeigt es doch das Interesse der Angreifer an solchen Systemen. Nicht zum ersten Mal wurde in einem Modellversuch gezeigt, ob und wie in die Steuersysteme besonders kleinerer Wasserkraftwerke eingedrungen werden kann. Bereits vor zwei Jahren hat ein entsprechender Bericht für Schlagzeilen gesorgt: Gerade einmal 15 Minuten hat es damals gedauert, um ein Kraftwerk im Kanton Glarus zu übernehmen.[15] Auch wenn das Hacken eines Kleinkraftwerkes noch keine Auswirkung auf das Stromnetz haben muss, so könnte doch ein orchestrierter Angriff auf zahlreiche kleinere Systeme zu plötzlichen Stromschwankungen und somit zu möglichen Kettenreaktionen bis hin zu einem grossflächigen Stromausfall führen.

---

14 http://www.sonntagszeitung.ch/read/sz_08_02_2015/nachrichten/Angriff-auf-die-Stromversorgung-27051 (Stand: 31. August 2015).

15 http://www.srf.ch/sendungen/10vor10/spur-von-snowden-entlastung-fuer-sachs-angriffe-via-internet (Stand: 31. August 2015).

Es stellt sich die grundlegende Frage, wieso es trotz bekannter Verwundbarkeiten und anscheinend auch trotz des Interesses seitens der Angreifer (wenigstens an den Honeypot-Systemen) nicht zu grösseren Ausfällen oder sonstigen Pannen kommt. Die Antwort auf diese Frage lässt sich nicht einfach beantworten. Eine Möglichkeit ist ein fehlendes Geschäftsmodell der Hacker: Da auf die Systeme - neben dem virtuellen Zugriff - meistens auch ein physischer Zugriff besteht, kann ein System bei einem Angriff leicht vom Internet getrennt werden (Autonomie-Anforderungen an untergeordnete Rückfallebenen). Ein möglicher anderer Grund ist eine gewisse Hemmschwelle seitens der in erster Linie pekuniär motivierten Angreifer, da man nicht genau weiss, welche Auswirkungen (beispielsweise auf Menschenleben) ein Angriff auf ein solches System hat.

4.3.2 Offene Systemsteuerung von Wasserversorgungssystemen

Nicht immer ist es für die Melde- und Analysestelle Informationssicherung (MELANI) einfach abzuschätzen, als wie kritisch offene Systeme einzustufen sind, sowie ob und wie allenfalls sensible Systeme betroffen sind[16]. Dies zeigte ein Beispiel vor zwei Jahren, als Hacker am Chaos Communication Congress (CCC) zahlreiche Screenshots von Systemen publizierten, in welche die Hacker angeblich eingedrungen waren. Unter diesen Bildern befand sich auch die Wasserversorgung einer kleinen Schweizer Gemeinde. Eine genauere Analyse und Nachfrage bei der Gemeinde ergab dann allerdings, dass der Zugang zwar nicht publiziert ist, interessierte Bürger sich aber durchaus diese Daten ansehen dürfen. Auf den Grafiken sah man, wieviel Wasser aus den einzelnen Quellen in das Reservoir fliesst. Kritische Daten waren jedoch keine ersichtlich und auch Manipulationen waren über den Fernzugang nicht möglich.

Dass dies auch durchaus anders sein kann, zeigte ein ähnlicher Fall der aktuellen Berichtsperiode. Auch hier ging es um eine Schweizer Wasserversorgung und um die Anzeige von Werten einzelner Quellen und Reservoire. Bei einer näheren Analyse hat MELANI jedoch erkannt, dass sich auf der Website fest einprogrammierte Passwörter befanden, um die Daten von den Steuergeräten abzuholen und damit auf die Steuerkomponenten zugreifen zu können. Ein so leicht zugängliches Passwort bietet wiederum eine gefährliche, zusätzliche Angriffsfläche.

[16] http://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (Stand: 31. August 2015).

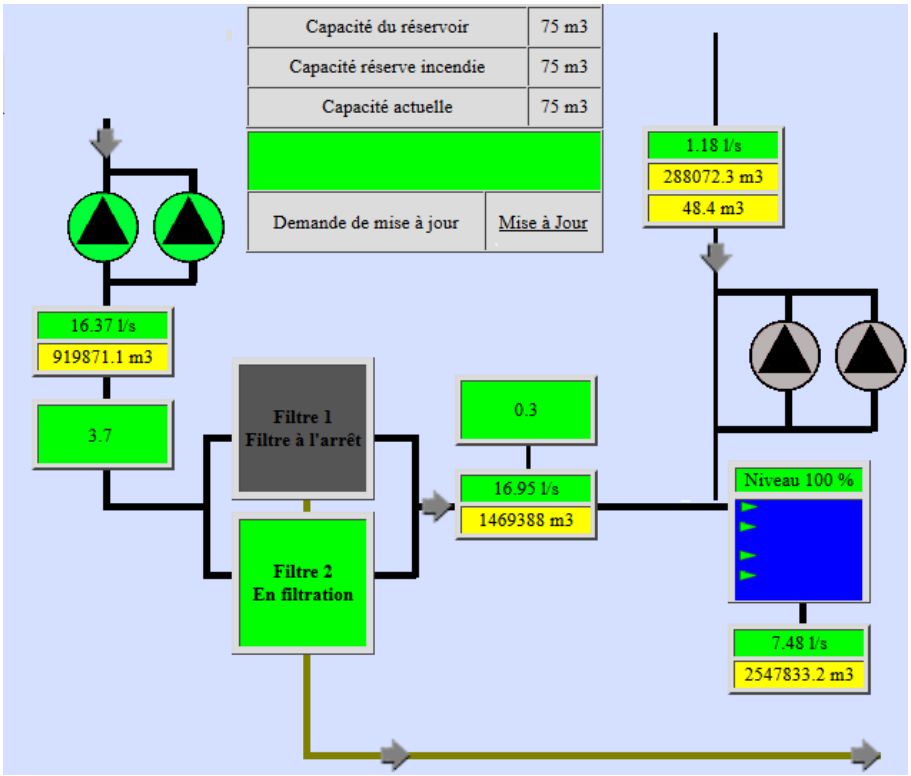


Abbildung 2: Beispiel einer öffentlich zugänglichen Plattform einer Wasserversorgung in der Schweiz

MELANI stellt eine Checkliste mit Massnahmen zum Schutz von Industriellen Kontrollsystemen zur Verfügung. Die aufgeführten Massnahmen sollten in einen übergeordneten Sicherheitsprozess eingebettet sein, welcher gewährleistet, dass die Massnahmen angewendet, regelmässig geprüft und kontinuierlich verbessert werden. Weiter ist es wichtig, dass der Betreiber einer Anlage seine aktuelle Bedrohungslage kennt, diese regelmässig überprüft und die Erkenntnisse in die Implementierung und Verbesserung der Sicherheitsmassnahmen einfliessen lässt. Dazu ist eine enge Zusammenarbeit zwischen Risikomanagement, Engineering und Betrieb von grosser Bedeutung.

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) hat im Februar 2015 eine neue Studie veröffentlicht. Diese liefert Informationen über die Herausforderungen und Empfehlungen für die Entwicklung von Systemen zur Zertifizierung der Fähigkeiten von Cyber-Experten, die mit Industriellen Kontrollsystemen (ICS) sowie Überwachungskontrolle und Datenerfassung (SCADA) in Europa arbeiten.

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

4.4 Angriffe (DDoS, Defacements)

Privatpersonen und Unternehmen in der Schweiz sind weiterhin das Ziel verschiedener Arten von Angriffen. Ein Angriffsziel stellen insbesondere Webseiten dar. Vor allem für Unternehmen, die auf eine verlässliche Präsenz im Internet angewiesen sind, kann sich die Verwundbarkeit gegenüber *DDoS-Angriffen* und *Defacements* als problematisch erweisen.

4.4.1 DDoS und Erpressung: Angriffswelle DD4BC

Erpressung ist derzeit eine beliebte Masche der Cyberkriminellen, die auf einen schnellen finanziellen Gewinn aus sind. Über verschiedene Angriffsarten wird versucht, von einem Opfer Geld zu erpressen. Dazu gehören auch DDoS-Angriffe. DD4BC ist eine Gruppe, die sich seit Juli 2014 auf diese Art Angriff spezialisiert hat. Ihr Markenzeichen ist ihre unspezifische Auswahl der Ziele: DD4BC war sowohl in Europa als auch in den USA, Asien und Ozeanien aktiv. Ausserdem waren zeitweise verschiedene Sektoren im Fokus. Nachdem sie sich auf die Bitcoinindustrie und die Online-Casinos konzentriert hatten, griff DD4BC Finanzunternehmen an und war im ersten Halbjahr 2015 besonders in der Schweiz aktiv. MELANI wurden über ein Dutzend Fälle gemeldet, welche unterschiedliche Unternehmen vor allem im Finanzbereich betrafen. Das Vorgehen des Akteurs stimmte mit demjenigen überein, was in anderen Ländern beobachtet wurde. Der Angriff beginnt in der Regel mit einem schwachen DDoS-Angriff (in der Regel 10-15 GBs), um die Möglichkeiten des Angreifers zu demonstrieren. Daraufhin erpresst der Betrüger das Opfer per E-Mail. Will das Opfer einen gravierenderen Angriff verhindern, muss es 30-40 Bitcoins zahlen (was zum Zeitpunkt des Angriffe in etwa 7500-10 000 CHF entsprach). DD4BC droht dabei mit einer Angriffsstärke von 400-500 GBs. Ob die Gruppe tatsächlich dazu in der Lage wäre, hat sie bisher noch nie unter Beweis gestellt. Bei Nichtzahlung wurden zum Teil Angriffstärken bis zu 30 GBs[17] beobachtet, während in anderen Fällen die Drohung gar nicht erst wahrgemacht wurde.
Nichterreichbarkeit im Internet kann eine grosse finanzielle Einbusse bedeuten, besonders wenn es sich um eine kommerzielle Webseite handelt. Der Angreifer hofft, dass das Opfer die drohenden negativen Folgen vermeiden will und deshalb zahlt.

MELANI empfiehlt Opfern solcher Angriffe, sich nicht erpressen zu lassen und umgehend den Host- und den Upstream-Provider zu kontaktieren, um Schutzmassnahmen zu ergreifen. Ausserdem kann Strafanzeige bei der Kantonspolizei eingereicht werden. MELANI hat ein Themenpapier zu DDoS-Angriffen und den Gegenmassnahmen herausgegeben:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

4.4.2 Defacements von Westschweizer Webseiten

Im ersten Halbjahr wurden erneut Wellen von Webseitenverunstaltungen (Defacements) namentlich in der Westschweiz registriert. Im Nachgang zum Anschlag auf Charlie Hebdo in Paris wurden zahlreiche Seiten vor allem in Frankreich, aber auch einige in der Westschweiz

[17] Externe Berichte bestätigen Angriffe bis zu 60 Gb/s
Siehe: http://pages.arbornetworks.com/rs/082-KNA-087/images/ATIB2015-04DD4BC.pdf (Stand: 31. August 2015).

von verschiedenen Gruppierungen mit islamistischer Propaganda und Sympathisantenbotschaften zum Anschlag verunstaltet. In Frankreich verzeichneten die Behörden 1300 Angriffe mit 25000 gehackten Seiten (siehe Kapitel 5.4.3.). Die betroffenen Schweizer Seiten waren offenbar wegen der Zugehörigkeit zum französischen Sprachraum ins Visier geraten. Es ist anzunehmen, dass die Angreifer nicht gezielt Schweizer Seiten angegriffen haben, sondern diese eher für französische Seiten hielten.

Im April wurden MELANI weitere Defacements von Westschweizer Webseiten gemeldet, über die auch in der Presse berichtet wurde. Auch hier wurden die gehackten Seiten von einer Gruppe, die sich zum Islamischen Staat (IS) bekannte, mit islamistischer Propaganda verunstaltet. Von einer Welle zu sprechen ist aber in diesem Fall übertrieben. Die Analyse der MELANI bekannten Fälle ergab, dass die Attacken allesamt von einem Angreifer stammten. Laut der Webseite zone-h.org, die solche Fälle erfasst und auflistet, soll ein Hacker mit dem Pseudonym «cwne» zwischen dem 24. und 26. April 2015 180 Webseiten gehackt haben. Allerdings waren alle Seiten beim gleichen Provider gehostet. Der Hacker hat sich wohl eine Sicherheitslücke auf einem Host-Server zu Nutze gemacht auf dem die 180 Webseiten gespeichert waren. Es handelte sich somit um ein so genanntes «Massendefacement». Das Beispiel zeigt, wie mit nur einem Angriff eine Vielzahl von Webseiten verunstaltet werden kann und damit eine grosse Sichtbarkeit erlangt wird, vor allem wenn es sich bei den betroffenen Seiten um Unternehmen oder Organisationen in einem begrenzten Umkreis handelt. Von den Medien oder der Öffentlichkeit wird dies als eine Aktion grossen Ausmasses wahrgenommen. In Tat und Wahrheit handelt es sich aber nur um das Ausnützen einer Lücke auf einem einzigen Server und durch einen einzelnen Hacker. Zum Teil wird versucht, einen Zusammenhang zwischen den gehackten Seiten und der verbreiteten Botschaft herzustellen, den es in der Regel gar nicht gibt. Meistens nutzen die Angreifer einfach unspezifisch verwundbare Seiten unabhängig von deren Inhalt.

Das Einhalten von Grundregeln der Sicherheit wie regelmässiges Aktualisieren der Programme auf der Webseite und dem Webserver hilft, sich vor derartigen Angriffen zu schützen. MELANI hat dazu folgendes Dokument herausgegeben:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

4.5 Social Engineering, Phishing

Neben den technischen Angriffen sind auch Methoden, welche die menschlichen Schwächen ausnützen, bei den Angreifern beliebt. Wie viel mit Social Engineering möglich ist, zeigt eindrücklich ein Fall aus den USA: Ein Manager des US-Unternehmens Scoular überwies sukzessive 17,2 Millionen US-Dollar an Betrüger auf ein chinesisches Bankkonto im Glauben, er handle im direkten Auftrag seines Chefs. Eine Studie der Wirtschaftsprüfungsgesellschaft KPMG stützt diese Beobachtung und zeigt, dass Firmen immer noch allzu sehr auf Technologie setzen und den menschlichen Faktor beim Schutz vor Cyber-Angriffen vernachlässigen. Grundsätzlich sollte ein integrierter und ausgewogener

Ansatz verfolgt werden, der Menschen und Prozesse ebenso berücksichtigt wie Technologien.[18]

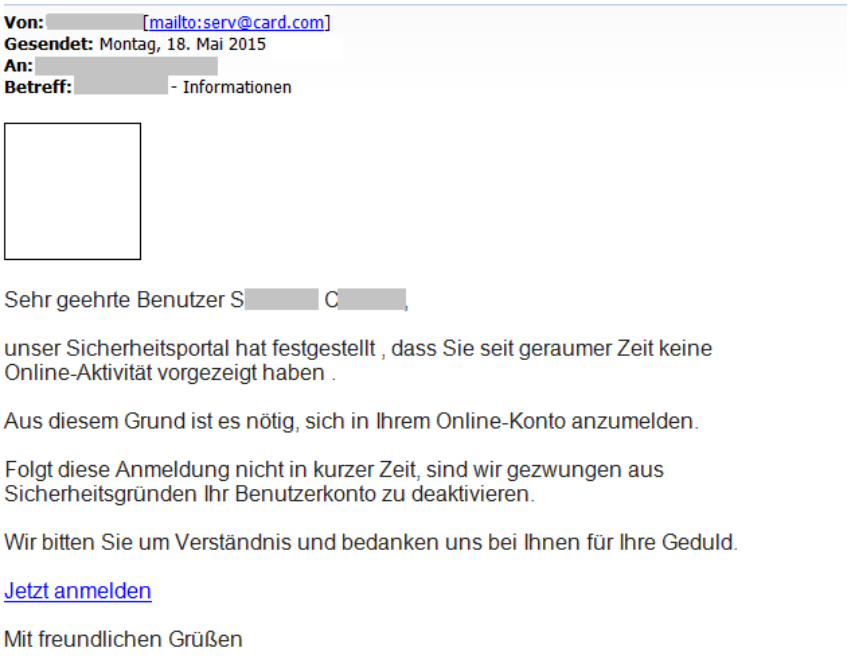
4.5.1 Phishing – Angriffe auf Kantonalbanken, Kreditkartendaten, Verbesserung der Phishing-E-Mails

Ein grosses, wenn nicht das grösste Themengebiet bei *Social Engineering* ist nach wie vor *Phishing*. Bei den meisten beobachteten Angriffen handelt es sich mittlerweile um Standardangriffe. Dabei wird zuerst ein Finanzinstitut ausgewählt, gegen dessen Kundschaft ein Phishing-Angriff gestartet werden soll. Danach wird sowohl das Seitenlayout als auch das E-Mail-Layout kopiert und aufgesetzt, eine für das Opfer glaubwürdige Geschichte erfunden und danach über Tage und Monate die gleichen Angriffe gefahren. Dabei gibt es Phishing-Wellen, bei denen die Webseiten sogar jedes Mal beim gleichen Provider gespeichert werden. Nach dem Deaktivieren der Phishingseite durch den Provider dauert es jeweils nur eine kurze Zeit und die gleiche Seite ist an anderer Stelle wieder online.

So verhielt es sich auch bei den beobachteten Phishing-Angriffen gegen Schweizer Kantonalbanken, die im ersten Halbjahr 2015 vermehrt registriert wurden. Ein Merkmal, dass diese Angriffswellen auszeichnete, war, dass nicht die Kantonalbank eines einzelnen Kantons das Ziel war, sondern generell Kunden von Kantonalbanken der ganzen (deutschsprachigen) Schweiz angesprochen wurden. Damit erhöhte sich die potentielle Opferzahl selbstredend. Erst in einem zweiten Schritt musste das Opfer dann die Kantonalbank präzisieren, wo es sein E-Banking Konto hat und dann natürlich auch seine persönlichen Daten angeben.

Aufgrund der steigenden Sensibilität der E-Banking Kunden müssen sich die Angreifer jedoch immer neue und bessere Angriffsmethoden einfallen lassen. Hierzu zählt auch die persönliche Anrede mit Vor- und Nachnamen, mit der das Vertrauen der potenziellen Opfer gewonnen werden soll. Flächendeckend durchgesetzt hat sich diese Methode bis heute zwar nicht – zu gross ist wohl immer noch der Aufwand, Vor- und Nachnamen mit den entsprechenden E-Mail-Adressen zu korrelieren. Bei diversen Phishing-Wellen im zweiten Halbjahr 2015 wurde aber genau dieses Vorgehen gewählt. Wo die Angreifer diese Daten jeweils her haben, ist schwer zu sagen. Sie können beispielsweise aus kompromittierten E-Mail-Accounts stammen, die von den Kriminellen ausgelesen werden.

[18] http://www.kpmg.com/CH/de/topics/cyber-security/Seiten/default.aspx?utm_source=mediarelease&utm_medium=email&utm_content=medien-de&utm_campaign=cybersecurity (Stand: 31. August 2015).



Von: [mailto:serv@card.com]
Gesendet: Montag, 18. Mai 2015
An:
Betreff: - Informationen

Sehr geehrte Benutzer S C,

unser Sicherheitsportal hat festgestellt , dass Sie seit geraumer Zeit keine Online-Aktivität vorgezeigt haben .

Aus diesem Grund ist es nötig, sich in Ihrem Online-Konto anzumelden.

Folgt diese Anmeldung nicht in kurzer Zeit, sind wir gezwungen aus Sicherheitsgründen Ihr Benutzerkonto zu deaktivieren.

Wir bitten Sie um Verständnis und bedanken uns bei Ihnen für Ihre Geduld.

Jetzt anmelden

Mit freundlichen Grüßen

Abbildung 3: Beispiel eines Phishing E-Mails mit Verwendung von Vor- und Nachnamen bei der Anrede

Dass die gezielte Anrede, eine plausible Geschichte und somit ein professionelles Social Engineering eine wichtige Rolle spielen, zeigen Fälle, bei welchen im Vorfeld eines Angriffs die Kundendatenbank einer Firma gehackt und kopiert worden ist. Dies geschieht meist über *SQL-Injections*. Anschliessend folgt ein gezieltes E-Mail im Namen der Firma und mit dem Verweis auf eine perfekt imitierte Webseite, dass zu irgendwelchem Zweck die Kreditkartennummer hinterlegt werden müsse. Da das Opfer wahrscheinlich schon in Kontakt mit der wirklichen Firma gestanden ist und der Vorwand plausibel klingt, ist die Chance gross, dass ein Opfer darauf hereinfällt. Der betroffenen Firma bleibt somit nur, die Kunden umgehend über diesen Betrugsversuch zu informieren.

4.5.2 Phishing nach Defacements und manchmal auch umgekehrt

MELANI hat in letzter Zeit zunehmend auch einen Zusammenhang zwischen *Defacements* und *Phishing-V*ersuchen festgestellt: Damit die Betrüger eine Phishingseite einrichten können, müssen sie zuerst eine Domäne kaufen oder aber eine bereits bestehende Website kompromittieren, indem sie Sicherheitslücken ausnutzen. Bei Defacements werden ebenfalls Sicherheitslücken bei Websites ausgenutzt, um anschliessend darauf Inhalte zu ändern und persönliche, religiöse oder politische Aussagen zu platzieren. Zudem werden verunstaltete Webseiten oft auf öffentlich zugänglichen Seiten wie zone-h.org[19] publiziert. Somit ist es für Phisher einfach, Websites mit bekannten Lücken zu finden, diese ebenfalls auszunutzen und ihre Phishingseiten zu platzieren. Die umgekehrte Situation, d. h. die Verunstaltung einer bestehenden Phishing-Seite, ist dagegen viel weniger wahrscheinlich. In erster Linie deshalb, weil es keine öffentlichen Listen mit Phishing-Seiten gibt und zweitens, weil diese Seiten, wenn sie entdeckt werden, so schnell wie möglich vom Netz genommen werden.

[19] Zone-h.org ist ein Archiv von verunstalteten Webseiten

Im Mai 2015 beobachtete MELANI aber zum ersten Mal genau eine solche Vorgehensweise: Zuerst wurde ein normaler Phishing-Angriff gegen ein Schweizer Finanzinstitut gemeldet. Wie in solchen Fällen üblich, wurde die Seite untersucht und anschliessend dem zuständigen Provider zur Kenntnis gebracht, damit dieser die Seite deaktivieren konnte. Noch bevor allerdings der Provider reagieren und die betrügerische Seite löschen konnte, wurde der Phishingangriff durch einen «Hacktivisten» bereits vereitelt. Indem der «Hacktivist» die Seite seinerseits mit einer Botschaft gegen Fremdenfeindlichkeit versah, hat er - wahrscheinlich unabsichtlich - verhindert, dass potentielle Opfer ihre Daten auf der Phishing-Seite preisgeben konnten.

4.5.3 Gefälschte Steuerformulare

Zahlreiche Firmen im Raum Genf haben im ersten Halbjahr angeblich von den Genfer Steuerbehörden ein E-Mail mit einem angehängten Formular erhalten. Das Formular, auf welchem Gewinne auf Immobilien und andere Unternehmensdetails deklariert werden mussten, sollte anschliessend zusammen mit der letzten Mietrechnung an eine E-Mail-Adresse gesendet werden. Das versendete Formular existiert zwar tatsächlich, die angegebene Rücksende-Adresse hatte aber mit den Genfer Steuerbehörden nichts zu tun und gehörte einem Betrüger.

Ein ähnlicher Fall wurde auch im Kanton Waadt beobachtet[20].

Doch für welche Zwecke können solche Daten missbraucht werden, wenn diese erst einmal im Besitze der Betrüger sind? Es dürfte sich hier vornehmlich um eine Vorbereitungshandlung zu sogenannten «President Scams» handeln. Hierbei werden durch die Angreifer im Vorfeld Informationen über die Firma eingeholt, um sich so ein genaues Bild über die Organisation und das Umfeld des Ziels zu machen. Diese Informationen werden zum Teil auch durch aktive Recherche, wie die hier beschriebene durchgeführt. Anschliessend beginnt der eigentliche Angriff. In der Regel wird dabei ein E-Mail an einen Mitarbeitenden der Finanzabteilung versendet, welches vorgibt von einem Mitglied des Kaders zu stammen. Das versendete E-Mail handelt dann meist von laufenden, vertraulichen Finanzgeschäften. Die Betrüger betonen den einmaligen Charakter und die Vertraulichkeit des Auftrages, jedoch auch die Dringlichkeit, welche die Situation erfordere. In manchen Fällen versuchen die Betrüger mit parallelen Telefonanrufen dem Szenario noch mehr Glaubwürdigkeit zu verleihen.

Der Kanton Genf hat auf seiner Website eine Warnmeldung aufgeschaltet.[21]

---

[20] http://www.24heures.ch/vaud-regions/arnaqueurs-utilisent-adresse-fisc-vaudois/story/10817017 (Stand: 31. August 2015).

[21] http://ge.ch/impots/courrier-lectronique-frauduleux (Stand: 31. August 2015).

Die wichtigsten Verhaltensregeln zum Umgang mit E-Mails helfen, sich vor Phishing und anderen Betrugsarten zu schützen:

Misstrauen Sie E-Mails, die Sie unaufgefordert erhalten: Seien Sie nicht nur bei E-Mails von Ihnen unbekannten Personen kritisch, sondern auch bei bekannten Absendern. Besonders vertrauenswürdige Firmen werden gerne als gefälschte Absender-Adressen missbraucht.

- Seien Sie skeptisch, wenn Sie E-Mails erhalten, die eine Aktion von Ihnen verlangen und ansonsten mit Konsequenzen drohen (Geldverlust, Strafanzeige oder Gerichtsverfahren, Konto- oder Kartensperrung, Verpasste Chance, Unglück).
- Klicken Sie in verdächtigen E-Mails auf keine Anhänge und folgen Sie keinen Links - Sie riskieren sonst, Ihr Gerät mit Schadsoftware zu infizieren. Fragen Sie im Zweifelsfall beim vermeintlichen Absender über eine auf seiner Webseite angegebene Kontaktmöglichkeit nach, worum es sich genau handelt und ob das Mail tatsächlich von ihm stammt.
- Die Grundregel, bei zweifelhaften oder ungewöhnlichen Kontaktaufnahmen keine internen Informationen preiszugeben und keinen Aufforderungen nachzukommen, ist angesichts der derzeitigen Fälle aktueller denn je.

Speziell für Firmen:

- Sämtliche Prozesse, welche den Zahlungsverkehr betreffen, sollten firmenintern klar geregelt sein und von den Mitarbeitenden in allen Fällen eingehalten werden.
- Insbesondere empfiehlt MELANI eine Sensibilisierung der Mitarbeitenden bezüglich dieser Vorfälle, vor allem der Mitarbeitenden in Schlüsselpositionen.
- Bei ungewöhnlichen Kontaktaufnahmen und Aufforderungen ist es empfehlenswert, innerhalb der Firma telefonisch Rücksprache zu nehmen, um die Richtigkeit des Auftrages zu verifizieren.
- Ein Merkblatt für KMU bezüglich IKT-Sicherheit finden Sie auf der MELANI Website unter: https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

4.6 Crimeware

Crimeware ist eine von Wirtschaftskriminellen weiterentwickelte Form der Schadsoftware, die kriminologisch zur Computerkriminalität zählt und rechtlich unter Internetbetrug anzusiedeln ist. In Sachen Crimeware sind E-Banking-Trojaner weiterhin sehr verbreitet, wie die untenstehende Statistik zeigt. Bei einem Grossteil der infizierten Systeme in der Schweiz, welche MELANI gemeldet worden sind, handelt es sich um E-Banking-Trojaner wie Beispielsweise «Torpig», «Dyre», «Tinba», «Gozi» oder «ZeuS».

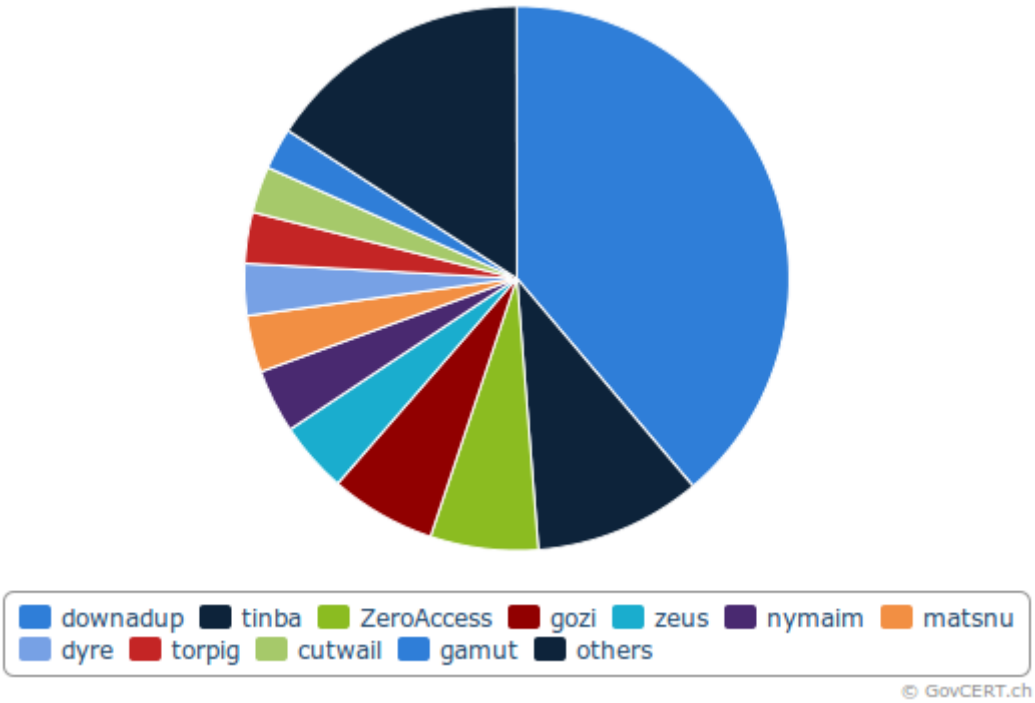


Abbildung 4: Verteilung der Schadsoftware in der Schweiz, welche MELANI bekannt ist. Stichtag ist der 30.Juni 2015. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

Bei der geografischen Verteilung zeigen vor allem die beiden Kantone Zürich und Wallis eine höhere Infektionsrate auf als andere Kantone (unter Berücksichtigung der Anzahl Einwohner).

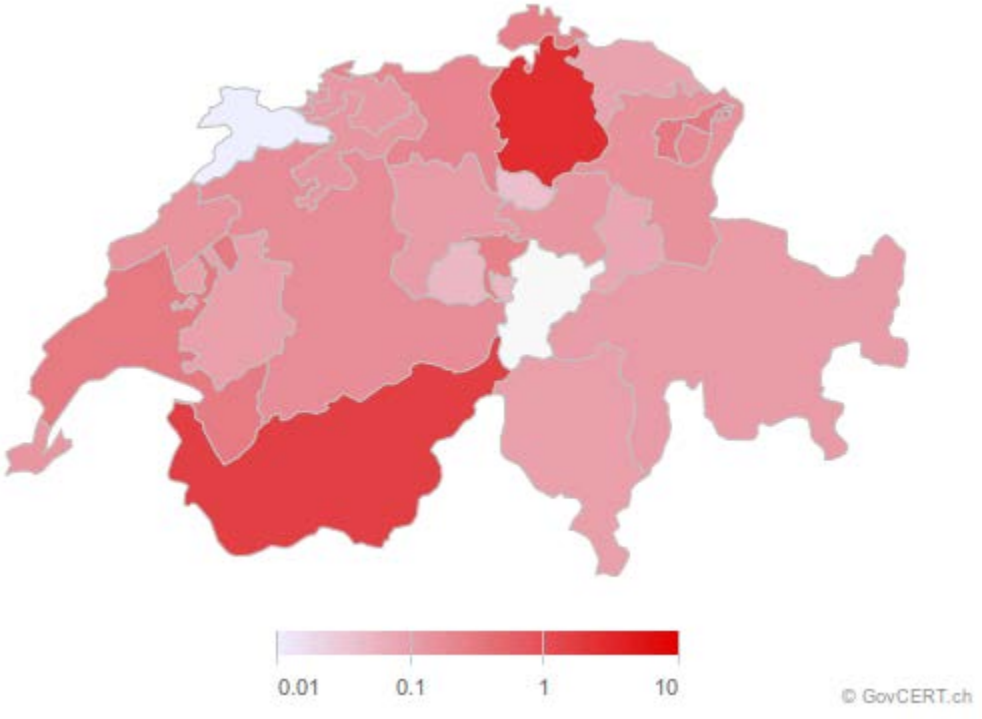


Abbildung 5: Anzahl Infizierungen pro Kanton unter Berücksichtigung der Einwohnerzahl. Stichtag ist der 30.Juni 2015. Aktuelle Daten finden Sie unter: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1.1.1 Downadup

Beunruhigend bei den Downadup-Infektionen (auch bekannt als Conficker) ist, dass dieser Wurm bereits über 8 Jahre existiert und offensichtlich immer noch weit verbreitet ist. Downadup verbreitet sich über eine im Jahr 2008 gefundene Sicherheitslücke in Windows Betriebssystemen, welche sich über das Internet ausnutzen lässt und mit dem beliebiger Schadcode auf einem fremden Rechner installiert werden kann. Die immer noch hohe Anzahl an Infektionen lässt sich möglicherweise damit begründen, dass viele Internet-Benutzer in der Schweiz noch eine ältere Version von Windows (Windows XP) verwenden und ihr Betriebssystem nicht regelmässig patchen. Eine weitere mögliche Erklärung wäre, dass es immer noch einige Internet Service Provider (ISPs) in der Schweiz gibt, welche die Meldungen betreffend infizierten Kunden nicht bearbeiten (z. B. aufgrund mangelnder Ressourcen, fehlenden technischen Mitteln oder fehlendem Know-How).

4.6.1.2 Dyre

Im ersten halben Jahr 2015 hat sich vor allem die Schadsoftware Dyre (auch bekannt unter dem Namen Dyreza) in der Schweiz verbreitet. Dabei handelt es sich um einen E-Banking-Trojaner, welcher sich via E-Mail verbreitet. Dazu präparieren die Internet-Kriminellen E-Mails, welche sich üblicherweise als Fax-Nachricht, Rechnung oder ähnliches ausgeben und Schadsoftware im Anhang mitführen (üblicherweise eine Ausführbare Datei - .exe – in einem ZIP-Archiv). Während Dyre in den ersten Monaten vor allem Schweizer KMU im Visier hatte[22] und im Falle eines Freiburger Unternehmens auch ein Siebenstelliger Betrag gestohlen wurde, werden seit Mai 2015 auch vermehrt Privatanwender von Dyre angegriffen[23]. In Spitzenzeiten wurden MELANI täglich bis zu 2‘000 Dyre-Infektionen gemeldet.

Sollten Sie bereits solche E-Mails erhalten und den Dateianhang geöffnet haben, empfehlen wir Ihnen, Ihr System mit einem Virenscanner oder einem Malware Removal-Tool zu überprüfen. Eine entsprechende Anleitung dazu finden Sie unter:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/anleitung-zur-entfernung-von-schadsoftware.html

MELANI hat ein Merkblatt erstellt, welches Schweizer KMU dabei helfen soll, die IKT-Sicherheit im Unternehmensnetzwerk zu erhöhen. Das Merkblatt finden Sie unter:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

Zudem finden Sie ein 10-Punkte Programm zur Erhöhung der IKT-Sicherheit auf dem KMU-Portal des Bundes:

http://www.kmu.admin.ch/kmu-betreiben/03710/03712/03715/index.html?lang=de

---

22 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking-trojaner-hat-schweizer-kmus-im-visier.html (Stand: 31. August 2015).

23 https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/information_dyre_2.html (Stand: 31. August 2015).

4.6.1.3 Retefe

Die Schadsoftware Retefe ist weiterhin aktiv in der Schweiz. MELANI hat das erste Mal vor zwei Jahren über Retefe berichtet. Diese verbreitet sich ausschliesslich via E-Mail, üblicherweise über gefälschte Rechnungen von bekannten Online-Shops, wie z. B. von Zalando oder Ricardo.

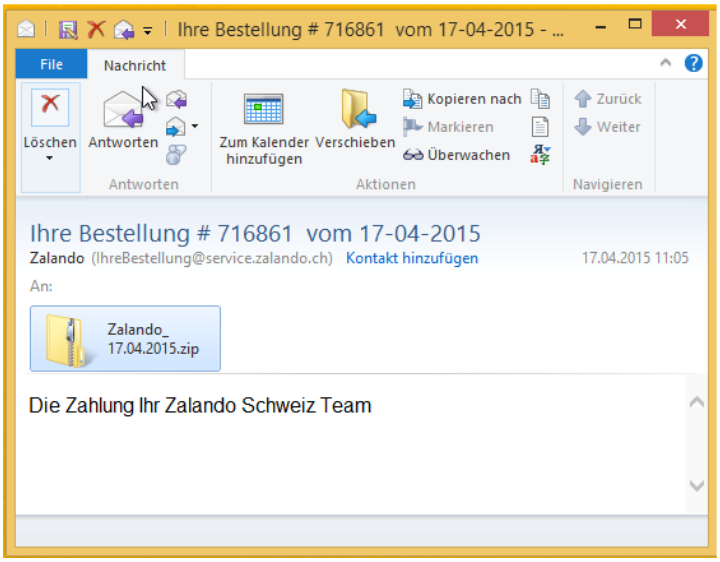


Abbildung 6: Beispiel eines gefälschten E-Mails, welches die Schadsoftware Retefe verbreitet

Führt der Empfänger des E-Mails die im Anhang enthaltene ausführbare Datei aus, so infiziert dieser seinen Windows-Computer mit Retefe. Nach erfolgreicher Infektion ändert Retefe die Einstellungen des Internet Explorers so, dass bestimmte Websites (namentlich die E-Banking-Portale einiger Schweizer Finanzinstitute) über einen Proxy-Server im Ausland umgeleitet werden. Zusätzlich installiert Retefe ein bösartiges *CA-Zertifikat* im Windows-Zertifikat-Speicher. Somit ist es Retefe möglich, Zertifikate für beliebige Finanzinstitute auszustellen und sich somit als solches auszugeben.

Meldet sich ein Opfer via einen mit Retefe infizierten Computer im vermeintlichen E-Banking-Portal an, wird diesem ein *QR-Code* angezeigt. Dieser QR-Code führt zu einer Website, auf welcher das Opfer aufgefordert wird, eine App «zur Erhöhung der Sicherheit» – in Wahrheit jedoch eine Android Schadsoftware, einen sogenannten SMS-Trojaner – herunterzuladen und zu installieren. Installiert das Opfer die angepriesene Android App, werden sämtliche von der Bank gesendeten SMS zur 2-Faktor Authentifizierung an einen Webserver im Ausland und damit an die Hacker weitergeleitet. Somit sind diese nun in der Lage, sich im E-Banking des Opfers einzuloggen und auch Zahlungen zu tätigen.

Falls Sie ein Android Smartphone oder Tablet verwenden, stellen Sie sicher, dass Sie nur Apps aus dem offiziellen Google Play Store installieren. Installieren Sie niemals Apps aus Dritt-Quellen, selbst wenn Sie dazu aufgefordert werden. Stellen Sie ebenfalls sicher, dass auf Ihrem Android Gerät folgende Einstellungen gesetzt sind:

Einstellungen -> Sicherheit -> Unbekannte Herkunft -> DEAKTIVIERT

Google Einstellungen -> Sicherheit -> Gerät nach Sicherheitsbedrohungen.. -> AKTIVIERT

Weitere Informationen zu Retefe finden Sie im GovCERT.ch Blog (Englisch):

http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

4.6.1.4 Tinba

Auch Tinba (auch bekannt als «Tiny Banker») hat im ersten halben Jahr 2015 Schweizer Internet-Benutzer beschäftigt und war zeitweise – neben Downadup – die an MELANI meist gemeldete Infektion in der Schweiz. Bei Tinba handelt sich um einen weiteren E-Banking Trojaner, welcher auch einige Schweizer Finanzinstitute im Visier hat. Anders als bei Dyre oder Retefe ist Tinba jedoch ein «Toolkit», welches in einschlägigen Foren im Internet für ein paar Tausend Franken erworben werden kann. Internet-Kriminelle kaufen die Software ein und können diese dann beliebig verwenden. Neben den in der Schweiz bekannten Tinba-Kampagnen, gibt es noch mehrere Dutzend andere Tinba-Kampagnen weltweit, welche Finanzinstitute rund um den Globus im Visier haben.

4.6.1.5 Verschlüsselungstrojaner – Cryptowall 3.0, Teslascript und ein Autor mit Gewissensbissen

Im ersten Halbjahr 2015 wurden wieder etliche Fälle gemeldet, bei welchen Daten durch einen Cryptotrojaner verschlüsselt wurden. Dabei handelte es sich meist um Cryptowall 3.0, aber auch Fälle mit der Ransomware Teslacrypt wurden MELANI vermehrt gemeldet. Betroffen sind meist Privatpersonen, aber auch Fälle von Firmen sind bekannt. Wer dann kein oder kein aktuelles Backup zur Hand hat, verliert alle oder zumindest einen Teil der Daten. Bemerkenswert war der Fall rund um die Ransomware Locker. Die Schadsoftware hatte sich zuvor auf diverse Computer verteilt und wartete drauf zuzuschlagen und Daten zu verschlüsseln, was dann anfangs Juni 2015 auch passierte. Kurz darauf meldete sich aber der Autor und entschuldigte sich nicht nur, sondern gab der Schadsoftware den Befehl zur Entschlüsselung und veröffentliche zeitgleich auch die Schlüssel.[24]

Auf dem Computer abgelegte Daten sollten regelmässig auf externe Speichermedien kopiert werden (*Backup*). Diese sollten nur während des Backupvorgangs am Computer angeschlossen sein.

[24] http://www.heise.de/security/meldung/Krypto-Trojaner-ueberlegt-es-sich-anders-und-entschluesselt-alles-wieder-2678669.html (Stand: 31. August 2015).

4.7 Präventive Massnahmen

Um gegen die diversen Bedrohungen Abhilfe zu schaffen, sind präventive Massnahmen essentiell. Diese Massnahmen können technischer, organisatorischer und auch strafrechtlicher Art sein. Die Sensibilisierung der Bevölkerung ist ebenfalls ein wichtiger Pfeiler im Kampf gegen Cyber-Angriffe. So nutzen die meisten Angriffe die Unwissenheit und Hilfsbereitschaft der Opfer aus und versuchen diese zu überrumpeln. Eine weitere wichtige Massnahme gegen Cyber-Vorfälle ist die Etablierung einer Meldekultur, sowohl in einem Betrieb als auch generell in der Bevölkerung. Nur wenn die Mitarbeitenden das Gefühl haben, dass sie bei einer Meldung eines Vorfalls ernst genommen werden, werden sie auch weiterhin Meldungen machen. MELANI hat deshalb das Portal «Antiphishing.ch» ins Leben gerufen, auf dem man E-Mails und Webseiten melden kann, die im Verdacht stehen, Zugangsdaten oder Kreditkartendaten zu stehlen.

4.7.1 Antiphishing.ch

Um die Meldungen bezüglich Phishing besser zu kanalisieren und effizienter zu analysieren, hat MELANI im Sommer 2015 das Portal antiphishing.ch lanciert. Die Meldung von Phishing-Webseiten kann über das Webformular erfolgen. Zusätzlich ist auf dem Meldeportal eine E-Mail-Adresse angegeben, an welche Phishing E-Mails weitergeleitet werden können. Das Meldeportal ist unter https://www.antiphishing.ch erreichbar.

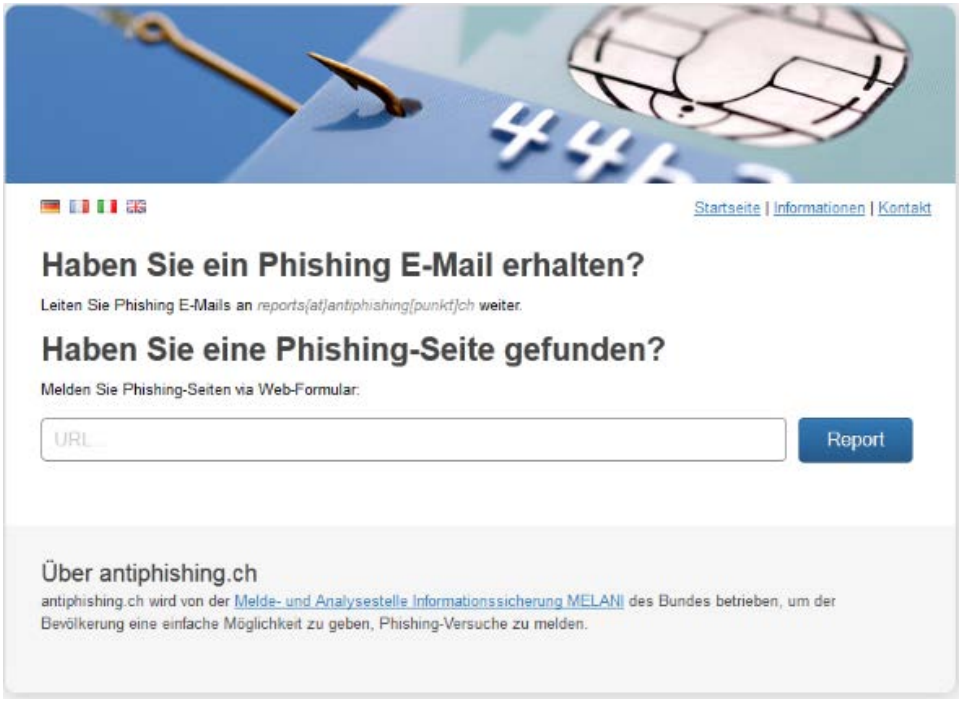


Abbildung 7: Bildschirmansicht der neuen Seite antiphishing.ch auf der Bürger Phishing-Seiten melden können

Die eingehenden Phishing-Meldungen werden einer automatischen Vorprüfung unterzogen. Basierend auf den Resultaten dieser Vorprüfung werden die Phishing-Meldungen sorgfältig manuell überprüft, bevor diese dann Herstellern von IKT-Sicherheitssoftware, Web-Browsern, Hosting Providern usw. sowie auf Wunsch auch den betroffenen Finanzinstituten und Internet-Dienstleistern gemeldet werden, um eine maximale Schutzwirkung zu erzielen.

5 Lage International

5.1 Spionage

5.1.1 Hacker-Angriff auf den deutschen Bundestag

Am 15. Mai 2015 wurde öffentlich bekannt, dass das Netzwerk des deutschen Bundestages «Parlakom» gezielt angegriffen worden war, und dass die Angreifer Daten in der Grössenordnung von 16 Gigabyte kopiert hatten.[25] Die Angreifer sollen dabei nach Systempasswörtern, Word-Dokumenten und lokal abgespeicherten E-Mails gesucht haben. Die Startinfektion soll laut Zeitung «die Welt», wie so oft, mit gezielten E-Mails mit präpariertem Link verübt worden sein.[26,27] Aufgefallen sei laut einem an die Öffentlichkeit gelangten Protokoll der Kommission des Ältestenrates für den Einsatz neuer Informations- und Kommunikationstechniken und -medien (IuK) des Bundestags[28] am 8. Mai 2015 eine «nicht übliche Kommunikation» zwischen Serversystemen. Bei einem Server der Bundestagsverwaltung sei eine ungewöhnlichen Menge an Daten festgestellt worden. Zu diesem Server hätten zudem nicht vorgesehene Verbindungen von einem Abgeordnetenbüro bestanden. Vier Tage später sei in einer weiteren Analyse festgestellt worden, dass zwei Rechner Kontakt zu potenziell gefährlichen Servern, so genannten *Command and Control Servern*, gehabt hätten. Dabei soll es sich um die gleichen Systeme gehandelt haben, welche schon ein paar Tage zuvor auffällig waren. Anscheinend waren zwar nur wenige Endgeräte betroffen, allerdings seien die Angreifer tief in das System eingedrungen, hätten sich dort frei bewegen können und könnten jederzeit wieder aktiv werden.

Im weiteren Verlauf soll es denn auch schwierig gewesen sein, die Angreifer aus dem Netz zu entfernen. Als Massnahme wurde der Neuaufbau von Teilen des Netzes ins Auge gefasst. Deshalb wurde das interne Netzwerk des Bundestags am 20. August 2015 für vier Tage abgeschaltet, um die Folgen des Cyber-Einbruchs zu beseitigen. Diese einschneidende Massnahme zeigt die Tragweite des Vorfalles, ist aber natürlich auch keine Garantie gegen zukünftige Infektionen.

Der Generalbundesanwalt prüft, ob in der vorliegenden Angelegenheit ein Anfangsverdacht für eine in die Zuständigkeit der Bundesanwaltschaft fallende Straftat gegeben ist. Das für den Angriff verwendete Spionageprogramm soll identifiziert worden sein. Es wurde spekuliert, dass es sich dabei um den Schadsoftwarekomplex «Sofacy/APT28» gehandelt hatte.[29] Die Programmstruktur soll einer Schadsoftware ähneln, welche bereits 2014 bei einem Cyberangriff auf ein deutsches Datennetz beobachtet wurde.

---

[25] http://www.spiegel.de/politik/deutschland/cyberangriff-auf-bundestag-abgeordneten-e-mails-erbeutet-a-1039388.html (Stand: 31. August 2015).

[26] http://www.welt.de/politik/deutschland/article142372328/Verfassungsschutz-verfolgt-Spur-nach-Russland.html (Stand: 31. August 2015).

[27] https://www.tagesschau.de/inland/bundestag-cyberattacke-105.html (Stand: 31. August 2015).

[28] http://www.bild.de/politik/inland/bundestag/spielte-cyber-angriff-laut-geheimprotokoll-herunter-41314062.bild.html (Stand: 31. August 2015).

[29] http://www.focus.de/politik/deutschland/bundestag-cyber-angriff-auf-bundestag-dauert-schon-laenger-als-bekannt_id_4761526.html (Stand: 31. August 2015).

5.1.2 Carbanak – der elektronische Banküberfall

Bislang beschränkten sich elektronische Banküberfälle auf den Endkunden. Mittels E-Banking-*Malware* wurde dabei der Computer des Kunden infiziert und die E-Banking Session übernommen. Eine neue Qualität elektronischer Banküberfälle wurde nun im Februar 2015 publik. Unter dem Namen «Carbanak» wurden während zwei Jahren im grossen Stil Banksysteme manipuliert. Der Aufwand, der für diesen Angriff betrieben wurde, ähnelt den gezielten Spionageangriffen, wie man sie von Staaten her kennt. Dabei wurde zuerst versucht, Computer von Bankangestellten zu infizieren. Dazu kam die klassische Methode mittels schädlichem Anhang in einem gezielten E-Mail zum Tragen. Danach suchten die Angreifer Arbeitsplatzrechner von Mitarbeitenden, mit welchen Überweisungen verwaltet werden, sowie ans Netzwerk angeschlossene Geldautomaten. Zwei bis vier Monate verweilten die Bankräuber dabei im Netz, um herauszufinden, wie bankinterne Abläufe für die eigenen Zwecke missbraucht werden könnten.[30] Nachdem diese Informationen zusammengetragen worden waren, imitierten die Angreifer die Bankangestellten und überwiesen sich Geld oder manipulierten Geldautomaten so, dass sie zu einem bestimmten Zeitpunkt Geld ausgaben. Ein Komplize wartete dann an dem entsprechenden Automaten und nahm das Geld entgegen. Damit die Überweisungen nicht auffielen, wurden die Kontostände der auszuraubenden Konti zuerst erhöht, um dann genau um diesen Betrag wieder erleichtert zu werden. Der Gesamtbetrag beim Opfer blieb also gleich und der Betrug wurde somit durch das Opfer nicht so schnell erkannt.

Laut Kaspersky sollen die Angreifer mindestens 100 Banken in 30 Ländern infiltriert haben. Die meisten davon in Russland. Das erbeutete Geld rechtfertigt dabei den Aufwand von bis zu zwei Jahren: Pro Bank wurden bis zu 10 Millionen Dollar erbeutet.

5.1.3 SIM-Karten angeblich im Visier von NSA und GCHQ

In diesem Halbjahr gab es wieder neue Enthüllungen, die auf Dokumenten von Snowden basieren. Im Fokus standen dabei *SIM-Karten*, also jene Karten, die in ein Mobiltelefon eingesteckt werden und zur Identifikation des Nutzers im Netz dienen. Eine gemeinsamen Einheit des britischen Government Communications Headquarters (GCHQ) und der NSA mit dem Namen «Mobile Handset Exploitation Team (MHET)» soll laut der Nachrichten-Website «The Intercept» die internen Netzwerke der grossen SIM-Karten-Hersteller, der grossen Endgerätehersteller und vieler Netzbetreiber kompromittiert haben. In den Fokus geriet vor allem der SIM-Karten-Hersteller «Gemalto». Dieser hat dann auch bekanntgegeben, ausgeklügelte Angriffe in seinem Netzwerk in den Jahren 2010 und 2011 beobachtet, respektive erkannt zu haben, welche auf Aktivitäten von NSA und GCHQ hindeuten könnten. Im Juli 2010 soll es auch gezielte E-Mails gegen Mitarbeitende gegeben haben[31]. Im Fokus stand vor allem der Austausch von Schlüsseln zwischen Mobile-Operatoren und deren Zulieferern. In den meisten Fällen war dieser Austausch bereits 2010 verschlüsselt. Alle Angriffe sollen aber nur auf die Büroautomation und nicht die produktiven Netzwerke gegangen sein. Ob diese Angriffe tatsächlich auf die NSA zurückzuführen sind, ist unklar. Ein massiver Diebstahl von Verschlüsselungscodes von SIM-Karten wurde von Gemalto

---

30 http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide (Stand: 31. August 2015).

31 http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx (Stand: 31. August 2015).

ausgeschlossen. Für einen Verschlüsselungsspezialisten wäre genau dies das schlimmste Szenario.

5.1.4 Spionage im Profisport

Dass Cyberspionage auch die Profisportwelt erfasst, ist nicht weiter verwunderlich, geht es doch hier um grosse finanzielle Summen. Dies gilt gerade auch für die US-Baseball League. Seit Jahren stehen sich hier die «Saint Louis Cardinals» und die «Houston Astros» auf dem Feld gegenüber. Mitarbeitende der Cardinals haben nun aber anscheinend beschlossen, das Spiel nicht mehr nur auf dem Baseball-Feld, sondern auch im Cyberspace auszutragen. Sie sammelten nicht mehr nur Punkte, sondern Informationen wie Trainingsstatistiken der Spieler, Spielstatistiken, Vertragsbestimmungen und Informationen über mögliche zukünftige Spielerkäufe, Strategien usw., die natürlich genauso wertvoll sein können.

Hintergrund ist anscheinend ein Wechsel des General Manager Luhnow von den Cardinals zu den Astros im Jahr 2011. Luhnow hat den Ruf, den Fokus auf statistische Analysen zu setzen. Noch bei den Cardinals rekrutierte er junge Talente, die er mithilfe einer Datenbank und einer Art elektronischem Screening der Spieler fand und so zum Erfolg der Mannschaft beitrug. Nach seiner Anstellung bei den Astros schlug er dort die gleichen Methoden vor, und setzte sich damit durch. Die Cardinals äusserten sich in der Öffentlichkeit dahingehend, dass sie befürchtet hätten, dass Luhnow den Gegnern Informationen über sie zur Verfügung gestellt hätte.

In einer zunehmend vernetzten und digitalisierten Welt steht auch der Sport unter Modernisierungsdruck. Immer mehr halten Analysen und Statistiken Einzug und damit verbunden auch die Verwendung von grossen Datenmengen, die interessante Spionageziele bilden. Gerade im Baseball sind Leistungsanalysen weit verbreitet, da die personenbezogene und geringe Anzahl an Variablen es einfacher machen, Voraussagen zu treffen und Messungen anzustellen. Im Fussball und Eishockey, sind solche Methoden weniger verbreitet, da sich nicht direkt Individuen, sondern zwei Mannschaften gegenüberstehen und es mehr Variablen gibt. Trotz alledem hat auch der Fussballclub «Manchester City» 2012 einen Wettbewerb lanciert, um junge Analysten zu ermutigen, Methoden für diesen Bereich zu entwickeln.

5.2 Datenabflüsse

5.2.1 Über 21 Millionen Datensätze beim US-Personalamt entwendet

Im April 2015 hat das «Office of Personnel Management OPM» (entspricht in der Schweiz in etwa dem Eidgenössischen Personalamt) entdeckt, dass persönliche Daten von 4.2 Millionen aktuellen und ehemaligen Bundesangestellten kopiert worden sind. Betroffen waren Informationen wie Name, Geburtstag, Adressen und Sozialversicherungsnummern. Während dieser Vorfall untersucht wurde, entdeckte das OPM einen weiteren, noch massiveren Datendiebstahl, welcher auch Hintergrundinformationen von aktuellen, ehemaligen und zukünftigen Bundesangestellten und Vertragspartnern betraf. Dieser neuerliche Vorfall umfasst höchstwahrscheinlich 21.5 Millionen individuelle Datensätze und

Informationen, die im Rahmen von Sicherheitsüberprüfungen erhoben worden sind.[32] Dabei sollen 19.7 Millionen Datensätze von Personen stammen, die sich um einen Job beworben haben und um 1.8 Millionen Datensätze von Personen, welche mit Jobbewerbern in Verbindung stehen, wie beispielsweise Ehepartner oder Mitbewohner. Teile der gestohlenen Datensätze beinhalten unter anderem Erkenntnisse von Interviews, welche von den Ermittlern zusammentragen worden sind, Informationen zu geistiger Gesundheit und finanzieller Geschichte. Auch 1.1 Millionen Fingerabdrücke wurden kopiert. Im Jahr 2014 hatte das interne Aufsichtsbüro des OPM empfohlen, elf seiner 47 IKT-Systeme stillzulegen, da sie keine gültige Sicherheitsbescheinigung besassen. Das OPM folgte der Empfehlung nicht. Ob allenfalls eines dieser IKT-Systeme vom Hack betroffen gewesen ist, bleibt unklar. Dieser bislang grösste Angriff auf ein Computernetzwerk der amerikanischen Regierung kostete die Chefin des OPM ihren Job.

US-Ermittler gehen davon aus, dass eine chinesische Gruppe hinter den Angriffen auf die Bundesverwaltung steckt. China hat erwartungsgemäss und umgehend eine Beteiligung an diesen Angriffen dementiert.

Gerade Personalämter sind für Datensammler sehr interessant. Insbesondere dann, wenn an einer Stelle alle Daten der Angestellten einer Verwaltung oder eines Konzerns zusammengefasst und an einem Ort verwaltet werden. Da hier eine Vielzahl von Dokumenten aus unterschiedlichen Quellen verarbeitet werden muss, bietet dies auch ein zusätzliches Gefahrenpotenzial ausgehend von Schadsoftware, die aus den verschiedenen Quellen eingeschleust werden kann.

5.2.2 AdultfriendFinder, British Airways und Krankenversicherung - Datenabflüsse in verschiedensten Branchen

Ein grosser Teil der Partnerschaftssuche hat sich mittlerweile ins Web verlagert. Die Errungenschaften des Internets und die Möglichkeiten von Social Media machen auch vor diesem Bereich nicht Halt und vereinfachen die Suche nach der geeigneten Bekanntschaft. Wird das genutzte Portal allerdings Opfer von Cyber-Kriminellen und die Benutzerdaten inklusive sexuelle Präferenzen landen öffentlich im Netz, ist es mit der geschätzten Anonymität dahin. Ein solcher Fauxpas unterlief der Partnerbörse «Adultfriendfinder»[33] im Mai dieses Jahres. Knapp 4 Millionen Nutzerdatensätze, mit denen sich mit geringem Aufwand die Personen hinter den Alias-Namen eruieren liessen, landeten auf einem einschlägigen Forum, einsehbar für jedermann. Dieser Vorfall wurde im vergangenen Juli vom Angriff auf das Seitensprungportal «Ashley Madison»[34] noch getoppt. Logins von 32 Millionen Benutzern wurden publiziert.

---

[32] https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/ (Stand: 31. August 2015).

[33] http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web (Stand: 31. August 2015).

[34] http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/ (Stand: 31. August 2015).

Im ersten Halbjahr wurden auch Datenabflüsse weit kritischerer Daten bekannt. Bei British Airways sind Kundendaten des Frequent-Flyer Programms entwendet worden[35]. Dies lässt zum Beispiel Bewegungsprofile der betroffenen Personen zu.

Noch heikler wird es, wenn detaillierte Steuerdaten in falsche Hände geraten, so geschehen im Mai bei der amerikanischen Steuerbehörde IRS[36]. Durch Social Engineering-Recherchen gelang es den Angreifern, einen Authentisierungsprozess des IRS auszuhebeln und so im Namen der Steuerzahler deren Daten abzuziehen.

Ebenfalls zu den sensibelsten Daten gehören Patientendaten. Niemand wünscht sich, dass seine Daten über Arztbesuche und Krankheiten an die Öffentlichkeit gelangen. Leider sind auch solche besonders schützenswerten Personendaten nicht in jedem Fall vor fremden Blicken gefeit. Im Februar beichtete die zweitgrösste amerikanische Krankenversicherung Anthem[37] einen Einbruch in ihre 80 Millionen Kunden umfassende Datenbank. Im März wurde ein weiterer Krankenversicherer mit Namen «Premera Health Care»[38] Opfer eines solchen Datendiebstahls.

Für Betreiber heisst dies, dass motivierte Angreifer vor niemandem Halt machen. Es wird deshalb dringend empfohlen, alle möglichen Vorkehrungen zu treffen, um nicht selbst Opfer eines Datendiebstahls zu werden. Eine gute Übersicht gibt hierzu unser Merkblatt IKT-Sicherheit für KMU:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

5.3 Industrielle Kontrollsysteme

Nachdem in den letzten Jahren die *Industriellen Kontroll- und SCADA-Systeme* als Forschungs- und Testfeld von IKT-Sicherheitsexperten entdeckt worden sind, widmen sich diese nun vermehrt auch den Komponenten, die in Autos, Zügen, Schiffen und Flugzeugen verbaut werden – denn die Vernetzung von allerlei Geräten und der Trend zum konstantem Internetanschluss macht auch vor Transportmitteln nicht Halt. Fluggesellschaften, Bahnbetreiber und Reedereien möchten ihren Passagieren an Bord Zugang zum Internet bieten und auch Autos sind immer häufiger netzwerkfähig.

Zu unterscheiden sind hierbei zwei Aspekte: Der Zugang zum Informations- und Unterhaltungsangebot im Internet auf der einen Seite sowie die Verwendung von Elektronik und Informationstechnologie zur operativen Steuerung des Transportmittels respektive zur Unterstützung dessen Führerin oder Führers auf der anderen Seite.

Während bei Ersterem der Zugang zum World Wide Web inhärent ist, kann man beim Zweiten wiederum unterscheiden zwischen Anwendungen, die Informationen von aussen

---

35 http://www.theregister.co.uk/2015/03/29/british_airways_frequent_flyers_hacked/ (Stand: 31. August 2015).

36 http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application (Stand: 31. August 2015).

37 http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720 (Stand: 31. August 2015).

38 http://www.huffingtonpost.com/2015/03/17/premera-blue-cross-cybera_n_6890194.html (Stand: 31. August 2015).

beziehen müssen (zum Beispiel *GPS-Daten*, Wetter- und Staumeldungen) und den rein internen Systemen: Beim Auto zum Beispiel Tankanzeige, Reifendruckmesser oder Heckkamera – aber auch Assistenzsysteme, die im Zusammenspiel von Sensoren und Aktuatoren den Abstand zum vorderen Fahrzeug konstant halten, im Stop-and-go-Verkehr selbständig bremsen und beschleunigen sowie automatisch einparken.

5.3.1 Sicherheit in der Automobilbranche

Autos können nicht erst elektronisch kontaktiert werden, seit sie via Mobilfunknetz ans Internet angeschlossen werden. Bereits die Einführung von elektronischen Türschlössern wussten böswillige Akteure für sich zu nutzen: Sei dies durch Kopieren des vom Schlüssel gesendeten Signals, um die Tür selber öffnen zu können (diese Gefahr wurde inzwischen von den meisten Herstellern erkannt und behoben) oder durch die Störung dieses Signals, damit die Tür den Befehl zum Verschliessen gar nicht erst empfängt.

Inzwischen werden Autos mehr und mehr zu fahrenden Computern: So wird in der Werkstatt mittlerweile häufig zuerst ein Diagnose-Laptop angeschlossen, um vom Auto zu erfahren, wie es ihm geht. Über eine solche Schnittstelle kann umfassend auf die Autoelektronik zugegriffen werden – dies ist so vorgesehen und keine Schwachstelle an sich (it's not a bug, it's a feature). Dennoch können solche Schnittstellen als Angriffsvektor dienen – bedürfen aber typischerweise physischen Zugang zum Auto. Demgegenüber kommunizieren verschiedene Systeme auch drahtlos miteinander: Zum Beispiel übermitteln Reifendrucksensoren ihre Messwerte, und das Mobiltelefon wird per *Bluetooth* mit der Autoelektronik verbunden, damit die eingebaute Freisprechanlage genutzt werden kann. Zudem wird in verschiedenen Fahrzeugen ein Mobilfunkanschluss installiert, um übers Internet Informationen senden und empfangen zu können. Dieser dient nicht nur der Unterhaltung, sondern soll es dem Hersteller allenfalls auch ermöglichen, den Standort des Fahrzeuges abzurufen, die Türen mittels Fernzugriff aufzuschliessen (wenn man den Schlüssel im Fahrzeug liegen gelassen hat) oder auch die Wegfahrsperre zu aktivieren, wenn das Auto als gestohlen gemeldet worden ist. Diese Funktionen bedingen eine Verbindung von der IKT zur Fahrzeugelektronik, welche folglich auch auf diesem Weg angreifbar ist.

Es erscheint selbstverständlich, dass in einem Fahrzeug die Unterhaltungssysteme von der operativen Elektronik sauber getrennt sind und die operative Elektronik soweit abgesichert sein muss, dass diese weder von aussen direkt noch via kompromittierte Unterhaltungsgeräte manipuliert werden kann. Hersteller halten dies jedoch nicht unbedingt ein, wie Forscher in letzter Zeit bei verschiedenen Gelegenheiten und diversen Automarken aufgezeigt haben.

Vielfach sind die verschiedenen Komponenten nicht ausreichend voneinander abgeschirmt. Dies führt dann zu so abenteuerlichen Hacks wie der Manipulation der Assistenzsysteme über Schadsoftware, welche zuvor via CD im Autoradio oder gar über das UKW-*Radio-Daten-System (RDS)* eingeschleust worden ist.[39] Wenn Befehle an Assistenzsysteme ausgegeben werden können – via Schadsoftware oder via direkter Drahtlosverbindung – ist es allenfalls möglich, den Wagen zu beschleunigen, zu bremsen oder zu lenken. Aber auch

[39] http://www.bbc.com/news/technology-33622298 (Stand: 31. August 2015).

über Verfälschung von Sensorwerten können unangemessene Reaktionen der Assistenzsysteme herbeigeführt werden.

Jegliche drahtlose Kommunikation innerhalb des Wagens muss verschlüsselt sein, damit sie nicht einfach ausgelesen und mitgeschnitten werden kann. Weiter sollten sich die verschiedenen Komponenten gegenseitig authentifizieren. Durch diese Massnahmen wird das Einspeisen von mutwilligen Befehlen oder falschen Sensorwerten massiv erschwert. Zudem muss sichergestellt sein, dass Komponenten, welche via Internet kommunizieren sollen, nicht als Einfallstor in die Autoelektronik missbraucht werden können

5.3.2 Reboot bei Boeing 787 Dreamliner

Das Allheilmittel, wenn die Büroanwendung mal wieder nicht so will wie der Mitarbeitende, scheint auch bei Flugzeugen ab und zu angebracht zu sein: Ein Neustart hilft nicht nur beim geschäftlichen oder privaten Computer, sondern in gewissen Fällen sogar beim Dreamliner von Boeing.[40]

Auch im Dreamliner kommt viel Software zum Einsatz. Bei Boeing internen Laborversuchen wurde bei Kontrollen der Steuerungs-Software der für die Stromproduktion zuständigen Generatoren festgestellt, dass sie nach 248 Tagen aufgrund eines Zählerüberlaufs in den «Fail-Safe Modus» wechseln. Für das Flugzeug bedeutet dies Stromausfall. Die simple Lösung lautet somit: Neustart der Steuerungs-Software des Dreamliners.

Als Passagier muss man sich zum Glück keine Sorgen machen, da ein solcher Neustart bei jeder Routinewartung durchgeführt und der Zählerüberlauf damit erfolgreich vermieden wird.

5.3.3 Infotainmentsysteme im Flugzeug

Der amerikanische IKT-Sicherheitsforscher Chris Roberts behauptet, er habe Schwachstellen in den Passagier-Unterhaltungssystemen (IFE) der Flugzeugtypen Boeing 757-200, Boeing 737-800, Boeing 737-900, und Airbus A-320 entdeckt, die es zulassen, auf kritische Systeme der *On-Board-Elektronik* zuzugreifen. Am 13. Februar 2015 unterrichtete er das US Federal Bureau of Investigation (FBI) freiwillig über seine Erkenntnis, in der Hoffnung, dass die Sicherheitslücken behoben werden. Am 15. April wurde er nach einer Anspielung, die Steuerung der Sauerstoffmasken manipulieren zu können, vom FBI festgenommen und die Gerätschaften, welche er auf sich trug, wurden dabei beschlagnahmt.

Aus dem Antrag für einen Durchsuchungsbefehl[41] vom 17. April 2015 betreffend den Fall Roberts ist zu entnehmen, dass Roberts mehrere Utensilien auf sich trug, die das Durchführen von Penetration-Tests in verschiedensten Netzwerkumgebungen erlauben würde. Darüber hinaus wurden bei Roberts Verkabelungsschemas und zusätzliche Fachdokumentation der Flugsteuerungs- und Informationssystemen sichergestellt. Von Avionik-Fachspezialisten wurde bestätigt, dass die von Roberts publizierten Steuerungsbefehle in entsprechenden Protokollen tatsächlich existieren. Als nach der

[40] https://s3.amazonaws.com/public-inspection.federalregister.gov/2015-10066.pdf (Stand: 31. August 2015).

[41] http://www.wired.com/wp-content/uploads/2015/05/Chris-Roberts-Application-for-Search-Warrant.pdf (Stand: 31. August 2015).

Festnahme am Flughafen Syracuse die Sitze des Flugzeuges untersucht wurden, auf welchen Roberts gesessen hatte, wurde festgestellt, dass versucht wurde, die Abdeckungen der Seat Electronic Boxes bei den beiden vorderen Sitzen zu entfernen. Roberts behauptete, sich auf diese Weise mit modifizierten Anschlusssteckern an mitgebrachten Ethernet Kabeln Zugang zum IFE-System verschafft zu haben und dass er sich anschliessend mit Penetration-Testing Methoden zu weiteren OnBoard-Systemen Zugang verschaffen konnte.

Im von Roberts beschriebenen Einzelfall darf davon ausgegangen werden, dass er zumindest versucht hat, in die IFE-Systeme und allenfalls weitere Netzwerkteile einzudringen. Bei ungenügenden Sicherheitsvorkehrungen hätte er über das nötige Fachwissen wie die geeigneten Werkzeuge verfügt, eine solche Aktion durchzuführen. Komplett ausschliessen lässt sich der Erfolg dieser Vorgehensweise zwar nicht. Es ist jedoch auch möglich, dass er die Vorfälle zu Selbstmarketing-Zwecken aufzubauschen versuchte.

5.3.4 Stromausfälle – Cyberhintergrund vermutet aber nicht bestätigt

Wie man auf etwas angewiesen ist, merkt man erst dann, wenn es nicht mehr funktioniert. An diesen einfachen Spruch fühlten sich wohl am 27. März 2015 zahlreiche Personen erinnert, die sich zu diesem Zeitpunkt in den Niederlanden aufgehalten haben. Bei einem grossflächigen Stromausfall fielen Ampeln, öffentliche Verkehrsmittel und auch Mobilfunkantennen aus. Supermärkte mussten schliessen, da die elektronischen Kassen wie auch die Diebstahlsicherung nicht mehr funktionierten. Lifte wurden evakuiert und Schulen geschlossen.[42] Beim Flughafen Schiphol wurden Flüge gestrichen. Es konnten auch keine Maschinen mehr landen und mussten auf andere Flughäfen umgeleitet werden. Obwohl vereinzelte Stimmen einen Hackerangriff hinter diesem Ausfall vermuteten, war die Ursache eine Überlastung in einem Umspannwerk in einem Vorort von Amsterdam. In der Vergangenheit hat sich immer wieder gezeigt, dass ein Defekt an einer zentralen Stelle der Stromversorgung eine Kettenreaktion auslösen kann.

Die Spekulationen über einen Hackerangriff wurden beflügelt, als kurz nach dem Ereignis in Amsterdam am 31. März 2015 ein Stromausfall weite Teile der Türkei lahmlegte: In den Städten Istanbul, Ankara und Izmir fiel der Strom aus. Insgesamt sollen 30 der 81 türkischen Provinzen betroffen gewesen sein. Andere Quellen sprachen sogar von 80 betroffenen Provinzen. Erst nach zehn Stunden konnte das zuständige Energieministerium verkünden, dass die Stromversorgung überall wieder hergestellt sei. Gerade in den Grossstädten Istanbul und Ankara haben sich private Betriebe für solche Vorfälle gewappnet und Notstromgeneratoren angeschafft. Deshalb hielten sich dort die Auswirkungen in Grenzen. Grosse Auswirkungen hatte der Stromausfall allerdings im öffentlichen Verkehr wie beispielsweise bei der U-Bahn, die unter dem Marmara-Meer durchführt. Auch in diesem Fall konnten die Spekulationen über einen Hackerangriff nicht bestätigt werden. Grund sollen Ausfälle mehrerer Kraftwerke und die damit zusammenhängenden Spannungsschwankungen gewesen sein.

5.3.5 US-Tankstellen aus dem Internet angreifbar

Eine Fahrt auf der Route 66 und die Tanknadel neigt sich nach unten. Die kleine Tankstelle fernab jeder Ortschaft verspricht zwar Hoffnung, doch die Zapfsäule ist leer. Eine äusserst

[42] http://nos.nl/artikel/2027141-noord-holland-heeft-weer-stroom.html (Stand: 31. August 2015).

unangenehme Vorstellung. Doch ist die Zapfsäule wirklich leer? Dies muss nicht sein, denn bei US-Tankstellen, welche aufgrund ihrer abgelegenen Lage per Fernzugriff verwaltet werden, wurden Sicherheitsprobleme bei den automatisierten Füllstandsanzeigen festgestellt[43]: 3% der ca. 150‘000 aus dem Internet erreichbaren Tankanzeigen waren ohne Schutz erreichbar und vor allem frei konfigurierbar. Durch Änderung der Einstellungen könnte somit einer Tankstelle bei leeren Zapfsäulen vorgegaukelt werden, dass sie noch über ausreichend Reserven verfügt, was zur Folge hätte, dass kein Nachschub bestellt wird. Durch spezifische Befehle könnten die Zapfsäulen auch problemlos ausser Betrieb gesetzt werden.

Für den Fernzugriff, wo dieser absolut erforderlich ist, muss ein angemessenes Sicherheitsverfahren gelten. MELANI hat dazu ein Themenpapier mit verschiedenen Empfehlungen herausgegeben:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

5.4 Angriffe (DDoS, Defacements)

5.4.1 Kein Signal bei TV5 Monde

Aus den vielen Angriffen, die im ersten Halbjahr 2015 verzeichnet wurden, sticht sicherlich derjenige auf den französischen Fernsehsender TV5 Monde am 8. April hervor. Es war das erste Mal, dass nicht nur die Internetpräsenz eines Senders durch einen Angriff betroffen war, sondern auch seine Produktionsanlagen lahmgelegt wurden.

5.4.1.1 Verlauf des Angriffs

Am 8. April 2015 war der Sender TV5 Monde Opfer eines Mehrfachangriffs, der verschiedene Produktionsanlagen und Plattformen traf. Der spektakulärste Aspekt ist die Lahmlegung der Sendeinfrastruktur, die TV5 ab 22 Uhr zum Sendeunterbruch zwang. Erst drei Stunden später konnte wieder gesendet werden, allerdings nur mit vorproduziertem Programminhalt. Parallel dazu wurden die Facebook- und Twitterkonten des Senders gehackt und mit dschihadistischer Propaganda geflutet. Die Webseite wurde ebenfalls verunstaltet. Gemäss den verfügbaren öffentlichen Quellen wurde beim Angriff ebenfalls die E-Mail-Kommunikation im Unternehmen gehackt und lahmgelegt. Kurz nach der Attacke bekannte sich eine Sympathisantengruppe des IS mit dem Namen «Cyber Caliphate» zum Angriff. Wer der Akteur und sein Auftraggeber genau waren, erwies sich jedoch in der Folge als weniger eindeutig, was uns einmal mehr daran erinnert, wie unsicher die Attribution von Angriffen oft ist (siehe hierzu Kapitel 5.4.1.3).

5.4.1.2 Verwundbarkeit der Produktionsanlagen?

Das Hacken von Konten in den sozialen Netzen ist insbesondere im Rahmen von Angriffen zur Verbreitung dschihadistischer Propaganda ein häufig beobachtetes Ereignis. Die

[43] https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges (Stand: 31. August 2015).

Produktionsanlagen oder genauer gesagt die Infrastruktur zur Ausstrahlung der Programme (Encoder und Multiplexer) eines grossen TV-Senders zu kapern, ist hingegen neu. Dies wirft natürlich die Frage nach der Verwundbarkeit dieser Art Infrastruktur auf. Schliesst man einen physischen Zugriff auf die Anlagen beispielsweise durch einen infizierten USB-Stick aus, setzt die Attacke einen Fernzugriff voraus. Öffentlichen Quellen zufolge sollen verschiedene Systeme des Senders vom Internet aus sichtbar gewesen sein, was die Angriffsfläche deutlich erhöht. Eine weitere Frage, die sich bei dieser Art des Angriffs stellt, ist die Trennung zwischen Büroautomation und produktiven Systemen. Zwar sind Details zu diesem Punkt nicht bekannt, einige Experten vermuteten aber diesbezügliche Mängel bei TV5 Monde. Es hat schon einzelne Fälle gegeben, bei denen die Büroautomation gekapert wurde und ohne wirksame Segmentierung, die Infektion anschliessend auch auf die produktiven Systeme hätte überspringen können. Ungeachtet der Massnahmen, die vor dem Angriff auf TV5 vorhanden waren, zeigt das Ereignis aber vor allem eins, nämlich wie wichtig der Schutz der industriellen Kontrollsysteme ist.

Für den Fernzugriff, wo dieser absolut erforderlich ist, muss ein angemessenes Sicherheitsverfahren gelten. MELANI hat dazu ein Themenpapier mit verschiedenen Empfehlungen herausgegeben:

https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsystemen--ics-.html

5.4.1.3 Schwierige Zuordnung

Am Tag nach dem Angriff stellte kein Kommentator die Zuordnung zu einer im Internet aktiven Islamistengruppe in Zweifel. Nur eine Beteiligung des IS war noch Gegenstand der Diskussion. Erst im Juni wurden die Kommentare durch neue Anhaltspunkte in eine andere Richtung gelenkt. Zuerst zeigte sich, dass bereits Anfang Jahr in das Netz von TV5 eingedrungen wurde. Die Täter hätten somit genug Zeit gehabt, sich umzusehen und interessante Systeme auszumachen. Diese Information war ein erster Hinweis auf einen Angreifer mit relativ hohem Professionalisierungsgrad. Von journalistischer Seite wurde dann gestützt auf Analysen der Sicherheitsfirmen Trend Micro und FireEye über eine Spur spekuliert, die zu einer Kampagne namens «Sofacy» (auch bekannt unter «Pawn Storm» oder «APT28») führen soll. Der Grund für die Annahme waren Spuren, die in den Netzen von TV5 Monde gefunden wurden und Sofacy zugeordnet werden konnten. Allerdings ist auch der Nachweis von Sofacy kein Beweis für einen Zusammenhang mit der Lahmlegung des Senders im April 2015. Diesbezüglich wurden verschiedene Hypothesen laut. Eine erste besteht darin, dass die Gruppe rund um Sofacy, bei der eine russische Herkunft vermutet wird, den Angriff tatsächlich durchführte und dabei eine falsche Spur zu Islamisten legen wollte («false flag»). Hier spricht allerdings dagegen, dass der Angriff nicht der normalerweise sehr stillen und heimlichen Vorgehensweise und den im Spionagebereich anzusiedelnden Zielen von Sofacy entspricht. Zudem ist nicht ersichtlich, welches Interesse ein mutmasslich russischer Angreifer an dieser Art Aktion haben sollte, auch wenn Spannungen auf diplomatischer Ebene zwischen Frankreich und Russland zu dieser Zeit bekannt waren[44]. Eine zweite Hypothese besteht darin, dass Sofacy durch dschihadistische

[44] Die Spannungen basieren auf dem Verkauf von zwei französischen Kriegsschiffen an Russland und der anschliessenden Annullation dieses Geschäfts.

Sympathisanten verwendet worden ist. Für diese Interpretation liegt aber kein konkreter Anhaltspunkt vor, und sie bedarf einer Erklärung, wie die fraglichen dschihadistischen Gruppen an die Malware gelangt sein sollen. Die dritte und plausibelste Hypothese geht von zwei parallel stattfindenden Operationen aus, die nichts miteinander zu tun hatten. Zum einen wäre ein russisches Interesse an einem Sender wie TV5 denkbar. Getreu seiner Gewohnheit wäre der Akteur geräuschlos und heimlich in das Netz eingedrungen, um sensible Daten zu beschaffen. Zum andern könnte parallel dazu die Cyberattacke eines anderen Angreifers stattgefunden haben, der es auf die Verbreitung islamistischer Propaganda abgesehen hatte und sichtbare Schäden herbeiführen wollte.

5.4.1.4 Medien als bevorzugtes Ziel

Bereits im Halbjahresbericht 2014/1[45] wies MELANI darauf hin, dass Medien besonders interessante Ziele darstellen und dadurch anfällig für Cyberattacken sind. Der Angriff auf TV5 hat diesen Trend bestätigt, der sich nicht nur auf die Printmedien beschränkt. Medien sind generell für Angreifer interessant, zum einen wegen der Vielzahl der dort bearbeiteten und teils sensiblen Daten und zum anderen wegen der grossen Resonanz, die sie für die Verbreitung von Propaganda oder falschen Informationen bieten. Darüber hinaus lassen sich gewisse für die Medien charakteristische Aspekte schlecht mit den besonders hohen Sicherheitsanforderungen vereinbaren, die eigentlich gelten sollten. Wir denken da beispielsweise an die Notwendigkeit eines raschen Zugriffs auf die Nachrichten von deren Eingang über die Bearbeitung bis zur Veröffentlichung. Eine weitere Schwierigkeit besteht darin, bei einer Vielzahl von Korrespondenten, die teils als Selbstständige arbeiten, sehr mobil sind und sich an verschiedenen Orten der Welt aufhalten, gesicherte Kommunikationsprotokolle bereitzustellen. Schliesslich darf man auch nicht vergessen, dass die Akteure, die es auf solche Ziele abgesehen haben, meist über deutlich mehr Ressourcen für ihre Angriffe als die Medien für deren Abwehr zur Verfügung haben.

Die Medien müssen aufgrund der breiten Palette an Risiken, denen sie ausgesetzt sind (z.B. *DDoS*, Spionage, Sabotage) neben präventiven auch reaktive Sicherheitsverfahren implementieren. Insbesondere müssen Eindringlinge und aussergewöhnliche Vorfälle erkannt und Notfallmassnahmen für die verschiedenen Szenarien vorbereitet werden.

5.4.2 Cyberangriff: Flüge von Polish Airlines gestrichen

Gerade Cyber-Angriffe auf Verkehrsmittel wie Eisenbahnen oder Flugzeuge erwecken Interesse und auch gewisse Ängste. Eine entsprechende Meldung sorgte am 21. Juni 2015 für Schlagzeilen und liess zunächst einen schwerwiegenden Angriff vermuten: Ein Hackerangriff auf das Computersystem der Fluggesellschaft «Polish Airlines (LOT)» habe diese gezwungen, etliche Flüge zu streichen, weil durch das betroffene System keine Flugpläne mehr generiert werden konnten. Flugpläne enthalten beispielsweise Daten zum Start- und Zielflughafen sowie zur Flugroute. Insgesamt 1400 Flugpassagiere sollen davon betroffen gewesen sein. Diese Daten werden unter anderem von den Fluglotsen verwendet, um Flugzeuge auf einer sicheren Flugroute zu halten. Können diese nicht übermittelt oder

[45] MELANI Halbjahresbericht 2014/1, Kapitel 5.2: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-1.html (Stand: 31. August 2015)

ausgedruckt werden, können die Flugzeuge auch nicht starten. Angaben zu den Hintergründen wurden indes keine gemacht.[46]

Der Mediensprecher gab einen Tag später als Grund eine Überlast des Netzwerks an, welche durch einen *DDoS-Angriff* ausgelöst wurde. Ob dieser gezielt oder ungezielt war, wurde nicht kommuniziert. Ebenso unklar sind die Art und die Grösse des Angriffs. Normalerweise sollten kritische Systeme, die mit dem Internet verbunden sein müssen, besonders gegen Angriffe auf ihre Verfügbarkeit geschützt werden. Der CEO von LOT, Sebastian Mikosz, erklärte, dass dies ein generelles Industrieproblem sei und er erwarte, dass dies zu jederzeit und an jedem Ort passieren könne.

Ruben Santamarta, ein Security-Consultant bei IOActive, bemerkte seinerseits, dass dies eine Trendwende bei der Airline-Industrie sein könnte und diese Branche nun auch für Cyber-Kriminelle attraktiv sein könnte. Tatsächlich ist in den letzten Monaten ein erhöhtes Interesse an den Sicherheitssystemen in der Luftfahrt erkennbar. Dies zeigt beispielsweise auch der Fall in Kapitel 5.3.3, bei dem versucht wurde, über das Infotainment-System in den kritischen Bereich der Flugzeugsteuerung zu gelangen.

In letzter Zeit lässt sich ein erhöhter Fokus der IT-Sicherheitsforscher auf Verkehrsmittel und -betriebe beobachten. Aber ist damit aber auch ein Interesse von Cyber-Kriminellen verbunden? Allgemein muss immer unterschieden werden zwischen Systemen, die notwendigerweise mit dem Internet verbunden sind und solchen, die aus Sicherheitsgründen nicht mit dem Internet verbunden sind. Unter erstere Kategorie fallen beispielsweise Buchungssysteme und alle Systeme, die einen Austausch zwischen verschiedenen Stellen beinhalten. Hier funktionieren die klassischen Geschäftsmodelle wie *DDoS*-Erpressung oder das Stehlen von Benutzerdaten mit anschliessender Erpressung genauso, wie bei jeder anderen Branche. Diesbezüglich ist anzunehmen, dass künftig auch diese Systeme (wie bei allen anderen Sektoren auch) ins Visier von Cyber-Kriminellen geraten werden. Im aktuellen Fall von einer Trendwende im Luftfahrtsektor zu sprechen, scheint allerdings übertrieben.

5.4.3 Cyberangriffe im Nachgang von Charlie Hebdo

Der Anschlag auf die Pariser Redaktion von Charlie Hebdo im Januar 2015 hatte auch im Internet Auswirkungen, die allerdings in keiner Art und Weise mit den physischen Angriffen vergleichbar sind. Beeindruckend ist zwar die Anzahl der virtuellen Angriffe, die zwischenzeitlich mit 25‘000 angegeben wurde, nicht aber deren Qualität. In den meisten Fällen handelt es sich um so genannte *Defacements*, bei denen Sicherheitslücken von Webseiten ausgenutzt werden, um darauf politische oder religiöse Parolen zu platzieren: So waren Sätze wie «Tod für Frankreich» oder «Tod für Charlie Hebdo» zu lesen. Die meisten Attacken wurden von Gruppen mit dem Namen wie «Middle East Cyber Army», «Fallaga team» und «Cyber Caliphate» durchgeführt. Die Angriffe waren wenig konzertiert, sondern eher zufällig ausgewählt, was bei dieser Art von Angriffen der üblichen Vorgehensweise entspricht. Es traf beispielsweise Schulen, Universitäten, Kirchen und Unternehmen. Die Opfer werden dabei nicht gezielt ausgewählt. Viel mehr werden verwundbare Systeme gesucht und deren Sicherheitslücken konsequent ausgenutzt. Gerade religiös motivierte

[46] http://www.reuters.com/article/2015/06/22/us-poland-lot-cybercrime-idUSKBN0P21DC20150622 (Stand: 31. August 2015).

Hacker bedienen sich dieser Methode. Währendem sich die Angriffe in Normallage über die ganze Welt verteilen, werden bei einem Vorfall die Kräfte dann gebündelt in Richtung des Erregers des Zorns gelenkt. Auswirkungen dieser Angriffe wurden auch in der Romandie bemerkt (siehe Kapitel 4.4.2).

Ein belgischer Ableger von Anonymous hat sich ebenfalls in diesen Konflikt eingeschaltet und in einer Gegenaktion angekündigt, alle Dschihadistischen Online-Aktivitäten zu verfolgen und entsprechende Konten auf Twitter, YouTube und Facebook zu sperren.

5.4.4 Hacker legen Website der US-Armee lahm

Im Juni 2015 sah sich das US-Militär mit einem Angriff auf seine Webinfrastruktur konfrontiert. Dabei wurde die öffentliche Webseite www.army.mil mit Propaganda versehen und musste deshalb kurzzeitig vom Netz genommen werden. Da auf dieser Seite keine vertraulichen oder personenbezogenen Daten gespeichert waren, konnten auch keine Daten gestohlen werden. Die «Syrian Electronic Army» hatte sich via Twitter zu diesem Angriff bekannt. Die Gruppe war in der Vergangenheit schon mehrmals mit Angriffen vor allem gegen verschiedene Medien aufgefallen[47]. Dabei geht es vordergründig nicht um das Stehlen von Daten, sondern um Desinformation und das Platzieren von politischen Aussagen. Das Pentagon betonte dann auch, dass es sich hier lediglich um Cyber-Vandalismus handelte.

Bereits im Januar sind die Twitter- und Youtube-Konten des US-Zentralkommandos der Streitkräfte (CENTCOM) von angeblichen Anhängern des Islamischen Staates (IS) kurzzeitig gekapert worden. Während des 30-minütigen Spuks wurden auf dem Twitterkonto der Text «Cyber Caliphate» eingeblendet und Propagandabilder verbreitet. Auch hierbei handelte es sich eher um einen einfachen Angriff: Die Angreifer dürften durch gezielte Phishing-E-Mails (sogenanntes *Spear Phishing*) an die Zugangsdaten gekommen sein. Youtube und Twitter bieten mittlerweile Zwei-Faktor-Authentifizierungsmethoden an, die solche Angriffe erschweren. Diese Methoden seien bei den betroffenen Konten aber noch nicht im Einsatz gewesen.

5.4.5 Superfish/Lenovo

Der Computer- und Notebook Hersteller Lenovo lieferte Notebooks standardmässig mit einer vorinstallierten Software namens «Superfish» aus. Dabei handelt es sich nach Einschätzung von IKT-Sicherheitsdienstleistern um eine *Adware*, welche unter anderem beim Aufruf der Google-Suche im Webbrowser Werbe-Einblendungen von Dritt-Anbietern einbindet.

Im Februar 2015 wurde nun bekannt, dass Superfish ein eigenes CA-Zertifikat im Windows-Zertifikats-Speicher installiert. Dies ermöglicht es Superfish, sich als beliebige Website auszugeben (beispielsweise Google) und selbst bei mit HTTPS verschlüsselten

---

[47] MELANI Halbjahresbericht 2013/1, Kapitel 4.4: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-1.html (Stand: 31. August 2015).
MELANI Halbjahresbericht 2013/2, Kapitel 4.8: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2013-2.html (Stand: 31. August 2015).

Verbindungen entsprechende Werbe-Einblendungen einzubinden. Da der geheime Schlüssel des durch Superfish installierten CA-Zertifikates in der Software einprogrammiert ist, kann dieser durch die Anwendung entsprechender Techniken aus Superfish extrahiert werden. Dies ermöglicht es Hackern, Zertifikate für beliebige Webseiten auszustellen, welche dann von Lenovo-Geräten als vertrauenswürdig eingestuft werden.

Superfish macht somit Geräte, auf welchen die Software vorinstalliert ist, beispielsweise für Man-In-The-Middle-Attacken angreifbar. Dadurch wäre es Hackern theoretisch möglich, sich als Bank auszugeben und somit Anmeldeinformationen (Benutzername, Passwort, Token) des Opfers zu stehlen, um E-Banking-Betrug zu begehen.

Das Offizielle Statement von Lenovo zur Superfish Problematik findet sich auf der Lenovo Webseite[48].

MELANI empfiehlt Anwendern von Lenovo Geräten zu überprüfen, ob Superfish auf dem Gerät installiert ist und die Software ggf. zu deinstallieren. Auf folgender Webseite kann überprüft werden, ob das eigene Gerät von der Superfish Problematik betroffen ist.

Superfish, Komodia, PrivDog vulnerability test (Englisch)

https://filippo.io/Badfish/

Zudem hat Lenovo ein Tool bereitgestellt, mit welchem Superfish entfernt werden kann (Deinstallation):

https://support.lenovo.com/us/en/product_security/superfish_uninstall

Für Computer mit sensiblem Verwendungszweck, empfiehlt MELANI, Computer und Notebooks vor Inbetriebnahme zu formatieren und eine frische Installation des Betriebssystems vorzunehmen. Dadurch kann verhindert werden, dass unnötige und möglicherweise unerwünschte vorinstallierte Software (beispielsweise Adware) den Betrieb des Gerätes stören oder sensible Daten ohne Wissen des Benutzers an Dritte weiterleiten.

5.4.6 Exploit Kits

Ein *Exploit Kit* ist ein Werkzeug für Angreifer, um auf den Endgeräten Lücken auszunützen, sei dies direkt im Browser oder in Hilfsprogrammen wie Flash, Acrobat Reader oder Java. Das Exploit Kit ermöglicht dabei eine hohe Arbeitsteilung in den kriminellen Gruppierungen, da es in der Regel so gestaltet ist, dass es praktisch ohne IKT-Kenntnisse bedient werden kann. In der Regel handelt es sich um eine webbasierte Oberfläche, welche die nötigen Funktionalitäten bereitstellt, wie z .B. die Auswahl der Exploits, Statistiken über infizierte Geräte und weitere Konfigurationsmöglichkeiten.

In der Regel ist die Vorgehensweise der verschiedenen Tätergruppen fast identisch:

[48] http://forums.lenovo.com/t5/Lenovo-P-Y-and-Z-series/Removal-Instructions-for-VisualDiscovery-Superfish-application/ta-p/2029206 (Stand: 31. August 2015).

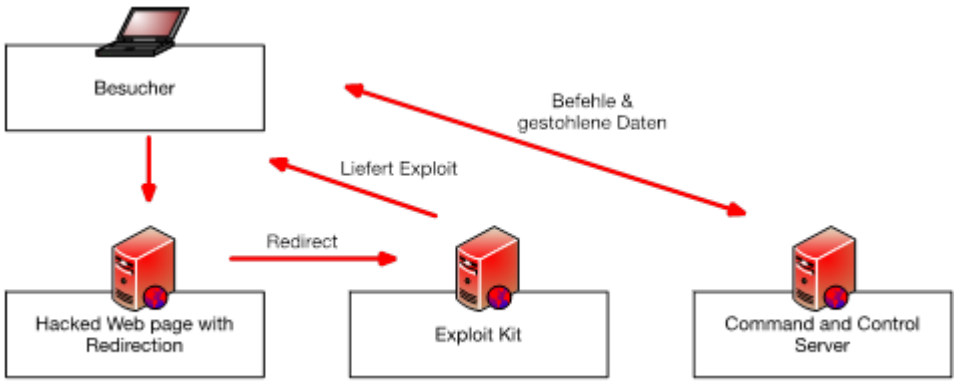


Abbildung 8:Schematische Darstellung der Funktionsweise eines Exploit-Kits

Der Angreifer leitet möglichst viele potenzielle Opfer zu seinem Exploit Kit um. Dies kann er auf verschiedene Arten machen:

- Er übernimmt Websites, die ein verwundbares CMS verwenden und platziert dort eine versteckte Weiterleitung auf den Server mit dem Exploit Kit. Aus diesem Grund ist es essentiell, dass alle Betreiber einer Website ihr CMS schützen und immer auf aktuellem Stand halten.[49,50]
- Er platziert Werbung, welche die Besucher dorthin leitet. Dies kann durch den Einkauf entsprechender Banner sein oder die Übernahme von verwundbaren Werbeservern.
- Er kauft sich bei einem anderen Dienstleister entsprechenden Traffic ein. Ein solches System wird *Traffic Distribution System (TDS)* genannt. Dabei sind nicht alle Betreiber dieser Systeme kriminell: Besucherströme werden oft auch in legalem Kontext gesteuert.

Das Exploit Kit selbst prüft das Zielgerät oft mit *JavaScript* auf die installierten Plug-Ins und ihre Versionen, um eine möglichst passende Lücke zu finden und mit einem Exploit anzugreifen. Es gibt eine Vielzahl an Exploit Kits, welche über unterschiedliche Fähigkeiten verfügen. Die bekanntesten Exploit Kits sind dabei Angler, Neutrino, Rig, Nuclear und Magnitude. Es ist interessant zu beobachten, wie rasch die entsprechenden Exploit Kits beim Erscheinen von neuen Lücken über passende Exploits verfügen. Dabei verfügen nicht alle Exploit Kits über dieselben Exploits, es gibt eine relativ grosse Variation.[51] Darüber hinaus kommt es immer öfter vor, dass die Exploit Kits selbst über *0-day Exploits* verfügen.[52]

Exploit Kits werden jedoch nicht nur von «gewöhnlichen» kriminellen Angreifern verwendet, sondern teilweise auch von staatlichen Angreifern im Zusammenhang mit Spionage Aktivitäten eingesetzt.

---

[49] Siehe auch die MELANI Checkliste: Massnahmen zum Schutz von Content Management Systemen (CMS): https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

[50] Siehe auch Kapitel 3 des aktuellen Halbjahresberichts.

[51] http://contagiodump.blogspot.ch/2010/06/overview-of-exploit-packs-update.html (Stand: 31. August 2015).

[52] http://malware.dontneedcoffee.com/ (Stand: 31. August 2015).

5.4.7 Log Jam und FREAK-Lücken

Es gab im Berichtszeitraum zwei grössere bekannt gewordene Lücken, welche die Sicherheit von verschlüsselten Verbindungen gefährden können: «FREAK» und «LogJam». Der Hintergrund beider Lücken liegt dabei in der Tatsache, dass es früher Export-Restriktionen der USA für kryptographische Produkte gab. Im Source Code von Kryptographie-Bibliotheken sind die dafür notwendigen *Fallback-Funktionen* teilweise noch vorhanden und können für diese Angriffskategorie ausgenutzt werden.

FREAK (Factoring Attack on *RSA*-EXPORT Keys) ermöglicht es, bei bestimmten Browsern schwache Schlüssel zu akzeptieren, die eine Entschlüsselung ermöglichen. Dies setzt aber voraus, dass sich ein verwundbarer Browser auf einen Server mit schwachen *Ciphers* verbindet. Betroffen waren eine Vielzahl von Browsern und client-seitigen Programmen.[53]

LogJam ist ein mit FREAK verwandter Angriff auf verschlüsselte Verbindungen, bei dem die Verschlüsselungsstärke der Verbindung soweit heruntergehandelt werden kann, dass die Verbindung dechiffrierbar wird. Dabei werden die beim Key Exchange mit *Diffie-Hellman* verwendeten Primzahlen so reduziert, dass eine Entschlüsselung möglich wird.[54]

5.5 Präventive Massnahmen

5.5.1 Neues Patch-Management von Microsoft

Während bei den Betriebssystemen für Mobilfunktelefone gerade über die Einführung eines regelmässigen Patch-Managements diskutiert wird, will Microsoft den traditionellen *Patchday* für Windows 10 Nutzer abschaffen und kontinuierliche Updates einführen. Ein Patchday wurde vor allem aufgrund der Anforderungen von Administratoren in grossen Firmen eingeführt, damit diese das Einspielen der Updates besser planen und testen können und dadurch verhindern, dass kritische Systeme nach dem Einspielen des Updates plötzlich nicht mehr funktionieren. Für Firmen will Microsoft unter dem Namen „Windows Update for Business„ diese Probleme mit sogenannten Distribution Rings lösen. Hierbei wird ein Netzwerk in verschiedene Ringe eingeteilt. Je nach Ring bekommen einige Systeme das Update früher als die anderen. Erst später werden dann die Updates an die restlichen Computer verteilt. Ausserdem können die Updates auf diese Weise risikoabhängig eingespielt werden. Computer, die ein höheres Infektionsrisiko haben, erhalten das Update schneller, die anderen etwas später. Zusätzlich können Administratoren Wartungsfenster bestimmen, wann Updates eingespielt werden sollen und wann nicht. Bei für Firmen kritischen Systemen will Microsoft aber erst einmal beim Patchday bleiben.[55]

---

53 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204 (Stand: 31. August 2015).

54 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000 (Stand: 31. August 2015).

55 http://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/ (Stand: 31. August 2015).

5.6 Weitere Themen

5.6.1 Einfache, aber folgenschwere Diebstähle

Das *Smartphone* ist aus der modernen Gesellschaft nicht mehr wegzudenken: Musik hören, E-Mails lesen, Termine managen oder sportliche Leistungen messen. Dem Smartphone werden fast alle unsere Daten anvertraut. Es ist klar, dass damit das Smartphone zu einer interessante Zielscheibe für Kriminelle aller Gattungen wird. Gerade bei elektronischen Geräten denkt man zuerst an elektronische Angriffsmethoden, sei es Datendiebstahl via Schadsoftware oder Erpressungsversuche via *Ransomware*. Im Juni 2015 kursierten in einigen deutschen Medien Meldungen, die daran erinnern, dass auch die herkömmlichen Erpressungsmethoden nicht zu unterschätzen sind. In Deutschland wurde eine Zunahme der Smartphone- und Laptopdiebstähle zwecks Erpressung von Managern und Geschäftsleuten verzeichnet. Die sinkenden Preise der Smartphones und die schwerer zu umgehenden Sicherheitsvorkehrungen machen den eigentlichen Diebstahl eines solchen Geräts grundsätzlich zunehmend unattraktiv. Sind auf einem Gerät aber Daten, die für eine bestimmte Person beziehungsweise deren Firma oder deren Kunden sehr wertvoll sind, lohnt sich ein solcher Diebstahl aus finanzieller Sicht rasch einmal.

In die Schlagzeilen brachte es ein Diebstahl, dem ausgerechnet Dieter Kempf, eine führende Persönlichkeit aus der Welt der Informatik, zum Opfer fiel. Der Geschäftsführer des Dienstanbieters Datev und Präsident des IT-Bundesverbandes BITKOM war auf dem Weg zum 14. Deutschen IT-Sicherheitskongress, an dem er einen Runden Tisch zur Frage «Sichere mobile Kommunikation» moderieren sollte. Als er aus dem Zug steigen wollte, näherten sich ihm drei Personen und entrissen ihm sein Notebook sowie ein Blackberry. Die Beschreibung des Tathergangs deckt sich mit derjenigen anderer Opfer: Die Diebe agieren in kleinen Gruppen, meistens zu Stosszeiten, in Zügen oder Bahnhöfen und bestehlen Personen, von denen sie vermuten, dass es sich um Geschäftsleute handelt.

Hierbei handelt es sich nicht um Cyberkriminelle, die sich physisch Zugang zu Daten verschaffen, sondern vielmehr um ganz gewöhnliche Taschendiebe, die begriffen haben, dass sich aus diesem Geschäftsmodell Gewinn schlagen lässt. Zu einer grossen Überfallswelle dürfte es zwar nicht kommen, da die Diebe vor Ort agieren müssen und bei der Kontaktnahme mit dem Opfer ein grosses Risiko eingehen. Dennoch zeigt das Beispiel exemplarisch auf, dass IKT-Geräte und vertrauliche Daten vielen Gefahren ausgesetzt sind.

- Sorgen Sie dafür, dass die Sicherheitsvorkehrungen auf Ihrem Smartphone korrekt aktiviert sind (z. B. Eingabe des PIN und automatische Sperre des Displays).
- Speichern Sie auf Ihren Privatgeräten keine vertraulichen Geschäftsinformationen.
- Lassen Sie Geräte, die vertrauliche Daten enthalten, nie unbeaufsichtigt.
- Sichern Sie Ihre Daten regelmässig (Backup / Cloud-Sync), um bei Verlust eines Gerätes nicht auch alle Daten zu verlieren.
- Diebstahlsicherung (z.B. „find my iPhone“)
- Diebstahlversicherung für Gerät und Daten

6 Tendenzen und Ausblick

6.1 Wenn Daten in ein anderes Leben führen

Die Problematik des Sammelns von personenbezogenen Daten und der anschliessenden Verwertungskette wurde bereits im letzten Halbjahresbericht angesprochen.[56] Häufig wird in diesem Zusammenhang der mögliche Missbrauch durch Firmen und Privatpersonen als Hauptproblem dargestellt. Kaum thematisiert wird jedoch, wie Einzelpersonen vorgehen können, wenn staatlichen Stellen und Aufsichtsbehörden Fehler unterlaufen, wie im nachfolgend erläuterten Vorfall. Es fehlt an Ratschlägen, was Betroffene unternehmen können, um die Fehlinformationen rückgängig zu machen und vor allem wie sie sich präventiv verhindern lassen.

Problematisch wird es beispielsweise, wenn Personen mit gleichem Namen und identischem Geburtsdatum in der Schweiz leben. Ihnen ergeben sich einige Stolpersteine, die mit der darin begründeten Verwechslungsgefahr einhergehen. Der «Beobachter», eine Schweizer Konsumentenzeitschrift, berichtete unter dem Titel «Verwechslung – Der doppelte Moser» über einen konkreten Fall. Die Vorkommnisse zeigen anschaulich, wie die Probleme zwar im Einzelfall gelöst werden können, die betroffene Person aber unverschuldet diese Korrekturen wiederholt einfordern muss. Die in diesem Fall erwähnten Personen Peter Moser aus Ipsach und Peter Moser aus Winterthur sind am exakt gleichen Tag geboren und werden von AHV und anderen Unternehmen resp. Behörden verwechselt.[57]

MELANI wurde im letzten Halbjahr über einen ähnlichen Fall informiert. Betroffen war hier ein Schweizer Bürger, der einen Doppelgänger mit identischem Vor- und Nachnamen, sowie dem exakt selben Geburtsdatum hat. Die Person, die sich bei MELANI gemeldet hat und fortan als Melder[58] bezeichnet wird, hat lediglich einen unterschiedlichen zweiten Vornamen. Die Serie der Verwechslungen startete mit einem Strafregister-Eintrag, die der Melder erhielt, aber eigentlich für den Doppelgänger bestimmt war. Es ist unangenehm, sich gegen einen Strafbefehl wehren zu müssen, mit dem man nichts zu tun hat. Weitere Verwechslungen gab es bei Krankenkassen, den Steuerbehörden und Gemeindeverwaltungen nach Wohnortwechseln. Ja sogar die Ombudsstelle, die auf das Problem aufmerksam gemacht wurde, verwechselte den Melder bei der Antwort mit dem Doppelgänger. In allen Fällen war die Beweislast durch das Opfer zu erbringen, obwohl der Fehler jedes Mal bei der Firma oder der Behörde lag. In anderen Fällen konnte der Melder durch die aktive Intervention bei den entsprechenden Stellen Verwechslungen gerade noch verhindern, welche zu Einreisesperren in gewisse Länder sowie falsche Zuweisung von Biometriedaten auf dem Passbüro geführt hätten. Wiederum hätte das System ohne Einfluss des unverschuldeten Opfers versagt.

---

[56] MELANI Halbjahresbericht 2014/2, Kapitel 5.1: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte/halbjahresbericht-2014-2.html (Stand: 31. August 2015).

[57] http://www.beobachter.ch/justiz-behoerde/buerger-verwaltung/artikel/verwechslung_der-doppelte-moser/ (Stand: 31. August 2015).

[58] Name ist der Melde- und Analysestelle Informationssicherung bekannt

Aus Sicht des Betroffenen ist das zentrale Problem, dass die oben geschilderten Angelegenheiten immer auf dieselbe Ursache der Identitätsverwechslung zurückzuführen sind. Als Betroffener muss man sich jedoch in jedem Einzelfall an die für die Branche, Verwaltungseinheit usw. zuständige Stelle wenden. Dies bringt für den Betroffenen einen enormen Aufwand ohne eigenes Verschulden mit sich, der nur in den seltensten Fällen vergütet wird. Man muss also jedes Symptom immer und immer wieder separat beseitigen. Es existiert keine zentrale Anlaufstelle, die im Querschnitt über alle betroffenen Institutionen für die Ursache der falschen Identifikation zuständig wäre und die Koordination für die Betroffenen übernehmen könnte. Auch sind durch die schnelle Weiterverbreitung von Fehlinformationen meistens nicht alle Systeme nach der Korrektur der Quelle automatisch nachgeführt, was wiederum Aufwand für den Betroffenen bedeutet.

In Anbetracht anstehender Abkommen beispielsweise dem automatischen Informationsaustausch (AIA), können sich auf der Verwechslung von Identitäten begründete Probleme schnell auf eine internationale Ebene ausweiten, was die Problematik bei der Richtigstellung der Falschzuordnungen noch steigern wird. Es sollte bei der Ausarbeitung von neuen Abkommen und Gesetzten nicht nur ein Fokus auf Verhinderung des Missbrauchs des Systems durch Einzelpersonen gelegt werden, sondern auch auf die Qualitätssicherung des Systems. Ausserdem sollte eine einfache Fehlerkorrektur sichergestellt sein.

6.2 Auf Leben und Tod - IKT im Gesundheitswesen

Infusionspumpen sind praktische Helfer im Behandlungsalltag. Für das entsprechende Krankheitsbild wird automatisch die richtige Dosierung des zugehörigen Medikaments bereitgestellt. Es ist ein unangenehmer Gedanke, dass der Inhalt des Infusionsschlauchs, der in den Körper mündet, von einem Aussenstehenden kontrolliert wird.

Im letzten Halbjahresbericht haben wir die Problematik der totalen Vernetzung von immer mehr Geräten im Rahmen des *Internet of Things (IoT)* beleuchtet. Dieser Trend macht auch vor medizinischen Geräten nicht halt. Mit deren Vernetzung hält aber auch die ganze Palette der damit verbundenen Risiken Einzug. So fand der Sicherheitsforscher Billy Rios Schwachstellen in Infusionspumpen der Marke Hospira.[59] Im ersten Anlauf gelang es ihm lediglich, die Grenzen zu manipulieren, bei denen dem zuständigen Pfleger eine Warnmeldung ausgegeben wird. Bei weiteren Versuchen gelang es ihm jedoch, die zu verabreichende Dosis aus der Ferne zu manipulieren. Dies teilte der Forscher Anfang Juni 2015 der Herstellerfirma, sowie der zuständigen amerikanischen Regulierungsbehörde «US Food and Drug Administration (FDA)» mit. Es dauerte anschliessend bis Ende Juli, bis die FDA eine offizielle Warnung herausgab.[60] Theoretisch genügend Zeit, um die Forschungsergebnisse in der Praxis zu erproben und die Schwachstelle zu testen. Aus dem Inhalt der Warnung ist ein weiteres Problem ersichtlich: Die FDA empfiehlt zwar, die Infusionspumpen vom Netzwerk zu trennen, warnt aber gleichzeitig, dass dann die Dosis-Datenbanken manuell aktuell gehalten werden müssen. Dies eröffnet wiederum neue Fehlerquellen. In vielen Branchen gewöhnt man sich schnell an praktische IKT-unterstützte

[59] http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ (Stand: 31. August 2015)

[60] http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm (Stand: 31. August 2015)

Funktionalitäten. Die Sicherheit der Automatisierungen muss zwingend bestmöglich aufgestellt sein und Rückfallebenen für den Problemfall müssen definiert sein.

In Folge des IoT-Trends werden immer neue Komponenten und Prozesse automatisiert und miteinander vernetzt. Neben den neuen Möglichkeiten und Optimierungen, welche diese Applikationen für den Anwender mit sich bringen, stellt es die Verantwortlichen aber auch vor neue Probleme. Wie das in Kapitel 5.3.2 beschriebene Beispiel des Boeing Dreamliners aufzeigt, wird zur Korrektur lieber ein funktionierender Workaround praktiziert, als durch einen gezielten Patch die zugelassene Konfiguration abzuändern, da dies allenfalls eine Re-Zertifizierung der Systeme zur Folge hätte.

Aber nicht nur die Anwender werden vor neue Probleme gestellt, auch die Regulatoren der entsprechenden Branchen müssen sich vermehrt mit IKT-Thematiken befassen. Im Falle der Medizinprodukte entscheidet die Richtlinie «93/42/EWG» über die Zulassung des Produktes in der Europäischen Union und auch der Schweiz. Auf 65 Seiten findet sich in Zusammenhang mit IKT einzig der Begriff Software mit dem einzigen spezifischen Passus: «Bei Produkten, die Software enthalten oder bei denen es sich um medizinische Software an sich handelt, muss die Software entsprechend dem Stand der Technik validiert werden, wobei die Grundsätze des Software-Lebenszyklus, des Risikomanagements, der Validierung und Verifizierung zu berücksichtigen sind.»

Der Stand der Technik wird hierbei in der Norm «EN62304» festgelegt: Eine methodisch umfassende Norm aus dem Jahre 2006 zum Softwarelebenszyklus von Medizinprodukten. Taucht eine Schwachstelle auf, liegt das Problem auch häufig nicht nur beim betroffenen Produkt, sondern bei der ungenügenden Konfiguration der umgebenden Netzwerke.

Wer sich bereits intensiv mit den neuen Risiken auseinandersetzt, sind die Versicherer. Für diese bedeuten die neuen Gefahren natürlich neue mögliche Geschäftsmodelle. Wer die mit der smarten Vernetzung einhergehenden Risiken nicht selber in den Griff bekommt, kann die möglichen finanziellen Schäden zumindest anderweitig absichern.

7 Politik, Forschung, Policy

7.1 Parlamentarische Vorstösse

Ge-schäft	Nummer	Titel	Einge-reicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Ip	15.3656	Gefahr für AKW Mühleberg durch Fernwartung des Computersystems. Fragwürdige Überwachung des Ensi	Martina Munz	18.06.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153656
Po	15.3359	Für eine innovative Armee	Fathi Derder	20.03.2015	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153359
Po	15.3769	Bericht zum Service public. SRG-Internetangebot auf Audio-/Videothek beschränken	Marco Romano	19.06.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153769
Ip	15.3723	Umsetzung der Experten-Empfehlungen zum Kinder- und Jugendmedienschutz	Barbara Schmid-Federer	19.06.2015	NR	EDI	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153723
Ip	15.3661	Verletzung der SRG-Konzession. Unterbindung illegaler Internetserien	Rutz Gregor A.	18.06.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153661
Ip	15.3657	Recht auf Vergessen für Internet-Nutzerinnen und -Nutzer	Martina Munz	18.06.2015	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153657
Po	15.3618	Bericht zum Service public Auftrag der SRG. Analyse nach Subsidiaritätsprinzip	Christian Wasserfallen	18.06.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153618
Ip	15.3615	Service public im Medienbereich	Edith Graf-Litscher	18.06.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153615
Po	15.3407	Schutz der Persönlichkeitsrechte	Yvonne Feri	05.05.2015	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153407
Mo	15.3358	Investitionsprogramm für die Informationsgesellschaft ankurbeln	Fathi Derder	20.03.2015	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153358
Ip	15.3352	Wie viel Steuern bezahlen die grossen Internetkonzerne in der Schweiz?	Margret Kiener Nellen	20.03.2015	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153352

Po	15.3307	Gesellschaft und Internet in der Schweiz 2030. Bericht	Edith Graf-Litscher	20.03.2015	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153307
Ip	15.3291	Export von Überwachungs- und Aufklärungstechnologie. Wo bleiben die Menschenrechte?	Pierre-Alain Fridez	19.03.2015	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153291
A	15.1027	Welche Vorkehrungen will der Bundesrat treffen, um in der Schweiz gewalttätigen Extremismus vorzubeugen?	Christian van Singer	20.03.2015	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20151027
Po	15.3759	Sicheres Datenverbundsnetz und weitere IT-Projekte des Bevölkerungsschutzes. Stand, Perspektiven, Ressourcenbedarf	Ida Glanzmann-Hunkeler	19.06.2015	NR	VBS	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153759
Ip	15.3692	Informatik in der Bundesverwaltung. Ein Fass ohne Boden?	Sylvia Flückiger-Bäni	18.06.2015	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153692
Ip	15.3137	Auslagerung der Bearbeitung von Steuerdaten	Philipp Hadorn	16.03.2015	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153137
Ip	15.3448	Welche Förderung für die Einführung autonomer Fahrzeuge?	Fathi Derder	06.05.2015	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153448
Ip	15.3375	Entwendung von SIM-Codes bei der Firma Gemalto durch die Geheimdienste NSA und GCHQ	Luc Recordon	20.03.2015	SR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20153375

7.2 Weitere Themen

7.2.1 Nationales Forschungsprogramm Big Data

Der Bundesrat hat Ende Juni 2015 ein neues Nationales Forschungsprogramm (NFP) *Big Data* lanciert. Das Budget für das NFP Big Data beläuft sich auf 25 Mio. CHF und sieht vor, die Grundlagen für einen wirksamen und angemessenen Einsatz der immer stärker wachsenden Datenmenge in allen Gesellschaftsbereichen zu schaffen. Die Forschungsdauer beträgt 5 Jahre. Die geförderten Projekte sollen wissenschaftliche Grundlagen für neuartige Lösungen im Bereich des Computing (Datenanalytik, Algorithmen, *Kryptologie*, Datenmanagement-Services, Sicherheit und Zugriffskontrollen) liefern, mit denen grosse Datenmengen effektiv und sicher genutzt werden können. Auf diesen Grundlagen aufbauend sollen gesellschaftliche (Gesundheitsbereich, öffentliche

Infrastrukturen) und wirtschaftliche Anwendungsbereiche kritisch untersucht werden, in denen grosse Datenmengen schon heute und in Zukunft noch mehr eine Realität sind. Namentlich auch unter dem Gesichtspunkt der Daten- und Systemsicherheit sowie unter regulatorischen Aspekten (Datenschutz, Schutz der Privatsphäre).

Die Leitungsgruppe des Nationalfondsprojekts Big Data wurde im Sommer 2015 gebildet. Die Ausschreibungen für die einzelnen Projekte und die Teilnahmebedingungen für Forschungsgruppen sollten im Laufe des Herbsts 2015 veröffentlicht werden. Wissenschaftliche Projektskizzen sind dann innert dreier Monate einzureichen, und mit einer definitiven Auswahl der Forschungsprojekte ist im Laufe des kommenden Jahres zu rechnen.

7.2.2 Neuorganisation Domainvergabe

Die per 1. Januar 2015 in Kraft getretene Verordnung über Internet-Domains (VID) zieht eine umfangreiche Neuorganisation der Domainvergabe in der Schweiz nach sich. Bis anhin hatte SWITCH sowohl die Funktion der Registerbetreiberin (Verwaltung der Datenbank der Domain-Namen, sog. Registry) als auch eines Registrars (Vermarktung von Domain-Namen) inne. Diese Doppelrolle ist nun aufgrund der neuen VID nicht mehr möglich. Die VID sieht vor, dass die Rolle des Network Information Center (NIC), also der Organisation, die die Ressourcen für den Betrieb des Domain Name Systems (DNS) eines Landes zentral verwaltet, dem BAKOM oder einer durch das BAKOM beauftragte Drittstelle zufällt (Art. 8 VID). Um in der Schweiz *Top Level Domains* (ccTLD oder gTLD) am Markt anbieten zu können, bedarf es eines Registrarvertrages mit der *ICANN* und der Registerbetreiberin. Mittlerweile sind 79 Registrare aus der ganzen Welt für den .ch TLD zugelassen, davon 46 Unternehmen aus der Schweiz. Der Transfer der .ch-Domain-Namen von SWITCH zu den Registraren ist denn auch seit geraumer Zeit im Gang. Für die gTLD .swiss ist gemäss VID jedoch ausschliesslich der Bund (BAKOM) zuständig, um den besonderen Nutzen für die Schweiz langfristig sicherzustellen.

Um einen geordneten und transparenten Migrationsprozess sicherzustellen und die Vergabe der Registrierungsstelle vorzubereiten, hat das BAKOM das Delegationsverhältnis mit SWITCH im Sinne einer Übergangsregelung im Rahmen von Art. 62 VID bis Mitte 2017 verlängert. Auf diesen Zeitpunkt wird die Registry-Funktion wiederum ausgeschrieben.

8 Publizierte MELANI Produkte

MELANI stellt neben den Halbjahresberichten für die breite Öffentlichkeit eine Anzahl verschiedenster Produkte zur Verfügung. Die folgenden Unterkapitel bieten eine Übersicht über die im Berichtszeitraum erstellten Blogs, Newsletter, Checklisten, Anleitungen und Merkblätter.

8.1 GovCERT.ch Blog

8.1.1 Joining the DNSSEC Day in Germany (nur in Englisch verfügbar)

30.06.2015 - DNSSEC stands for Domain Name System Security Extensions and has been introduced in 1999. The goal of DNSSEC is to implement authenticity and integrity in the DNS by taking advantage of digitally signing DNS records using public-key cryptography. DNSSEC helps you to prevent man-in-the-middle attacks on the DNS layer and DNS cache poisoning. Besides that, DNSSEC also provides a secure ground that allows you making usage of further security mechanisms that rely on DNSSEC, such as DNS-based Authentication of Named Entities (DANE).

➔ http://www.govcert.admin.ch/blog/9/joining-the-dnssec-day-in-germany

8.1.2 Outdate WordPress: Thousands of websites in Switzerland are vulnerable (nur in Englisch verfügbar)

08.06.2015 - The internet has grown very fast in the past 15 years. Thousands of new websites are going online every day. According to Netcraft, there are currently more than 850'000'000 active websites in the internet (May 2015). One of the reasons why the number of websites has grown that much is the use of content management systems (CMS), for example WordPress, Typo3, Joomla and Durpal. By using a CMS, you can easily publish content in the internet without needing IT knowledge. While CMS are something great, they are also a valuable target for hackers.

➔ http://www.govcert.admin.ch/blog/8/outdate-wordpress-thousands-of-websites-in-switzerland-are-vulnerable

8.1.3 Increase in DDoS extortion (DD4BC) (nur in Englisch verfügbar)

08.05.2015 - In the past days MELANI / GovCERT.ch has received several requests regarding a Distributed Denial of Service (DDoS) extortion campaign related to 'DD4BC'. The DD4BC Team (that is how the attackers call themselves) started its DDoS extortion campaigns in 2014. Since earlier this week, the DD4BC Team expanded their operation to Switzerland. MELANI / GovCERT.ch is aware of several high profile targets in Switzerland that have recently received a blackmail from DD4BC and have consequently suffered from DDoS attacks, obviously conducted by DD4BC.

➔ http://www.govcert.admin.ch/blog/6/increase-in-ddos-extortion-dd4bc

8.1.4 e-Banking Trojan Retefe still spreading in Switzerland (nur in Englisch verfügbar)

01.05.2015 - In July 2014, Trend Micro published a report about a threat called Retefe, an ebanking Trojan that is targeting financial institutions in Switzerland, Austria, Sweden and Japan. In fact, Retefe is already around since November 2013. Back then, MELANI already took appropriate action together with the affected financial institutions and ISPs in Switzerland to mitigate the threat. However, Retefe is still being distributed in recent spam campaigns, targeting Swiss Internet users.

➔ http://www.govcert.admin.ch/blog/5/e-banking-trojan-retefe-still-spreading-in-switzerland

8.1.5 Critical vulnerability in Magento: Many Swiss websites are still vulnerable (nur in Englisch verfügbar)

30.04.2015 - In February 2015, Magento (a popular eCommerce software for webshops) released a security patch addressing a critical vulnerability in its product. The vulnerability allows an attacker to send a special prepared HTTP request to any website running a vulnerable version of Magento in order to execute malicious code on the remote webserver (a so called Remote Code Execution RCE vulnerability). More than two months later, MELANI / GovCERT.ch still sees a fairly big amount of websites in Switzerland running an old, vulnerable version of Magento, exposing themselves and its visitors to cyber-attacks from the internet. Hackers can (ab)use the vulnerability to e.g. place malicious code on the victims website to infect its visitors with malware (Drive-By exploits).

➔ http://www.govcert.admin.ch/blog/4/critical-vulnerability-in-magento-many-swiss-websites-are-still-vulnerable

8.2 MELANI Newsletter

Im ersten Halbjahr 2015 hat MELANI folgende Newsletter publiziert:

8.2.1 Meldeportal gegen Phishing

29.07.2015 - In den vergangenen Jahren ist die Zahl der durch die Melde- und Analysestelle Informationssicherung MELANI bearbeiteten Anfragen bezüglich Phishing stark angestiegen. Bei den meisten Anfragen wurden uns Phishing E-Mails und Phishing-Webseiten gemeldet, welche Kunden von Finanzinstituten in der Schweiz, aber auch international bekannte Internet-Plattformen (wie z. B. Social Networks, E-Mail Dienste oder Online Payment Service Provider) im Visier haben. Um die Vielzahl der eingehenden Meldungen betreffend Phishing effizienter bearbeiten zu können, hat die Melde- und Analysestelle Informationssicherung MELANI eine Website aufgeschaltet, auf welcher vermeintliche Phishing Seiten gemeldet werden können.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/meldeportal_gegen_phishing.html

8.2.2 DDoS Angriffe und Erpressung : eine äusserst aktuelle Kombination

20.05.2015 - Verschiedene Fälle, welche MELANI in den letzten Wochen gemeldet wurden, deuten auf eine Zunahme von DDoS-Angriffen hin, welche vor allem den Zweck haben, von

den Opfern Geld zu erpressen. MELANI empfiehlt, nicht auf die Erpressung einzugehen und publiziert eine Anleitung mit verschiedenen Schutzmassnahmen vor DDoS-Angriffen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/ddos_angriffe_und_erpressung.html

8.2.3 E-Banking Trojaner «Dyre»: Lawinenartige Verbreitung

07.05.2015 - Im Februar 2015 hat die Melde- und Analysestelle Informationssicherung MELANI vor dem E-Banking Trojaner «Dyre» gewarnt, welcher Schweizer KMU im Visier hat. In den vergangenen Wochen wurden MELANI täglich mehrere hundert Neuinfektionen in der Schweiz gemeldet. Mittlerweile sind nicht mehr nur KMU betroffen, sondern vermehrt auch Privatanwender.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/information_dyre_2.html

8.2.4 10 Jahre MELANI: Ein Blick zurück und auf die aktuellen Bedrohungen in der Cyberwelt im 20. Halbjahresbericht

30.04.2015 - Die Melde- und Analysestelle Informationssicherung MELANI feiert ihr zehnjähriges Bestehen. Der 20. Halbjahresbericht legt deshalb nicht nur den Fokus auf die wichtigsten Ereignisse im zweiten Halbjahr 2014, welches vor allem durch Erpressungen sowie Angriffe auf schlecht geschützte Systeme geprägt war. Der Bericht, welcher heute publiziert wurde, wirft auch einen Blick auf die Entwicklung der Internetkriminalität während des letzten Jahrzehnts.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/20_melani_halbjahresbericht.html

8.2.5 Kunden von Schweizer KMUs: Ziel von massgeschneiderten Phishing-Angriffen

31.03.2015 - Nach wie vor versuchen Betrüger an sensible Daten wie Passwörter, Kreditkartendaten usw. zu gelangen. Zu diesem Zweck werden meist Webseiten kreiert, welche derjenigen einer Firma täuschend ähnlich sehen (beispielsweise werden gerne Internetauftritte von Banken oder Kreditkarteninstituten missbraucht). MELANI interveniert täglich, um solche betrügerische Webseiten vom Netz zu nehmen und so die Internetnutzer zu schützen.
Schon seit einiger Zeit missbrauchen die Betrüger allerdings nicht mehr ausschliesslich nur die Namen von grossen und bekannten Unternehmen, sondern verüben auch sehr gezielte Phishing-Angriffe mit dem Namen kleinerer Firmen. Diese Tendenz scheint sich zu akzentuieren: verschiedene Fälle, welche MELANI kürzlich zur Kenntnis gebracht wurden, zeugen von einer zunehmenden Professionalität dieser Angriffe. Betroffen sind KMU in den verschiedensten Tätigkeitsbereichen, welche eine Website betreiben, die in irgendeiner Weise Kunden-E-Mail-Adressen verwenden respektive gespeichert haben, beispielsweise für den Versand eines Newsletters.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/kunden-von-schweizer-kmus--ziel-von-massgeschneiderten-phishing-.html

8.2.6 E-Banking Trojaner hat Schweizer KMU im Visier

02.02.2015 - In den vergangenen Tagen gingen bei der Melde- und Analysestelle Informationssicherung MELANI vermehrt Meldungen von Schweizer KMU ein, welche verdächtige Spam E-Mails erhalten haben. Die gemeldeten E-Mails stammen dabei offensichtlich von angeblichen Geschäftspartnern und versuchen, den Empfänger der E-Mail mit einem e-Banking Trojaner zu infizieren. Bei einem kürzlich bekannt gewordenen Fall, welcher ein Freiburger Unternehmen betraf, wurde mittels demselben Trojaner ein siebenstelliger Betrag gestohlen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/e-banking-trojaner-hat-schweizer-kmus-im-visier.html

8.3 Checklisten und Anleitungen

Im ersten Halbjahr 2015 hat MELANI folgende Checklisten und Anleitungen publiziert:

8.3.1 Massnahmen gegen DDoS-Attacken

2015.06.25 - Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören.

Für das Opfer kann dies weitreichende wirtschaftliche Folgen haben. Die Motivation hinter solchen DDoS-Attacken sind meistens politischer Aktivismus, Erpressung oder Schädigung eines Konkurrenten. MELANI beobachtet aktuell eine Zunahme von erpresserischen DDoS-Attacken, bei welchen Lösegeld in Form von Cryptowährungen wie Bitcoin oder Litecoin eingefordert wird.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

8.3.2 Merkblatt IKT-Sicherheit für KMU

2015.01.30 - Dieses Merkblatt richtet sich an Schweizer KMU und soll diesen dabei helfen die IT-Sicherheit im Unternehmensnetzwerk zu erhöhen.

➔ https://www.melani.admin.ch/melani/de/home/dokumentation/checklisten-und-anleitungen/merkblatt-it-sicherheit-fuer-kmus.html

9 Glossar

Begriff	Erklärung
0-day Exploit	Sicherheitslücke, für die es vom Hersteller noch keinen Patch gibt.
Adware	Adware, eine Wortkombination aus Advertisement und Software, wird vielfach für Werbezwecke verwendet, indem die Surfgewohnheiten des Benutzers aufgenommen und dazu benutzt werden, entsprechende Produkte (z.B. durch Links) zu offerieren.
Big Data	Big Data bezeichnet Datenmengen, die zu gross oder zu komplex sind, um sie mit händischen und klassischen Methoden der Datenverarbeitung auszuwerten.
Bitcoin	Bitcoin ist ein weltweit verfügbares dezentrales Zahlungssystem und der Name einer digitalen Geldeinheit.
Bluetooth	Eine Technologie, die eine drahtlose Kommunikation zwischen zwei Endgeräten ermöglicht und vor allem bei Mobiltelefonen, Laptops, PDAs und Eingabegeräten (z.B. Computermaus) zur Anwendung gelangt.
Zertifikat	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.
Ciphers	Mit einem Cipher (Verschlüsselungsverfahren) kann ein Klartext in einen Geheimtext umgewandelt werden und umgekehrt der Geheimtext wieder in den Klartext rückgewandelt werden.
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.
Content Management Systemen (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. Die darzustellende Information wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Cross-Site-Scripting Angriff (XSS)	Eine Cross-Site Request Forgery (zu Deutsch etwa «Site-übergreifende Aufruf-Manipulation», ist ein Angriff auf ein Computersystem, bei dem der Angreifer unberechtigt Daten in einer Webanwendung verändert. Er bedient sich dazu eines Opfers, das ein berechtigter Benutzer der Webanwendung sein muss. Mit technischen Massnahmen oder zwischenmenschlicher Überredungskunst wird hierzu ein kompromittierter HTTP-Request an die Webanwendung abgesetzt.
Defacement	Verunstaltung von Webseiten
Diffie-Hellman Key Exchange	Mit dem Diffie-Hellman Key Exchange erzeugen zwei Kommunikationspartner einen geheimen Schlüssel, den nur diese beiden kennen.
Distributed Denial of Service (DDoS)	Eine DoS Attacke hat zum Ziel einen bestimmten Dienst für deren Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken. Dabei wird das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
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.
Ethernet	Ethernet ist eine Technologie, die Software und Hardware für kabelgebundene Datennetze spezifiziert.
Exploit Kit	Baukasten, mit denen Kriminelle Programme, Scripts oder Codezeilen generieren können, mit denen sich Schwachstellen in Computersystemen ausnutzen lassen.
Fallback Funktion	Eine Fallback-Funktion (Rückfallebene) repräsentiert ein Zweitsystem, das bei Ausfall des Erstsystems den Totalausfall verhindert.
FTP	File Transfer Protocol FTP ist ein Netzwerkprotokoll zur Dateiübertragung über TCP/IP-Netzwerke. FTP kann beispielsweise verwendet werden, um Webseiten auf einen Webserver zu laden.
Geolocation	Positionsbestimmung

GPS	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
Honeypots	Als Honeypot (deutsch: Honigtopf) wird in der Computersicherheit ein Computerprogramm oder ein Server bezeichnet, das Netzwerkdienste eines Computers, eines ganzen Rechnernetzes oder das Verhalten eines Anwenders simuliert. Honeypots werden eingesetzt, um Informationen über Angriffsmuster und Angreifverhalten zu erhalten.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) Die ICANN ist eine privatrechtliche Non-Profit-Organisation mit Sitz in der kalifornischen Küstenkleinstadt Marina del Rey. ICANN entscheidet über die Grundlagen der Verwaltung der Top-Level-Domains. Auf diese Weise koordiniert ICANN technische Aspekte des Internets, ohne jedoch verbindliches Recht zu setzen. Die ICANN untersteht dem US-amerikanischen Handelsministerium (Department of Commerce) und ist somit der US-Regierung unterstellt.
Industrielle Kontrollsysteme	Kontroll- oder Steuerungssysteme bestehen aus einem oder mehreren Geräten, welche das Verhalten von anderen Geräten oder Systemen steuern, regeln und/oder überwachen. In der industriellen Produktion ist der Begriff «Industrielle Kontrollsysteme» (engl. Industrial Control Systems, ICS) geläufig.
Internet of Things (IoT)	Der Begriff Internet der Dinge (englisch Internet of Things, Kurzform: IoT) beschreibt die zunehmende Computerisierung und Vernetzung von (Alltags-) Gegenständen.
IP Adressen	Adresse, welche einen Computer im Internet (oder einem TCP/IP-Netzwerk) identifiziert (Beispiel: 172.16.54.87).
JavaScript	Eine objektbasierte Script-Sprache zur Entwicklung von Applikationen. JavaScripts sind im HTML-Code integrierte Programmteile, die bestimmte Funktionen im Internet Browser ermöglichen. Ein Beispiel kann das Kontrollieren von Benutzereingaben bei einem Webformular sein. So kann überprüft werden, ob alle eingegebenen Zeichen bei geforderter Angabe einer Telefonnummer auch wirklich Zahlen sind. Wie ActiveX Controls werden JavaScripts auf dem Rechner des Webseitenbesuchers ausgeführt. Neben nützlichen, lassen sich leider auch schädliche Funktionen programmieren. Im Gegensatz zu ActiveX werden JavaScripts von allen Browsern unterstützt.

Kryptographie	Kryptographie ist die Wissenschaft der Verschlüsselung von Informationen.
Malware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde).
On-Board-Elektronik	Elektronik, die sich in einem sich bewegenden Objekt befindet und hilft die Steuerung dieses Objektes zu unterstützen.
One Time Passwort (OTP)	Ein One Time Passwort (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.
Patchday	Als Patchday wird ein Tag bezeichnet, an dem ein Hersteller seine Software-Aktualisierungen veröffentlicht.
Patch-Management	Patch-Management nennt man die Organisation, Softwareupdates zu verteilen respektive einzuspielen.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Nutzern 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 und Firmenlogos zustellen.
Plug-In	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plug-Ins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
QR-Code	Der QR-Code ist eine Methode, Informationen so aufzuschreiben, dass diese besonders schnell maschinell gefunden und eingelesen werden können.
Radio-Daten-System (RDS)	Das Radio Data System ermöglicht die Übermittlung von Zusatzinformationen beim Radio.
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
RSA-Verschlüsselung	Abkürzung für Rivest-Shamir-Adleman

	Verschlüsselung. Verschlüsselungsverfahren mit öffentlichen Schlüsseln, das 1978 eingeführt wurde. RSA ist ein asymmetrisches Verfahren.
SCADA-Systeme	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z.B. Energie- und Wasserversorgung).
SIM Karten	Die SIM-Karte (englisch: Subscriber Identity Module) ist eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient.
Smartphone	Ein Smartphone ist ein Mobiltelefon, das mehr Computerfunktionalität und -konnektivität als ein herkömmliches fortschrittliches Mobiltelefon zur Verfügung stellt.
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.
Spear Phishing	Gezielte Phishing-Attacke. Dem Opfer wird zum Beispiel vorgegaukelt, mit einer ihr vertrauten Person via E-Mail zu kommunizieren.
SQL-Injection	SQL-Injection (SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Überprüfung von zu übermittelnden Variablen entsteht.
SSL/TLS Tunnel	Tunnel bzw. Tunneling bezeichnet in einem Netzwerk die Konvertierung und Übertragung eines Kommunikationsprotokolls, das für den Transport in ein anderes Kommunikationsprotokoll eingebettet wird. SSL und TLS sind Protokolle, um im Internet verschlüsselt zu kommunizieren.
Top Level Domains	Jeder Name einer Domain im Internet besteht aus einer Folge von durch Punkte getrennten Zeichenfolgen. Als Top-Level-Domain bezeichnet man dabei den letzten Namen dieser Folge, der die höchste Ebene der Namensauflösung darstellt. Ist der vollständige Domain-Name eines Rechners bzw. einer Website beispielsweise de.example.com, so entspricht das rechte Glied (com) der Top-Level-Domain dieses Namens.
Traffic Distribution System (TDS)	Traffic Distribution Systems (TDS) sind Systeme, welche den Internetverkehr beim Abruf von Online Werbung zu der eigentlichen Zielseite leiten. Dies wird

	häufig verwendet um Schadsoftware auszuliefern.
Web Application Firewall	Eine Web Application Firewall (WAF) ist ein Verfahren, das Webanwendungen vor Angriffen über das Hypertext Transfer Protocol schützen soll.