Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

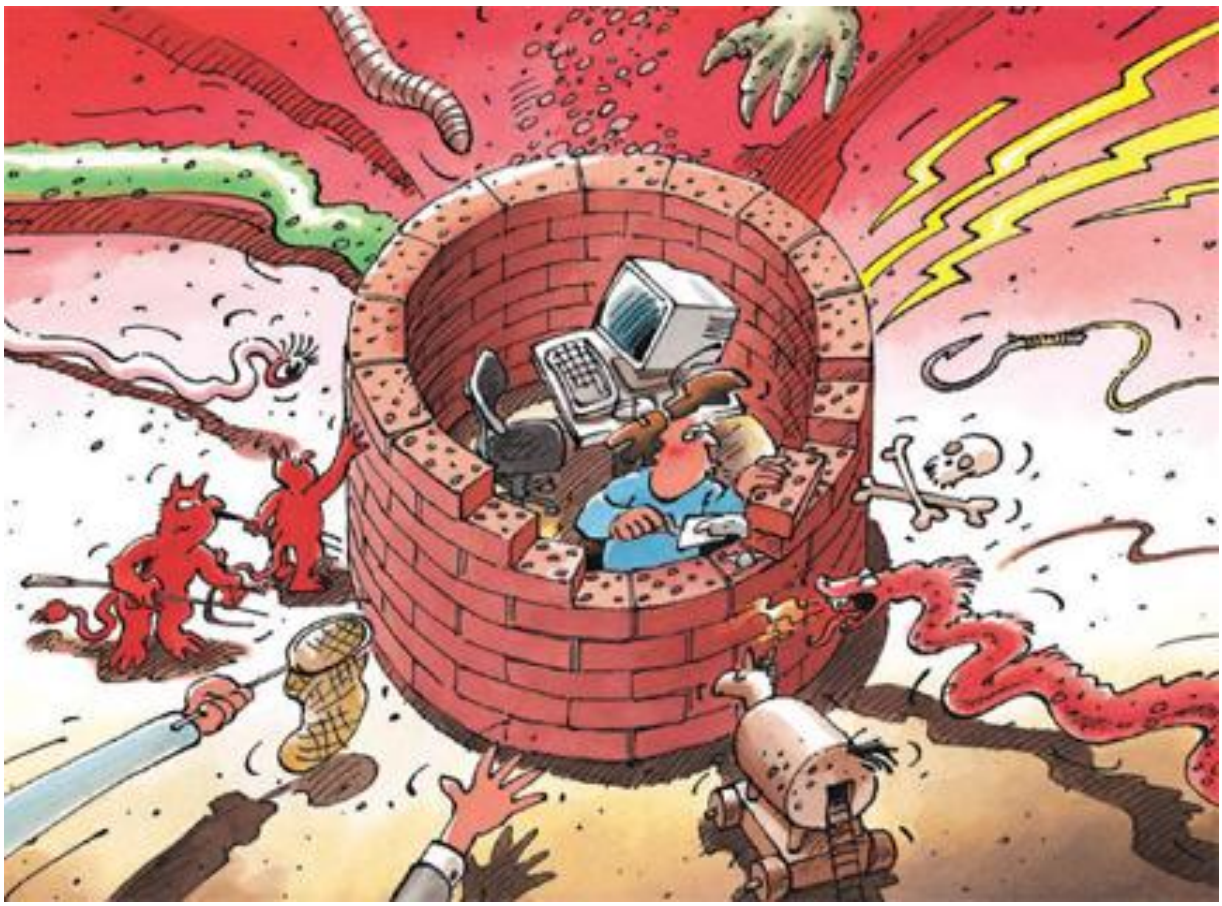
Informatiksteuerungsorgan des Bundes ISB
Nachrichtendienst des Bundes NDB

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

Informationssicherung

Lage in der Schweiz und international

Halbjahresbericht 2014/II (Juli – Dezember)



Inhaltsverzeichnis

1 Schwerpunkte Ausgabe 2014/II

- **10 Jahre MELANI**

  Die Melde- und Analysestelle Informationssicherung (MELANI) feierte am 1. Oktober 2014 ihr 10-jähriges Bestehen. 10 Jahre in denen eine enorme Entwicklung in den Informations- und Kommunikationstechnologien (IKT) stattgefunden hat. Die steigende Anzahl an Plattformen, Diensten und Internetnutzer wirkte sich auch auf die kriminelle Strukturen aus. In der Zwischenzeit hat sich ein regelrechter Cyber-Untergrundmarkt entwickelt, auf dem alles, was es für einen Angriff braucht, beschafft werden kann. Doch auch einige Staaten haben ihre Spionage- und Überwachungsmethoden stark ausgebaut und verfeinert. Fakten und Gedanken zu der Entwicklung im Internet der letzten 10 Jahre finden Sie in Kapitel 3.1.

  ► Aktuelle Lage national: Kapitel 3.1

- **Wieder Sicherheitslücken bei Verschlüsselung**

  Nach der Heartbleed-Lücke war *SSL* erneut von einer gravierenden Schwachstelle betroffen. Die als Poodle benannte Lücke, ist jedoch im Gegensatz zu Heartbleed kein Programmierfehler, sondern ein Designfehler. Abhilfe schaffte daher nur das Deaktivieren eines alten Verschlüsselungsstandards. Daneben sind auch diverse andere zum Teil gravierende Sicherheitslücken bekannt geworden. In der von der Firma MITRE unterhaltenen Datenbank, mit allen öffentlich bekannten Schwachstellen in Programmen, wurden weltweit im Jahr 2014 insgesamt 7945 Schwachstellen aufgenommen; so viele wie nie zuvor. Aufgrund dieser Zahl drängt sich zunehmend die Frage nach den Prozessen auf, die den Umgang mit gefundenen Sicherheitslücken regeln.

  ► Aktuelle Lage International: Kapitel 4.9, Kapitel 4.10, Kapitel 4.11
  ► Tendenzen / Ausblick: Kapitel 5.5

- **Schlecht geschützte Systeme – nicht nur eine Gefahr für die Betreiber**

  Offene Webcams, schlecht geschützte Funknetzwerke, veraltete *Content Management Systeme (CMS)* sind beliebte Angriffsziele. Auf den ersten Blick hinterlassen die Angriffe nur einen Schaden für den Betreiber, doch oft haben sie auch weitere Auswirkungen. So können kompromittierte Webseiten für *Phishing* oder das Verteilen von *Schadsoftware* missbraucht und kompromittierte E-Mail-Kontos für das Versenden von Spam eingesetzt werden. In Relation zur Bevölkerung war die Schweiz als Absender von Spam zwischenzeitlich weltweit auf Platz 3.

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

- **Spionage – am Arbeitsplatz, unterwegs und beim Kommunizieren**

  Es besteht ein ständiges Interesse und demzufolge ein ständiger Druck auf sensible Daten. Die im Bericht aufgeführten Beispiele zeigen, dass Spionageversuche immer und überall möglich sind, sei es am Arbeitsplatz, auf Dienstreise oder beim Telefonieren mit dem Mobiltelefon.

  ► Aktuelle Lage International: Kapitel 4.5, Kapitel 4.6, Kapitel 4.10

- **Die totale Vernetzung! Smart und Sicher?**

  Nicht nur das Telefon ist mittlerweile «smart», sondern auch Autos (smart car / smart drive), Wohnräume (smart home) respektive ganze Gebäude (smart building) und nicht zuletzt auch Industrieanlagen (smart factory / smart manufacturing) können Daten erheben, erhalten, verarbeiten, versenden, aus ihnen Befehle ableiten und physische Aktionen ausführen. Die damit verbunden Gefahren werden in Kapitel 5.2 diskutiert.

  ► Tendenzen / Ausblick: Kapitel 5.2

2 Einleitung

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

Ausgewählte Themen dieses Halbjahresberichtes sind in **Kapitel 1** kurz umrissen.

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

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

Kapitel 5.6 enthält ausgewählte parlamentarische Geschäfte mit Bezug zu Themen im Bereich Informationssicherung.

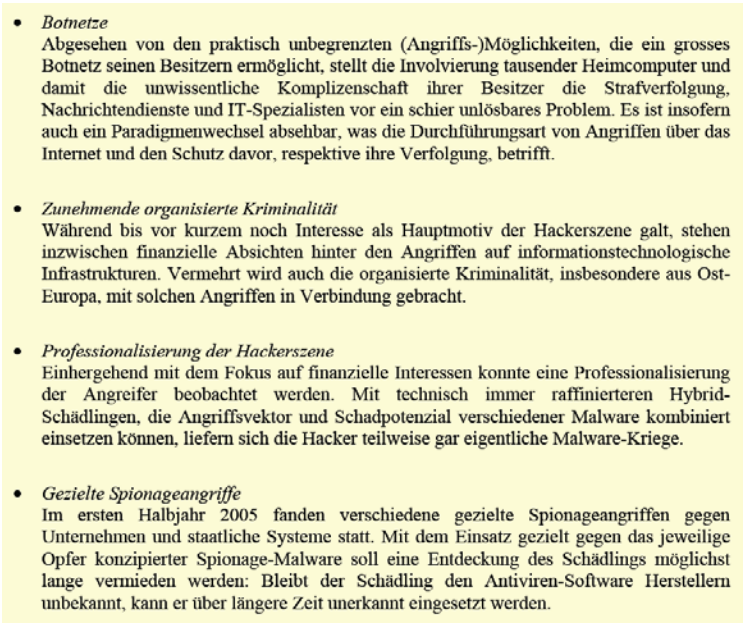
Aus Anlass des 10-jährigen Bestehens der Melde- und Analysestelle Informationssicherung ist dieser Ausgabe eine Tabelle mit den wichtigsten Ereignissen rund um das Thema Internet und Informationssicherung der letzten 10 Jahre beigelegt.

3 Aktuelle Lage IKT-Infrastruktur national

3.1 10 Jahre MELANI – ein Rückblick

Die Melde- und Analysestelle Informationssicherung (MELANI) feierte am 1. Oktober 2014 ihr zehnjähriges Bestehen. Zehn Jahre, in denen eine enorme Entwicklung in den Informations- und Kommunikationstechnologien (IKT) stattgefunden hat. Während dieser Zeit sind neue Plattformen, *Protokolle* und Kommunikationsgeräte erschienen. Man denke da nur an die Entwicklung im Bereich *Social Media* oder an die rasante Entwicklung bei *Smartphones*. Es sei erinnert, dass Facebook bei der Gründung der MELANI gerade mal acht Monate alt war und dementsprechend noch in den Kinderschuhen steckte. Der Kurznachrichtendienst Twitter startete sogar erst 2006 und das erste iPhone kam noch ein Jahr später auf den Markt. Rasant gestiegen ist zudem die Zahl der Internetnutzer: Gab es 2004 erst 900 Millionen Internetbenutzer waren es im Jahr 2014 bereits 3 Milliarden.[1]

Es ist selbstverständlich, dass auch Kriminelle und andere unfreundliche Akteure mit dieser technologischen und gesellschaftlichen Entwicklung mitgehen und es nicht verpasst haben, Profit aus den neuen Möglichkeiten zu schlagen. Die Zahl neuer, noch unerfahrener Internetnutzer generierte auch neue Opferkreise. Neue Dienste und Anwendungen schufen zusätzliche Gelegenheiten, Schwachstellen zu finden und auch auszunutzen. Beispielsweise ergab der Einsatz von standardisierter *Content Management System*-Software, welche oftmals nicht regelmässig aktualisiert wird, unzählige neue Angriffspunkte.[2]



- *Botnetze*
  Abgesehen von den praktisch unbegrenzten (Angriffs-)Möglichkeiten, die ein grosses Botnetz seinen Besitzern ermöglicht, stellt die Involvierung tausender Heimcomputer und damit die unwissentliche Komplizenschaft ihrer Besitzer die Strafverfolgung, Nachrichtendienste und IT-Spezialisten vor ein schier unlösbares Problem. Es ist insofern auch ein Paradigmenwechsel absehbar, was die Durchführungsart von Angriffen über das Internet und den Schutz davor, respektive ihre Verfolgung, betrifft.

- *Zunehmende organisierte Kriminalität*
  Während bis vor kurzem noch Interesse als Hauptmotiv der Hackerszene galt, stehen inzwischen finanzielle Absichten hinter den Angriffen auf informationstechnologische Infrastrukturen. Vermehrt wird auch die organisierte Kriminalität, insbesondere aus Ost-Europa, mit solchen Angriffen in Verbindung gebracht.

- *Professionalisierung der Hackerszene*
  Einhergehend mit dem Fokus auf finanzielle Interessen konnte eine Professionalisierung der Angreifer beobachtet werden. Mit technisch immer raffinierteren Hybrid-Schädlingen, die Angriffsvektor und Schadpotenzial verschiedener Malware kombiniert einsetzen können, liefern sich die Hacker teilweise gar eigentliche Malware-Kriege.

- *Gezielte Spionageangriffe*
  Im ersten Halbjahr 2005 fanden verschiedene gezielte Spionageangriffen gegen Unternehmen und staatliche Systeme statt. Mit dem Einsatz gezielt gegen das jeweilige Opfer konzipierter Spionage-Malware soll eine Entdeckung des Schädlings möglichst lange vermieden werden: Bleibt der Schädling den Antiviren-Software Herstellern unbekannt, kann er über längere Zeit unerkannt eingesetzt werden.

Abbildung 1: Schwerpunkte der ersten Ausgabe des MELANI-Halbjahresberichts: Botnetze, zunehmende Kriminalität, Professionalisierung der Hackerszene und gezielte Spionageangriffe

Wenn man den ersten MELANI-Halbjahresbericht aus dem Jahr 2005 analysiert, stellt man allerdings fest, dass die Themen weitgehend dieselben sind: Bereits 2005 gab es gezielte

[1] http://de.statista.com/statistik/daten/studie/186370/umfrage/anzahl-der-internetnutzer-weltweit-zeitreihe/ (Stand: 28. Februar 2015).

[2] Siehe aktueller Halbjahresbericht, Kapitel 3.5

Spionageangriffe, *Phishing*, *DDoS*, *Defacements* und *Social Engineering*. Sogar die Gefahren und Risiken für Nutzerinnen und Nutzer von Mobiltelefonen wurden im ersten Halbjahresbericht aufgebracht und die immer noch aktuelle Frage über die Anonymität im Internet wurde ebenfalls behandelt. Während sich die Grundthemen also nur wenig verändert haben, fand auf Seiten der Angreifer in den letzten zehn Jahren eine enorme Professionalisierung und Ausweitung der Arbeitsteilung statt. Heute spezialisieren sich die Cyberkriminellen auf die verschiedenen Themenbereiche wie das Suchen von Schwachstellen, die Produktion von Schadsoftware oder das Versenden von Spam-E-Mails. Vor zehn Jahren war gerade der Wechsel von «Hacken zur Freude» zu «Hacken mit finanziellen Absichten» im Gange und das Feld der Akteure beschränkte sich auf wenige Kriminelle. Bis heute hat sich ein regelrechter Cyber-Untergrundmarkt entwickelt, auf dem alles, was es für einen Angriff braucht, beschafft werden kann. Aber auch einige Staaten haben ihre Spionage- und Überwachungsmethoden stark ausgebaut und verfeinert.

Selbstredend hat sich dadurch die Anzahl der Angriffe enorm erhöht. Internetnutzer sehen sich im Gegensatz zum Jahr 2005 nicht mehr isolierten Ereignissen, sondern einer ständigen Bedrohung ihrer Daten oder Kommunikationsmittel gegenüber. Stellen, wie die Melde- und Analysestelle Informationssicherung MELANI, sowie ihre verschiedenen Partner, die im Umfeld der Sicherheit kritischer Informationsinfrastrukturen aktiv sind, stehen immer wieder vor neuen Herausforderungen. Um diese zu meistern, müssen Gegenmassnahmen überprüft und wenn nötig adaptiert werden. Firmen müssen Erkenntnisse über das sich rasch ändernde Umfeld ständig in ihre Risikostrategie einfliessen lassen und ihre Prozesse entsprechend anpassen. Auf der anderen Seite hat sich aber auch eine gewisse Routine und Gelassenheit eingespielt. Während beispielsweise 2005 eine auf die Schweiz ausgerichtete *Phishing*-Welle noch für Aufregung und ein grosses mediales Echo sorgte und auch die Bearbeitung eines solchen Vorfalles Neuland war, ist die Abwehr solcher *Phishing*-Angriffe, die heute mehrfach pro Tag passieren, zur Routine geworden. Auch das mediale Interesse beschränkt sich lediglich noch auf einzelne Fälle mit prominenten Opfern oder spektakulären Verlusten.

Bleibt noch die Frage, ob das Sicherheitsbewusstsein im IKT-Bereich in der Bevölkerung zugenommen hat. Anhand der Meldungen, die MELANI jeden Tag erhält, ist klar zu erkennen, dass die Nutzerinnen und Nutzer vorsichtiger geworden sind. Genau so deutlich ist aber auch, dass gerade in der Prävention noch grosses Potential steckt, um zukünftige Angriffe zu vereiteln.

Wussten Sie, dass die Melde- und Analysestelle Informationssicherung MELANI in den letzten 10 Jahren

- 20 Halbjahresberichte publizierte
- 33 Workshops für Betreiber kritischer Infrastrukturen organisierte
- 111 Newsletter publizierte
- 141 Betreiber kritischer Infrastrukturen in den MELANI-Informationsverbund aufnahm
- 1765 Informationen von und für Betreiber kritischer Infrastrukturen verarbeitete
- über 3000 Mal Provider anschrieb, damit diese *Phishing*-Webseiten deaktivieren
- über 9000 Anfragen aus der Bevölkerung beantwortete
- über 27000 Hinweise aus der Bevölkerung über das öffentliche Meldeformular erhielt

MELANI hat Trends in Form einer Timeline rund um die drei Themen Internet, Bedrohungen und Tätigkeit von MELANI bildlich dargestellt. Angesichts der vielen Ereignisse in den letzten zehn Jahren will die Grafik keinen Anspruch auf Vollständigkeit erheben, sondern auf einige Schwerpunkte hinweisen (siehe beigelegtes Dokument).

3.2 Spam – gegen aber auch von Schweizerinnen und Schweizern

Neben den üblichen *Spam*-E-Mails, die irgendwelche Medikamente und Potenzmittel anpreisen und bereits seit über einem Jahrzehnt Postfächer von Internetbenutzenden füllen, waren im zweiten Halbjahr 2014 vermehrt auch wieder E-Mails mit *Schadcode* (Malware) im Anhang unterwegs. Anders als in den Jahren zuvor, verzeichnete MELANI vermehrt E-Mails, welche anstelle einer ausführbaren Datei (üblicherweise mit der Dateiendung *.exe*, *.pif*, *.scr* oder *.com*) ein Text-Dokument im *Rich Text Format* (Dateiendung *.rtf*) beinhalteten. Dabei wird der Schadcode in das Text-Dokument eingebettet und der Empfänger dazu animiert, die darin enthaltene Datei mit einem Doppelklick zu öffnen.

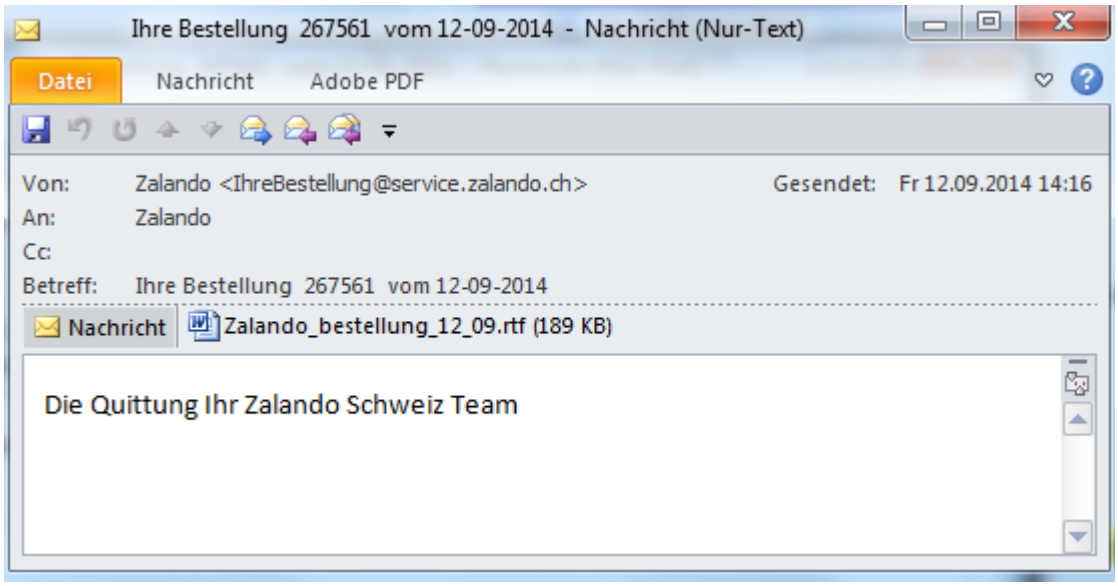


Abbildung 2: Gefälschte E-Mail mit angeblichem Absender Zalando und bösartigem rtf-Dokument im Anhang.

Viele dieser Spam-Kampagnen waren auf die Schweiz zugeschnitten und gaben vor, von bekannten Internet-Händlern wie z. B. Zalando oder Le-Shop zu stammen. Dies verleitete viele Nutzerinnen und Nutzer in der Schweiz, trotz sprachlicher Fehler im Text, das Dokument zu öffnen, den Schadcode auszuführen und dabei ihr Gerät mit einem E-Banking-Trojaner zu infizieren.

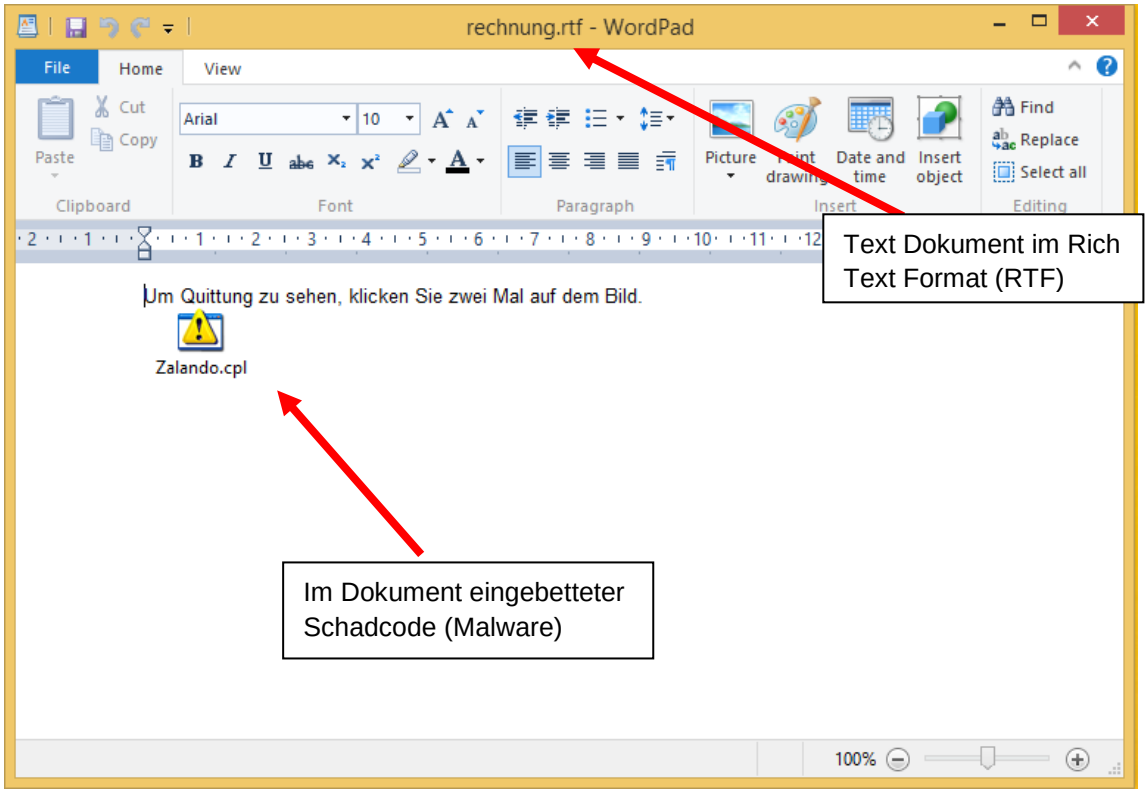


Abbildung 3: Beispiel einer bösartigen RTF Datei

Schweizer Nutzer sind jedoch nicht nur Ziel von Spam-E-Mails, sondern auch oftmals Absender solcher unerwünschten digitalen Sendungen. Dies zeigt zumindest ein im Juli 2014 veröffentlichter Bericht des Antiviren-Herstellers Sophos[3]. Darin wird die Anzahl von versendeten Spam-Mails in Relation zur Anzahl Einwohner der Länder gesetzt. Dabei landete die Schweiz im zweiten Quartal 2014 auf Platz 3. MELANI sind verschiedene Fälle bekannt, bei denen der Absender von Spam-Mails aus der Schweiz stammte. In einem Fall wurden über einen gehackten Account einer Schweizer E-Mail Adresse über 18‘000 Spam E-Mails versendet. Meist haben die unwissenden Besitzer der E-Mail Konten zuvor ihre Login-Daten bei einem *Phishing*-Angriff preisgegeben. In anderen Fällen befand sich Schadsoftware auf den betroffenen Computern.

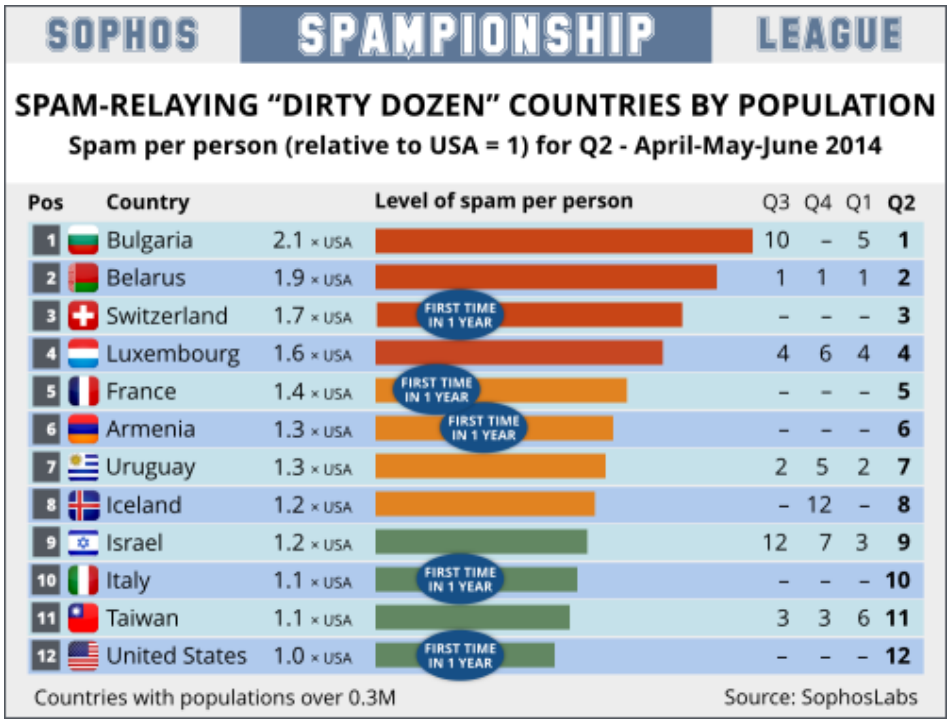


Abbildung 4: Spam-Statistik (Quelle: Sophos)

MELANI empfiehlt beim Umgang mit E-Mails Vorsicht walten zu lassen und verweist auf die Verhaltensregeln von MELANI:
http://www.melani.admin.ch/themen/00166/00172/index.html?lang=de

Um das Fälschen von Absender-E-Mail-Adressen zu verhindern bzw. einzuschränken, empfiehlt MELANI den E-Mail-Providern zudem, den Einsatz entsprechender Technologien wie beispielsweise SPF und DKIM:

Sender Policy Framework (SPF):
http://www.openspf.org/

DomainKeys Identified Mail (DKIM):
http://www.dkim.org/

[3] Sophos: Dirty Dozen Spampionship – which country is spewing the most spam? https://nakedsecurity.sophos.com/2014/07/22/dirty-dozen-spampionship-which-country-is-spewing-the-most-spam/ (Stand: 28. Februar 2015).

3.3 Weltwoche – Opfer einer Cyber-Attacke

Auf polarisierende Ereignisse wird immer mehr auch im Internet reagiert, insbesondere wenn es um religiöse oder politische Themen geht. Das Internet dient dabei regelmässig als Ventil. Aktuelles Beispiel sind die Reaktionen auf das Attentat gegen das Satiremagazin Charlie Hebdo: Neben den weltweiten Solidaritätsbekundungen «Je suis Charlie» auf verschiedensten Social Media Plattformen, wurden in Frankreich auf der anderen Seite massenhaft *Webseiten verunstaltet (Defacements)* und mit Propaganda von Islamisten versehen. Solche Defacements bedürfen zwar keines grossen Know-hows, rufen jedoch meist ein grosses Medieninteresse hervor und verfehlen demzufolge ihre Wirkung nicht.

Auch die Schweiz war schon mehrere Male von solch politisch oder religiös motivierten Angriffen betroffen. Erwähnt sei beispielsweise der *DDoS*-Angriff auf die Postfinance nach der Sperrung des Kontos von Wikileaks Gründer Julien Assange im Jahre 2010[4] oder die Verunstaltung von mehreren tausend Webseiten nach der Annahme der Minarettbauverbotsinitiative im Jahre 2009[5].

Die Publikation eines Koran-kritischen Artikels von Andreas Thiel in der Ausgabe der Weltwoche vom 28. November 2014 führte ebenfalls zu einer Reaktion im Internet: Ein *DDoS*-Angriff legte die Webseite der Weltwoche für längere Zeit lahm.[6]

Die Zunahme und teils schiere Wucht von *DDoS*-Angriffen in den letzten Monaten ist eine bedenkliche Entwicklung. So gelang es beispielsweise der Hackergruppe Lizard Squad an Weihnachten, zwei der grössten Online-Dienste im Unterhaltungsbereich, das Sony Playstation Network und Xbox Live, gleichzeitig für mindestens 24 Stunden de facto vom Netz zu nehmen. Der damit angerichtete Schaden lässt sich schwer beziffern. Es ist deshalb für jedes Unternehmen, dessen Geschäftstätigkeit von der Erreichbarkeit seiner Website und/oder der Internetkonnektivität abhängig ist, empfehlenswert, mit den Website- und Hosting-Verantwortlichen die Risiken solcher Angriffe abzuklären und Abwehrmassnahmen zu planen. Dies beinhaltet neben eigenen technische Massnahmen zur Erkennung und Abwehr typischerweise auch die Einschätzung der Fähigkeiten des *Upstream*-Providers und dessen vertragliche Verpflichtungen im Ereignisfall.

3.4 Schlecht geschützte Systeme – 141 offene Webcams in der Schweiz

Immer mehr Geräte besitzen eine *Ethernet*- oder *WLAN*-Schnittstelle und können ans Internet angeschlossen werden. Die gebräuchlichsten Geräte sind zum Beispiel Webcams, Dateiablagen, Drucker, Scanner und Musik- oder Videoserver. In Zukunft wird sich diese Palette noch stark erweitern (siehe hierzu das Kapitel 5.2 Totale Vernetzung! Smart und Sicher?). Gerne geht dabei vergessen, dass diese Geräte meist für den Gebrauch in einem internen Netzwerk vorgesehen und vorkonfiguriert sind. So sind diese entweder gar nicht

[4] MELANI Halbjahresbericht 2010/2, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01122/index.html?lang=de (Stand: 28. Februar 2015).

[5] MELANI Halbjahresbericht 2009/2, Kapitel 3.2: http://www.melani.admin.ch/dokumentation/00123/00124/01109/index.html?lang=de (Stand: 28. Februar 2015).

[6] http://www.tagesanzeiger.ch/schweiz/standard/Nach-KoranKritik-Weltwoche-ist-Opfer-einer-CyberAttacke/story/19607439 (Stand: 28. Februar 2015).

oder nur durch ein schwaches Standard-Passwort geschützt. Der Schutz wird dabei über die zentrale *Firewall* respektive den *Router* gewährleistet, welche den direkten Zugriff aus dem Internet auf die Geräte verhindert. Fehlt dieser Schutz und sind diese direkt am Internet angeschlossen oder werden die Geräte absichtlich für den Zugriff im Internet freigegeben, sind sie dementsprechend für alle sichtbar und können theoretisch, wenn nur ein schlechter oder gar kein Passwortschutz vorhanden ist, auch von jeder beliebigen Person aufgerufen werden.

Ein diesbezüglicher Fall machte im November 2014 Schlagzeilen. Von zahlreichen Zeitungen wurde berichtet, dass tausende Webcams gehackt worden seien und die Live-Bilder über eine russische Webseite abgerufen werden konnten. Darunter befanden sich auch 141 Webcams, die der Schweiz zugeordnet werden konnten.[7] Neben eher unspektakulären Ansichten auf Garagen, fanden sich auch problematische Aufnahmen beispielsweise von Kleinkind-Überwachungskameras (Baby-Cams). Eine genauere Analyse ergab jedoch, dass das Hacken lediglich daraus bestand, Standardpasswörter zu benutzen. Die Benutzer hatten vergessen, die voreingestellten Passwörter zu ändern.

Geräte, welche direkt am Internet angeschlossen sind, gehören besonders geschützt. Dies umfasst nicht nur das Setzen von Passwörtern, die den aktuellsten Anforderungen entsprechen, sondern auch das konsequente Updaten der Geräte mit der neuesten Software respektive *Firmware*.

Dieser Fall hat also weniger mit Hacking, denn mit fahrlässiger Konfiguration durch den Betreiber zu tun. Er zeigt jedoch beispielhaft auf, dass auch der Zugang zu Kameras im Fokus von Kriminellen stehen kann. Dies hängt unter anderem auch damit zusammen, dass Webkameras mittlerweile in vielen Geräten zu finden sind. So besitzen Smartphones, Tablets, Laptops und auch diverse Fernsehgeräte eine eingebaute Kamera. Auf der anderen Seite ist die Sensibilität der Benutzenden bezüglich eingebauter Kameras noch gering. Ist beispielsweise eine Malware auf einem Gerät mit Kamera installiert, ist es möglich, in diese einzudringen. Je nachdem, wo ein solches Gerät steht, kann dies für das Opfer grosse Nachteile mit sich bringen, insbesondere, wenn man daran denkt, an welche Orte beispielsweise ein Smartphone überall mitgenommen wird.

MELANI empfiehlt, Webcams bei Nichtgebrauch durch ein Klebeband abzudecken. Mittlerweile gibt es auch spezielle Kamera-Abdeckungen, mit welchen man die Kameralinse temporär abdecken kann.

[7] http://www.tagesanzeiger.ch/digital/internet/141-Schweizer-Webcams-gehackt-und-live-ins-Netz-gestellt/story/20973442 (Stand: 28. Februar 2015).

Abbildung 5: Temporäre Kamera-Abdeckung in offener (links) und geschlossener Position[8]

3.5 CMS – Schwachstellen und fehlende Sensibilität bei Web-Administratoren

Ein Grossteil der *Phishing*-Seiten und *Drive-by-Infektionen* wird auf Webseiten platziert, welche mit *Content Management Systemen (CMS)* administriert werden, die nicht auf dem neusten Stand sind. Allein im Jahr 2014 wurden in der CMS-Software Drupal 14 Schwachstellen entdeckt, in Joomla! deren neun und in Wordpress sogar 29.[9] Ein regelmässiges Update der CMS-Software ist deshalb für jeden Betreiber von Websites essentiell – trotzdem wird in vielen Fällen gerade diesem Bereich zu wenig Beachtung geschenkt. Es gibt immer noch viele Website-Betreiber, die ein CMS installieren und es dann versäumen, regelmässig die Updates einzuspielen. Solche verwundbaren Websites können mit entsprechenden Tools automatisiert aufgefunden und angegriffen werden. Somit ist es für Kriminelle relativ einfach, auf diese Weise eine grosse Zahl von Webauftritten aufzuspüren und zu manipulieren.

In einem besonders schwerwiegenden Fall sperrte Google sogar 11'000 Webseiten aus dem Suchindex. Dies, nachdem angeblich bereits über hunderttausend WordPress-Installationen mit der Schadsoftware «Soak Soak» infiziert worden waren und somit Malware auf die Rechner der Website-Besucher installierten.

In einem anderen Fall erfolgte die Kompromittierung nicht über das Ausnutzen einer Sicherheitslücke. Die Angreifer stellten Betreibern von Content Management Systemen (CMS) kostenlos ein manipuliertes *Plug-in* oder (Design-)Thema zur Verfügung. Dieses enthielt jedoch eine Malware, die den Zugriff auf die Webserver ermöglichte. Zehntausende Webserver wurden mit diesem Schadcode namens «CryptoPHP» infiziert, welcher vor allem für Drupal, WordPress oder Joomla verteilt wurde. Einmal mit CryptoPHP infiziert, wird der Code für die so genannte *Black Hat Search Engine Optimization (BHSEO*) verwendet. Damit werden meist Schlüsselwörter oder manipulierte Seiten in kompromittierte Websites eingefügt, um das *Ranking* bei Suchmaschinen zu beeinflussen. Über den Zugriff auf die Webserver können die Angreifer aber auch die Inhalte von Webseiten verändern und Drive-by Infektionen oder *Phishing*-Seiten, aber auch schlicht Falschinformationen aufschalten. Zudem agieren die mit CryptoPHP infizierten Webserver als Teil eines *Botnetzes*.

---

8 http://www.soomz.io (Stand: 28. Februar 2015).

9 http://www.cvedetails.com (Stand: 28. Februar 2015).

Angriffe auf CMS lassen sich durch das erwähnte *Patch*ing (zeitnahes Einspielen von Sicherheitsaktualisierungen) massiv reduzieren. Es gibt jedoch eine Reihe weiterer Massnahmen, welche zur Sicherheit von CMS beitragen. Empfehlungen finden Sie auf der MELANI-Webseite unter «Checklisten und Anleitungen».[10]

3.6 Erpresserische Schadsoftware im Vormarsch: Neue Schadsoftware Synolocker – Fälle auch in der Schweiz

Die Landschaft von erpresserischer Schadsoftware weitet sich ständig aus. Nachdem vor ein paar Jahren nur *Ransomware* gesehen wurde, welche den Bildschirm blockiert, aber die mit einigen Kniffen wieder deblockiert werden konnte, besitzen die aktuellen Versionen ein viel grösseres Schadenspotential. Nach «Cryptolocker», den wir im letzten Halbjahresbericht thematisiert haben, ist in der aktuellen Berichtsperiode eine neue Schadsoftware mit dem Namen «Synolocker» aufgetaucht. Auch in der Schweiz gab es zahlreiche Fälle, welche MELANI gemeldet wurden. Bei einer Infektion werden alle Daten auf einem betroffenen Netzwerk-Datenspeicher (*Network Attached Storage, NAS*) verschlüsselt und für den Private Key, der für die Entschlüsselung benötigt wird, eine Geldforderung gestellt. Auf dem Rechner des Opfers landet nur der für die asynchrone Verschlüsselung nötige Public Key. Eine Entschlüsselung ohne den dazugehörigen Private Key ist nahezu unmöglich. Die Infektion benötigte in diesem Falle keine Benutzerinteraktion, sondern nutzte gezielt eine Sicherheitslücke in den NAS-Geräten der Firma Synology aus. Dabei handelte es sich allerdings nicht um eine unbekannte Sicherheitslücke, sondern um eine, die bekannt war und für die seit Dezember 2013 ein *Patch* verfügbar ist.[11] Die gleiche Sicherheitslücke wurde anscheinend im Februar 2014 bereits durch eine andere Schadsoftware ausgenutzt. Damals hatten Hacker auf den NAS-Geräten Bitcoin-Schürfprogramme installiert und ohne Wissen der Nutzer Kryptomünzen erzeugt.[12]

Gerade bei Routern, Netzwerk-Datenspeichern und ähnlichen Geräten wird allzu oft vergessen, dass hier auch ein Update einzuspielen ist (siehe hierzu auch Halbjahresbericht 1/2014[13]). Dies ist besonders gravierend, wenn diese Geräte direkt am Internet angeschlossen sind.

Im August 2014 tauchte ein weiterer Verschlüsselungs-Trojaner mit dem Namen «CTB-Locker» auf. Speziell an diesem Trojaner ist, dass die Kommunikation mit seinen Kommandoservern verschlüsselt verläuft und er den *Anonymisierungsdienst Tor* verwendet, um seine Spuren zu verwischen. Dies erschwert der Polizei und den Sicherheitsfirmen das Finden und die Analyse dieser Kommandoserver.

Es gab aber auch gute Nachrichten im zweiten Halbjahr 2014: Die IKT-Sicherheitsdienstleister FireEye und Fox-IT haben einen Gratis-Service zur Verfügung gestellt, der es Opfern von Cryptolocker ermöglicht, die durch die Schadsoftware

---

10 http://www.melani.admin.ch/dienstleistungen/00132/01556/index.html?lang=de

11 http://www.heise.de/security/meldung/Jetzt-updaten-Aeltere-Synology-NAS-Geraete-anfaellig-fuer-Ransomware-2287427.html (Stand: 28. Februar 2015).

12 http://www.synology-forum.de/showthread.html?50468-Aktive-Hackangriffe-auf-DSM-Versionen-kleiner-4-3-3810-Update-3 (Stand: 28. Februar 2015).

13 MELANI Halbjahresbericht 2014/1, Kapitel 4.13: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=de (Stand: 28. Februar 2015).

verschlüsselten Daten wieder zurückzuerlangen.[14] In einer Aktion des FBI gegen das Cryptolocker-*Botnetzwerk*, konnten die privaten Schlüssel sichergestellt werden. Mit diesen ist es möglich, die Daten zu entschlüsseln. Auch im Falle von Synlocker ist es nicht ausgeschlossen, dass durch Recherchen und Ermittlungen, die entsprechenden Kryptoschlüssel, wie im Fall von Cryptolocker, zu einem späteren Zeitpunkt sichergestellt werden können. So sollten allfällig bereits durch Synolocker verschlüsselte und nicht wiederherstellbare Daten auf jeden Fall aufbewahrt werden.

Auf dem Computer abgelegte Daten sollten regelmässig auf externe Speichermedien kopiert werden (*Backup*). Diese sollten nur während des Backupvorgangs am Computer angeschlossen sein. Sowohl Betriebssysteme als auch alle auf den Computern installierte Applikationen (z. B. Adobe Reader, Adobe Flash, Sun Java etc.) müssen konsequent auf den neuesten Stand gebracht werden. Falls vorhanden, am besten mit der automatischen Update-Funktion. Dies gilt ebenfalls für die *Firmware* von *Routern*, *NAS*, Musikservern, usw.

3.7 Swiss Internet Security Alliance - Zusammenarbeit für mehr Sicherheit im Internet

Mit dem Ziel, der Cyberkriminalität mit vereinten Kräften die Stirn zu bieten, gründeten Internet-Anbieter, Banken und weitere Partner am 12. September 2014 die Swiss Internet Security Alliance (SISA). Mit dieser branchenübergreifenden Partnerschaft wollen die Mitglieder ihr Engagement für die Sicherheit ihrer Dienstleistungen und Kunden unterstreichen. Die Gründung der SISA bringt das Expertenwissen verschiedener Branchenvertreter zusammen und fördert den Austausch unter Mitbewerbern. So stellt sie denn auch als grösstes Kapital das Wissen, die Erfahrung und die technische Kompetenz ihrer Mitglieder ins Zentrum. Zu ihren Mitgliedern zählen: asut, Centralway, Credit Suisse, cyscon Schweiz, Hochschule Luzern, Hostpoint, Migros Bank, PostFinance, Raiffeisen, Sunrise, Swisscard, Swisscom, SWITCH, UBS, upc cablecom und Viseca. Sie verfügen über langjährige Erfahrung im Umgang mit Sicherheit im Internet. Der Verein steht weiteren Interessierten offen.[15]

[14] https://www.fireeye.com/blog/executive-perspective/2014/08/your-locker-of-information-for-cryptolocker-decryption.html (Stand: 28. Februar 2015).

[15] https://www.swiss-isa.ch/ (Stand: 28. Februar 2015).

4 Aktuelle Lage IKT-Infrastruktur international

4.1 Cyberangriff gegen Netzwerk von Sony Pictures Entertainment

Am 24. November 2014 erschien weltweit auf Computer-Arbeitsplätzen von Sony Pictures Entertainment (SPE) eine Nachricht, dass das Firmennetz von einer Gruppe namens «Guardians of Peace» gekapert worden sei. Die Gruppe gab an, interne Daten aus dem Firmennetzwerk kopiert zu haben und drohte, diese zu veröffentlichen. Neben der Fähigkeit, Daten zu stehlen, soll die Schadsoftware auch eine Daten-Löschroutine besessen haben. Das gesamte Netzwerk war anschliessend während mehreren Tagen nicht mehr verfügbar. Die Gruppe «Guardians of Peace» behauptete, im Besitz von 100 Terrabytes Daten zu sein, was in etwa 150‘000 Daten CDs entspricht. Sie wollen dabei Personaldaten, wie die Lohnliste der 6000 Mitarbeitenden und des Topkaders, interne E-Mails aber auch nicht veröffentlichte Filme kopiert haben. Fünf noch unveröffentlichte Filme tauchten dann Anfang Dezember tatsächlich auf Tauschbörsen auf, ebenfalls kursierte eine Version des Drehbuchs zum neuen James-Bond-Film «Spectre» im Netz. Bereits am 21. November 2014 ging eine Erpressungs-E-Mail mit einer Geldforderung bei der Geschäftsleitung von Sony Pictures Entertainment ein. Eine andere Gruppe mit dem Namen «God’s Apostls» drohte SPE mit einem «ganzheitlichen Angriff», wenn sie für einen nicht näher definierten Schaden, den sie angerichtet hätten, nicht aufkommen würden. Die in der E-Mail gesetzte Deadline an die Geschäftsleitung war der 24. November – also der Tag der Veröffentlichung des Angriffs.[16] Der Zusammenhang der beiden Gruppen «Guardians of Peace» und «God’s Apostls» blieb allerdings unklar.
Bald wurde spekuliert, dass dieser Angriff mit der geplanten Veröffentlichung des Filmes «The Interview» zusammenhängen könnte. «The Interview» ist eine Filmkomödie, welche von einem Mordkomplott der CIA gegen Nordkoreas Staatsoberhaupt Kim Jong-un handelt und an Weihnachten 2014 in die Kinos kommen sollte. Im Juli 2014 hat sich der nordkoreanische UN-Botschafter beim UN-Generalsekretär über die Handlung des geplanten Filmes beschwert. Bereits am 1. Dezember wurde aus US-Kreisen eine nordkoreanische Täterschaft hinter dem Angriff gegen Sony vermutet.[17] Am 8. Dezember tauchte dann eine Mitteilung der Gruppe «Guardians of Peace» auf der Webseite des Hostingdienstleisters GitHub auf, welche explizit forderte, auf die Veröffentlichung des Filmes zu verzichten: «Stop immediately showing the movie of terrorism which can break the regional peace and cause the War!».
Das für die Aufklärung des Vorfalls eingeschaltete FBI hat am 19. Dezember die ersten Erkenntnisse publiziert.[18] Die Ermittler erklärten dabei, dass sie genug Informationen hätten, die darauf schliessen lassen, dass die nordkoreanische Regierung hinter diesem Angriff stecke. So gebe es beispielsweise bei der Schadsoftware, welche die Daten gelöscht habe, Verbindungen zu einer Schadsoftware, welche Nordkorea schon früher entwickelt habe. Es seien Ähnlichkeiten in Programmiercode, Verschlüsselungsalgorithmen und Löschmechanismen gefunden worden. Zudem soll es eine bedeutende Überschneidung zwischen den verwendeten Infrastrukturen und früheren Angriffen mit mutmasslich nordkoreanischem Ursprung geben. So hatten die in der Malware einprogrammierten IP-

[16] http://www.hotforsecurity.com/blog/leaked-emails-reveal-that-hackers-demanded-money-from-sony-pictures-before-attack-10964.html (Stand: 28. Februar 2015).
[17] http://www.reuters.com/article/2014/12/02/us-sony-cybersecurity-malware-idUSKCN0JF3FE20141202 (Stand: 28. Februar 2015).
[18] http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (Stand: 28. Februar 2015).

Adressen mit bekannter nordkoreanischer Infrastruktur kommuniziert. Ebenfalls gebe es Ähnlichkeiten mit den Angriffen gegen südkoreanische Banken und Rundfunkanstalten im März 2013 (DarkSeoul)[19], bei welchen das FBI ebenfalls Nordkorea verantwortlich gemacht hatte.
Das Aussenministerium Nordkoreas wies die Anschuldigungen umgehend mit der Aussage zurück, dass sie beweisen könnten, dass der Angriff nichts mit der nordkoreanischen Regierung zu tun hat. Gleichzeitig luden sie die USA dazu ein, gemeinsame Ermittlungen zu tätigen.
Am 7. Januar 2015 wiederholte der FBI-Chef James Comey an einer IKT-Sicherheitskonferenz in New York, dass die US-Geheimdienstbehörden davon ausgehen würden, dass die Angriffe aus Nordkorea ausgeführt wurden.[20] Genauere Angaben lieferte er jedoch nicht. Das FBI soll aber gravierende Fehler entdeckt haben, welche die Hacker gemacht hätten. Die Gruppe «Guardians of Peace» hatte diverse Meldungen auf ihrem Facebook-Konto gepostet und soll beim Login nordkoreanische IP-Adressen verwendet haben.[21] Nachdem sie diesen Fehler entdeckt hätten, sei der Zugriff über Computer anderer Länder geleitet worden, um die Spuren zu verschleiern.
Daneben gab es aber auch immer wieder Stimmen, dass Nordkorea nicht oder nicht der einzige Akteur war, der hinter diesem Angriff stecke. Einige Experten vermuteten Ex-Sony-Mitarbeiter hinter dem Angriff. So wurde spekuliert, dass ein im Mai 2014 entlassener Mitarbeiter mit dem Angriff in Verbindung stehe.[22]

Die USA haben ihre Sanktionen gegen Nordkorea im Zuge des Angriffs auf Sony Pictures Entertainment verschärft. Strafmassnahmen gegen zehn Vertreter der Regierung in Pyongyang sowie gegen drei Organisationen und Unternehmen wurden verhängt.

Als Reaktion auf die wiederholten Cyber-Angriffe gegen US-Unternehmen und US-Regierung wollen die USA eine neue Behörde mit der Bezeichnung «Cyber Threat Intelligence Integration Center» aufbauen. Diese soll Informationen aus verschiedenen Quellen kanalisieren und analysieren.

Dieser Vorfall zeigt, dass es im Cyberbereich sehr schwierig ist, bei mutmasslich staatlichen Angriffen die Täterschaft schlüssig zu beweisen. Auf der einen Seite gibt es - im Gegensatz zu konventionellen Angriffen - viele Möglichkeiten, den Ursprung eines Angriffs zu verschleiern und auch falsche Fährten zu legen. Auf der anderen Seite dürfte die Vorstellung, dass bei staatlichen Angriffen ausschliesslich Verwaltungsangestellte hinter den Tastaturen sitzen, zu kurz greifen. Der Übergang zwischen staatlichen Angriffen, von Staaten in Auftrag gegebenen Angriffen bis hin zu staatlich geduldeten Angriffen dürfte fliessend sein. Im besten Fall findet man so Hacker, die einem Land zugeordnet werden können. Der Beweis, dass der Staat dahinter steckt, ist aber damit noch lange nicht erbracht und müsste vor Ort geführt werden. Vor Ort durchgeführte Untersuchungen sind aber typischerweise in einem solchen Fall nicht möglich.
Vielfach geht deshalb der Beweis über die Motivation der Angriffe. Findet man keinen monetären Hintergrund, wird schnell von einem professionellen, staatlichen Angriff

[19] MELANI Halbjahresbericht 2010/2, Kapitel 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=de (Stand: 28. Februar 2015).
[20] http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (Stand: 28. Februar 2015).
[21] http://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html?ref=technology&_r=3 (Stand: 28. Februar 2015).
[22] http://blog.norsecorp.com/2014/12/29/ex-employee-five-others-fingered-in-sony-hack/ (Stand: 28. Februar 2015).

gesprochen. Nicht erst seit dem Verkauf von Steuer-CDs sind auch Freischaffende unterwegs, welche Daten in Eigenregie stehlen, um sie anschliessend Staaten anzubieten. Die Struktur des Cyber-Untergrund-Marktes ist sicherlich zu komplex, als dass diese einfache Formel für alle Fälle anwendbar ist. Auch im vorliegenden Fall ist denkbar, dass es sich um mehrere Akteure handelte, welche alle ihren Teil zum Fallkomplex beitrugen.

4.2 Angriffe gegen Industrieanlagen

Industrieanlagen werden zunehmend vernetzt. Dies birgt neben einfacherer Fernkontrolle und –wartung aber auch ein erhöhtes Risiko von unbefugten Zugriffen und Manipulationen. Neben strategisch agierenden staatlichen Akteuren, die sich allenfalls nicht zuletzt aus militärischen Gründen für solche Anlagen interessieren, sind mittlerweile auch viele Sicherheitsexperten und Hobbyhacker auf diesen Trend aufmerksam geworden. Am 31. Kongress des Chaos Computer Club im Dezember 2014 waren *SCADA*- und industrielle Kontrollsysteme entsprechend ebenfalls Thema.[23] Mittlerweile gibt es Simulationen von Steuersystemen, wie sie beispielsweise in Chemiewerken verbaut sind, an denen Hacking-Fähigkeiten ausprobiert werden können. Zudem sind *Exploit-Kits* verfügbar, die spezifisch für die Erkennung und Ausnützung von Sicherheitslücken bei industriellen Anlagen programmiert wurden.

In Deutschland hat sich gemäss einem im Dezember 2014 veröffentlichten Berichts des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI)[24] ein gezielter Angriff auf ein Stahlwerk ereignet, welcher zu Schäden an einem Hochofen geführt hat. Die Angreifer hätten durch *Spear-Phishing* und ausgefeiltes *Social Engineering* Zugang zum Büronetzwerk des Unternehmens erlangt und sich von dort sukzessive bis in die Produktionsnetze vorgearbeitet. In der Folge führten Ausfälle einzelner Steuerungskomponenten oder ganzer Anlagen dazu, dass ein Hochofen nicht geregelt heruntergefahren werden konnte und die Einrichtung massiv beschädigt wurde. Laut Einschätzung des BSI kannten sich die Angreifer nicht nur im Bereich der klassischen IKT-Sicherheit sehr gut aus, sondern hatten auch detailliertes Fachwissen zu den eingesetzten Industriesteuerungen und Produktionsprozessen. Der Bericht des BSI hält sich nüchtern an die Fakten und äussert sich nicht zu einer möglichen Täterschaft.

Die Motivation der Urheber von reinen Sabotage-Aktionen sind nicht sehr vielfältig: Entweder versucht ein konkurrierendes Unternehmen sich einen Vorteil zu verschaffen, ein unzufriedener (ehemaliger) Mitarbeiter will seinem Arbeitgeber eins auswischen und nützt sein Insider-Wissen dazu aus, oder es handelt sich um Akteure, die herausfinden oder beweisen möchten, was alles möglich ist. Dass vorliegend ein fremder Staat die Stahlproduktion in Deutschland sabotieren wollte, erscheint demgegenüber kaum realistisch. Das Potenzial von Cyber-Sabotage wird jedoch zunehmend in Militärstrategien und Kriegsszenarien eingeplant.

Die Möglichkeit zu Sabotage bietet nicht zuletzt auch eine Gelegenheit für Kriminelle, den Betreiber einer Anlage zu erpressen.[25] Dies ist insbesondere dort erfolgsversprechend, wo eine Anlage auf die Verbindung zu anderen Netzwerken und Systemen angewiesen ist und nicht einfach bei einer solchen Drohung kurzfristig isoliert werden kann. Daneben ist gleichwohl denkbar, dass eine Schadsoftware eingeschleust wird, welche unabhängig von Internet-Konnektivität zu einem bestimmten Zeitpunkt aktiv wird. In einem solchen Fall wäre

[23] https://events.ccc.de/congress/2014/wiki/

[24] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf

[25] Siehe auch Kapitel 5.3 des aktuellen Halbjahresberichts.

die Gefahr selbst durch Abkoppelung des Systems vom Netz nicht gebannt, sondern die Schadsoftware müsste gefunden und unschädlich gemacht werden. Dies kann je nach Komplexität des Systems herausfordernd sein, wenn man nicht genau weiss, wonach man suchen muss.

Es ist wichtig, bei der Vernetzung von physischen Systemen den Sicherheitsaspekt mit einzubeziehen. Die gängigsten Angriffsvektoren bei Kontrollsystemen sind das Büronetzwerk, *Wechseldatenträger* und unzureichend abgesicherte Fernzugänge. Abhilfe schaffen können hier die strenge Segmentierung der Netzwerke (Kontrollsysteme vom Büronetzwerk abschirmen und wenn Datenaustausch notwendig ist, diesen gut kontrollieren), die Verwendung von dedizierten Wechseldatenträgern inklusive regelmässige Prüfung derselben sowie die Absicherung von Fernzugängen durch starke Authentifizierungsmethoden und verschlüsselte Datenübertragung. Siehe dazu auch die MELANI-Checkliste «Massnahmen zum Schutz von Industriellen Kontrollsystemen (ICS)».[26]

4.3 Angriffe gegen Energie- und Ölsektor

Im August 2014 wurde bekannt, dass in Norwegen rund 300 Firmen im Energie- und Ölsektor angegriffen wurden. Die Angreifer waren mit ihren *Social Engineering*-Methoden zumindest teilweise erfolgreich: Gemäss Aussagen der norwegischen Sicherheitsbehörden hätten die Angreifer in einem ersten Schritt durch Recherchen Schlüsselfunktionen und entsprechendes Personal in den Unternehmen identifiziert, um diesen dann massgeschneiderte, legitim anmutende E-Mails mit Schadsoftware im Anhang zu senden. Das Öffnen eines solchen Anhangs installierte einen *Exploit-Kit*, der das System nach Schwachstellen absuchte und gegebenenfalls eine hochspezialisierte Spionagesoftware nachlud. Auf diese Weise sollten Geschäftsgeheimnisse ausgekundschaftet, sowie Zugangsdaten zu weiteren Systemen erlangt werden.

Energieunternehmen – insbesondere im Bereich der Öl- und Gasversorgung – sind schon seit längerer Zeit einem erhöhten Druck von Cyber-Angriffen ausgesetzt.[27] Dies mag mit der politischen, wohl aber eher der wirtschaftlichen Bedeutung dieses Sektors zusammenhängen. Einige Akteure versuchen, sich mit Hilfe des durch Spionage gewonnenen Informationsvorsprungs einen Vorteil gegenüber Konkurrenten zu sichern – seien diese nun staatlich oder privat. Andere versuchen gezielt, den Betrieb von Energieunternehmen zu sabotieren, um dann von deren Produktionsausfall oder Aktienkursschwankungen direkt zu profitieren. Schliesslich sei auch auf die nach wie vor (militär-) strategische Bedeutung der fossilen Energieträger – insbesondere für die Treibstoffversorgung – hingewiesen, die staatliche Akteure auf Angriffs- wie auch Verteidigungsebene auf den Plan ruft.

[26] http://www.melani.admin.ch/dienstleistungen/00132/01557/index.html?lang=de (Stand: 28. Februar 2015)

[27] MELANI Halbjahresbericht 2014/1, Kapitel 4.3: http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=de (Stand: 28. Februar 2015).

4.4 Bezahlterminals (Point of Sales) im Visier von Angreifern

Die Problematik der Angriffe auf Bezahlterminals *(Point of Sales)* wie beispielsweise gegen die amerikanische Ladenkette Target wurde schon in einem früheren Halbjahresbericht thematisiert.[28] Diese Angriffe zielen hauptsächlich darauf ab, an Kreditkartendaten zu gelangen, wobei gleichzeitig teilweise auch andere Personendaten gestohlen werden. Ende 2014 machte ein weiterer Fall dieser Art Schlagzeilen, als die amerikanische Baumarktkette Home Depot am 14. September 2014 bekanntgab, zwischen April und September 2014 Opfer eines Diebstahls von rund 56 Millionen Kreditkartendaten geworden zu sein. Mit der Meldung bestätigten sich die Informationen in Fachzeitschriften und Blogs in den Wochen zuvor. Die angewendete Methode erinnert stark an den Fall Target: Nach der Kompromittierung bei einem Lieferanten des Unternehmens wurde bei den Verkaufspunkten eine Malware des Typs «Ram Scraper» installiert.

Bezahlterminals wurden aber noch auf andere Weise kompromittiert. Bereits im Juli 2014 hat die Sicherheitsfirma FireEye auf die Malware «BrutPOS» aufmerksam gemacht, die es auf Remote Access Zugänge abgesehen hat, welche mit einem schwachen Passwort geschützt sind. Laut FireEye soll BrutPOS solche Schwachstellen über ein Botnetz identifizieren, das über 5500 infizierte Maschinen umfasst. Dabei werden Standardpasswörter wie «admin», «client» oder «password» ausprobiert. Sind die Täter einmal im System, versuchen sie via Ram Scraping an die Kreditkartendaten zu gelangen.

Wie diese Beispiele zeigen, sind Bezahlterminals weiterhin im Visier krimineller Gruppierungen. Es wird viel investiert, um diese Systeme, die sehr lukrative Ziele darstellen, zu knacken. Die ergaunerten Kreditkartendaten werden auf Untergrund-Foren verkauft und dann für Einkäufe benutzt, ohne dass die Besitzer etwas merken. Bislang wurden hauptsächlich US-Unternehmen angegriffen, weil diese in Anbetracht ihres Geschäftsvolumens und des oft ungenügenden Schutzes für die Kriminellen am Interessantesten sind. In den USA ist das Kreditkartensystem mit Chip und Pin anders als in Europa nämlich verhältnismässig wenig verbreitet[29]. Obwohl auch Angriffe gegen Dienstleister gegen das Chip- und Pin-System denkbar sind, ist der Aufwand für einen Angriff höher und somit das Kosten-Nutzen-Verhältnis für die Angreifer schlechter.

Insbesondere der Fall BrutPOS macht deutlich, wie wichtig es ist, alle Fernzugänge zu Geräten oder Systemen zu schützen. MELANI hat schon mehrfach auf die Risiken hingewiesen, mit denen der zunehmende Trend zur Fernsteuerung von physischen Prozessen im Industrie- und im Haushaltsbereich über das Netz behaftet ist. Ungeachtet der Unterschiede, die diese Geräte und Systeme aufweisen, gelten in Bezug auf den Fernzugriff doch für alle grundsätzlich die gleichen Sicherheitsregeln.

[28] MELANI Halbjahresbericht 2013/2, Kapitel 4.4, Angriffe bei Target-Verkaufsstellen: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 28. Februar 2015).

[29] Bei den Kreditkarten, die in den USA und vielen weiteren Ländern im Umlauf sind, werden die Daten auf Magnetstreifen gespeichert.

4.5 Spionage – Ausgewählte Fälle des zweiten Halbjahres 2014

Regin – Indizien für Urheberschaft gefunden

Auch im letzten Halbjahr wurden wiederum einige Spionagevorfälle aufgedeckt. Am meisten Aufsehen erregten dabei die Berichte von Symantec, Kaspersky und F-Secure im November 2014 über eine Schadsoftware mit dem Namen «Regin».[30] Mehrere Jahre lang soll der Trojaner Regin unbemerkt diverse Opfer ausspioniert haben, darunter Ziele in Russland und Saudi Arabien, aber auch in westeuropäischen Ländern wie Belgien oder Österreich. Regin ermögliche seinen Programmierern Überwachung und Ausspähung im grossen Stil und soll gegen Regierungsorganisationen, Infrastrukturbetreiber, Unternehmen, Forschungsstellen sowie gegen Privatpersonen eingesetzt worden sein. Besonders erwähnenswert sind die Spionageaktivitäten bei Telekommunikationsanbietern: Jeder vierte Fall soll Telekommunikationsanbieter betroffen haben. Symantec hat diesbezüglich eine Funktion entdeckt, welche auf GSM-Base Stationen ausgerichtet ist. Kaspersky, welche die Schadsoftware ebenfalls untersuchte, doppelte nach, dass Regin im April 2008 GSM-Zugangsdaten von Administratoren gestohlen habe, mit denen man GSM-Netzwerke im Mittleren Osten hätte manipulieren können. Kurz darauf wurde auf der Website «The Intercept» berichtet, dass Regin unter anderem auch gegen das Telekommunikationsunternehmen Belgacom eingesetzt worden sein soll. Hinter diesem Angriff wurde aufgrund der veröffentlichten Dokumente des Whistleblowers Edward Snowden der britische Geheimdienst GCHQ vermutet. Im Januar 2015 wurden von Kaspersky weitere Beweise über die Täterschaft publiziert. Das Sicherheitsunternehmen fand Ähnlichkeiten zwischen Regin und einer Schadsoftware namens Qwerty. Der *Quellcode* von Qwerty wurde zuvor von der deutschen Zeitung «Der Spiegel» veröffentlicht und stammt aus dem Fundus der Dokumente von Edward Snowden. Bei Qwerty soll es sich um das *Keylogger*-Modul von Regin handeln.[31]

Ende 2014 wurde in einigen Zeitungen berichtet, dass auf einem Computer im deutschen Bundeskanzleramt die Schadsoftware Regin entdeckt worden sei. Es wurde spekuliert, dass beim Einstecken eines USB-Sticks im Kanzleramt der Virenscanner angeschlagen habe. Zuvor soll der USB auf einem privaten Gerät eines Mitarbeitenden verwendet worden sein. Eine Regierungssprecherin erklärte anschliessend, dass das Netz nicht infiziert worden sei.[32]

Red October reloaded?

Das Sicherheitsunternehmen Bluecoat hat im Dezember 2014 einen gezielten Spionageangriff entdeckt, der sich unter anderem dadurch auszeichnet, dass er auch Mobilgeräte mit Android oder iOS sowie Blackberry-Geräte infizieren kann. iPhones und iPads konnten allerdings nur infiziert werden, wenn bei diesen zuvor die Nutzungseinschränkungen ausgeschaltet wurden (*Jailbreak*). Zudem verwendet die

---

30 http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance (Stand: 28. Februar 2015).
http://www.kaspersky.com/about/news/virus/2014/Regin-a-malicious-platform-capable-of-spying-on-GSM-networks (Stand: 28. Februar 2015).

31 http://www.spiegel.de/netzwelt/netzpolitik/nsa-trojaner-kaspersky-enttarnt-regin-a-1015222.html (Stand: 28. Februar 2015).
http://www.spiegel.de/netzwelt/netzpolitik/snowden-dokumente-wie-die-nsa-digitale-kriege-vorbereitet-a-1013521.html (Stand: 28. Februar 2015).

32 http://www.heise.de/newsticker/meldung/Offenbar-Spionagesoftware-Regin-auf-Rechner-im-Kanzleramt-entdeckt-2507042.html (Stand: 28. Februar 2015).

Schadsoftware einen unüblichen Command&Control-Mechanismus. Die infizierten Computer kommunizieren via https und WebDav über einen gleichen Server des Schwedischen *Cloud*dienstes namens CloudMe. Die Schadsoftware, welche den Namen «Inception» trägt, wurde vor allem eingesetzt, um Führungskräfte in den Bereichen Öl und Gas, Finanz, Militär, Behörden und Botschaften auszuspionieren. Verteilt wurde die Schadsoftware über *Spear Phishing*-E-Mails mit trojanisierten Dokumenten. Kaspersky, welche ebenfalls Informationen zu dieser Spionagekampagne unter dem Namen Cloud Atlas[33] veröffentlichte, vermutet, dass es sich um eine neue Version der Schadsoftware «Red October» handeln könnte. Nach der Veröffentlichung des Kaspersky Berichtes über Red October im Januar 2013 wurde das Spionagenetzwerk sofort heruntergefahren. Bei Cloud Atlas wurden nun Spuren entdeckt, welche der Red October Kampagne ähneln. So ist nicht nur der Opferkreis ähnlich, bei einem *Spear-Phishing*-Angriff wurde auch ein ähnliches Dokument verwendet.

Cloud Atlas ist ein typisches Beispiel für einen *Advanced Persistent Threat (APT).* Neben dem Fokus Professionalität (Advanced) liegt in diesem Fall der Schwerpunkt vor allem auf dem Begriff Persistent. Wird ein gezielter Spionageangriff aufgedeckt und dementsprechend auch unterbunden, ist damit zu rechnen, dass die Angreifer entweder an einem anderen Ort bereits im System sind oder dies eher früher als später wieder versuchen werden.

Sandworm - Angriffe gegen NATO und ukrainische Regierungsmitglieder

Das Sicherheitsunternehmen iSight machte Ende Oktober 2014 eine gezielte Spionagekampagne gegen Regierungsmitglieder der Ukraine, der europäischen Union, sowie der NATO publik, bei der unter anderem eine Windows-Sicherheitslücke ausgenutzt wurde.[34] Weitere Angriffsziele waren eine französische Telekommunikationsfirma sowie ein polnisches Unternehmen im Energiesektor. Die Ausnutzung der bis zu diesem Zeitpunkt unbekannten Sicherheitslücke in Microsoft Windows und Windows Server (CVE-2014-4114), lässt auf einen sehr professionellen Akteur schliessen.[35]

Attacken gegen ukrainische Regierungsangestellte sollen seit Sommer 2014 anhalten und mittels gezielt an Opfer gesendete PowerPoint-Dokumente, welche oben erwähnte Lücke ausnützten, durchgeführt worden sein. Die ersten Aktivitäten der Gruppe konnte iSight aber bereits auf das Jahr 2009 zurückführen. Obwohl die Interessen wie auch gewisse Sprachsteine auf einen russischen Ursprung hindeuten, konnte auch in diesem Fall die Urheberschaft nicht restlos geklärt werden.

Angeblich diverse Angriffe auf israelische Firmen

Ende Juli 2014 publizierte der unabhängige Journalist Brian Krebs, dass in den Jahren 2011 und 2012 diverse Male Pläne für den Raketenschild «Iron Dome» der Israelischen Armee gestohlen worden sein sollen.[36] Krebs beruft sich auf die US-amerikanische Sicherheitsfirma CyberESI, welche die Kampagne untersucht hat. Betroffen sein sollen die drei Israelischen Waffenhersteller Rafael Advanced Defense Systems, Israel Aerospace Industries und die Elisra Group. Als Angreifer wird die als APT1 oder PLA-Einheit 61398 bekannte Gruppe aus China vermutet. Die betroffenen Firmen haben die Angriffe nicht bestätigt.

---

33 https://securelist.com/blog/research/68083/cloud-atlas-redoctober-apt-is-back-in-style/ (Stand: 28. Februar 2015)

34 http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/ (Stand: 28. Februar 2015)

35 http://www.isightpartners.com/2014/10/cve-2014-4114/ (Stand: 28. Februar 2015).

36 http://krebsonsecurity.com/2014/07/hackers-plundered-israeli-defense-firms-that-built-iron-dome-missile-defense-system/ (Stand: 28. Februar 2015).

US-Atombehörde

Auf die US Atombehörde Nuclear Regulatory Commission soll es in den letzten drei Jahren mindestens drei erfolgreiche Hackerangriffe gegeben haben. Ein staatlicher Hintergrund wurde vermutet. Angeblich konnten die Spuren in zwei Fällen auf ein bestimmtes Land zurückgeführt werden, welches jedoch nicht öffentlich genannt wurde. Laut Nextgov[37] wurden die üblichen Angriffsmethoden wie *Phishing* und *Spear-Phishing* eingesetzt. Interessant ist, dass beim dritten Angriff das E-Mail Konto eines Mitarbeiters benutzt wurde, um eine kompromittierte PDF-Datei an weitere 16 Mitarbeiter zu senden. Für den Empfänger wird es damit umso schwieriger, eine bösartige E-Mail zu erkennen. Dies ist eine übliche Vorgehensweise, um via einfacher zu infiltrierende Zwischenstationen auf «interessante» Computer innerhalb einer Firma zu gelangen.

Gezielte Spionageangriffe sind keine Einzelereignisse. Es besteht ein ständiges Interesse und demzufolge ein ständiger Druck auf sensible Daten. Schwierig ist in allen Fällen die Bestimmung der Urheberschaft. Auch wenn bei den meisten *Advanced Persistent Threats (APT)* aufgrund der Opfer eine staatliche Urheberschaft vermutet wird, sind die Übergänge zwischen staatlichen und kriminellen Hackern vielfach fliessend.

Amnesty International stellt Detektionstool zur Erkennung von Überwachungssoftware zur Verfügung

Im November 2014 stellte Amnesty International ein Programm zur Verfügung, das staatliche Überwachungssoftware wie beispielsweise «FinFisher» erkennen soll. Mit Hilfe von FinFisher können beispielsweise Skype-Gespräche abgehört, E-Mails abgefangen und sogar die Kamera von Geräten ferngesteuert werden. Die Software wird unter anderem auch gegen Menschenrechtsaktivisten und Dissidenten in Ländern mit autoritären Regimes und eingeschränkter Meinungsäusserungsfreiheit eingesetzt. Unklar ist, wie umfangreich das Tool die verschiedenen Typen von Überwachungssoftware erkennen kann.[38]

4.6 Spionageangriff auf Dienstreise

Bereits seit Längerem wird davor gewarnt, bei der Verwendung von öffentlichen *WLAN*-Anschlüssen besonders vorsichtig zu sein. Das bekannteste Beispiel eines Angriffs in einem Funknetzwerk war bislang unter dem Namen «Firesheep» bekannt: Hierbei war es möglich, in einem ungesicherten, d. h. offenen Netzwerk (zum Beispiel in einem Internetcafé) mit wenig Aufwand ein *Session Hijacking* durchzuführen und damit Nutzerdaten wie Passwörter auszuspähen. Allerdings funktioniert dieser Angriff nur, wenn Daten unverschlüsselt ohne sicheres Übertragungsprotokoll https übermittelt werden. Der Sicherheitsdienstleister Kaspersky publizierte nun im November 2014 unter dem Namen Darkhotel einen Report über eine Gruppe von Angreifern, die gezielte Angriffe in Funknetzwerken von Hotels verübten, welche über diese bislang bekannten Angriffe hinausgehen.[39] Seit vier Jahren sollen gezielt hochrangige Manager auf deren Geschäftsreisen in Asien angegriffen worden sein. Dies legt nahe, dass es sich um Wirtschaftsspionage handelt. Daneben wurden allerdings auch zufällig Personen angegriffen. Der Angriff wird gestartet, sobald die Zielperson nach dem Einchecken ihren Computer benutzt und sich ins hoteleigene WLAN

[37] http://www.nextgov.com/cybersecurity/2014/08/exclusive-nuke-regulator-hacked-suspected-foreign-powers/91643/ (Stand: 28. Februar 2015).

[38] http://www.amnesty.ch/de/themen/weitere/meinungsaeusserungsfreiheit/dok/2014/detekt-software-zum-aufdecken-von-ueberwachung (Stand: 28. Februar 2015).

[39] http://blog.kaspersky.com/darkhotel-apt/ (Stand: 28. Februar 2015).

einloggen will. Dazu wird ihr eine Benachrichtigung gesendet, dass ein bestimmtes Programm ein Update benötige. Als Beispiele werden die Google-Toolbar, Adobe Flash oder Windows Messenger genannt. Logischerweise handelt es sich bei diesem Update um eine Schadsoftware, welche Daten vom Computer stehlen kann.

Andererseits warnte der US-Secret Service im letzten Halbjahr vor *Keyloggern* auf Computern, die in Hotels oder an Flughäfen der Öffentlichkeit zur Verfügung gestellt werden. In einer Mitteilung an das Gastgewerbe wurde dieses aufgefordert, Computer zu überprüfen, welche der Öffentlichkeit zur Verfügung gestellt werden. Auslöser dieses Communiqués war die Verhaftung von Verdächtigen, welche Computer in verschiedenen grossen Hotel-Businesscentern in Dallas/Fort Worth mit *Keyloggern* versehen haben sollen.[40]

Beim Verwenden von öffentlichen WLANs sollte immer eine gesunde Portion Vorsicht mitsurfen. Es dürfen keine Programme, die während dem Einwahlversuch ins Funknetzwerk, installiert werden sollen, akzeptiert werden. Zusätzlich muss genauestens darauf geachtet werden, dass der Computer auf dem neuesten Stand ist. Ansonsten reichen bereits so genannte *Webseiteninfektionen* um einen Computer zu infizieren. Personen, welche unterwegs geschäftskritische Daten bearbeiten müssen, sollten sich überlegen, hierzu nicht besser über die persönliche Hotspot-Funktion des Mobilfunktelefons und dessen *Roaming*-Funktion zu gehen. Auch wenn die Benutzung dieser Funktion grosse Kosten verursacht.

An öffentlichen Computern sollte man keine Dienste verwenden, welche Login oder Passwort verlangen. Diese Dienstleistung der Hotels sollte nur dazu genutzt werden, sich beispielsweise über die Sehenswürdigkeiten der Stadt zu informieren.

4.7 Datendiebstähle im grossen Stil

Auch in diesem Jahr machten wieder etliche Datendiebstähle Schlagzeilen. Ein Fall sticht dabei besonders heraus – nicht aufgrund der Anzahl gestohlener Datensätze, sondern die Art und Weise des Diebstahls: Im August meldete einer der grössten Krankenhausbetreiber der USA, dass 4.5 Millionen Patientendaten gestohlen worden waren. Gerade im Gesundheitsbereich erwarten die Patienten eine besonders hohe Sensibilität bezüglich Datenschutz. Auf der anderen Seite schreitet die Digitalisierung auch im Gesundheitsbereich besonders schnell voran. Was auf der einen Seite Vorteile hat und auch zur Verminderung von Fehlern beiträgt, birgt auf der anderen Seite gewisse Gefahren.

Im konkreten Fall hatte das «Community Health System», einer der grössten Krankenhausbetreiber der USA, im August 2014 einen Einbruch in seine Computersysteme gemeldet. Beim Einbruch sollen Daten von bis zu 4,5 Millionen Patienten entwendet worden sein, die in den vergangenen fünf Jahren in einem Krankenhaus des Unternehmens behandelt worden waren. Für die Tat hat die Sicherheitsfirma Mandiant chinesische Hacker verantwortlich gemacht. Gestohlen wurden nach Angaben des Unternehmens, welches 206 Krankenhäuser in 29 Bundesstaaten verwaltet, unter anderem Namen, Adressen, Telefonnummern, Geburtsdaten und Sozialversicherungsnummern. Es konnte weder eruiert werden, was das genaue Ziel der Angreifer war, noch ob hinter dem Angriff auch staatliche Akteure gestanden haben.

Ein weiterer Fokus bei Datendiebstählen bildet der Finanzsektor. Schlagzeilen machte diesbezüglich ein Angriff auf die US-Grossbank J.P. Morgan. Daten von rund 76 Millionen Haushalten und sieben Millionen Unternehmen sollen bei diesem Angriff, der Mitte August

[40] http://krebsonsecurity.com/2014/07/beware-keyloggers-at-hotel-business-centers/ (Stand: 28. Februar 2015).

2014 entdeckt wurde, kopiert worden sein. Demnach wurden Kundendaten wie Namen, Adressen, Telefonnummern und E-Mail-Adressen von den Servern des Kreditinstituts entwendet. Für den Diebstahl heiklerer Daten wie Kontonummern, Geburtsdaten, Passwörtern oder Sozialversicherungsnummern, gab es bislang keine Hinweise. Der Angriffsvektor wurde nach Angaben von J.P. Morgan identifiziert: Ausgenutzt wurde eine Sicherheitslücke, welche schon seit Juni 2014 bestanden habe. Um was für eine Sicherheitslücke es sich genau gehandelt hat, ist nicht bekannt. Gefährdete Konten wurden deaktiviert und die Passwörter aller IKT-Techniker geändert. Nach Ansicht der Behörden deuten verschiedene Hinweise auf hochprofessionelle Hacker hin, die möglicherweise in Russland zu finden sind. Ob die Motivation hinter den Angriffen in den US-Sanktionen gegen Russland zu suchen ist, wurde zwar vermutet, aber nicht bewiesen.

Eine etwas andere Ankündigung machte die Firma Holdsecurity Anfang August 2014. Dabei soll ein Datendiebstahl durch russische Hacker von bislang noch nie dagewesenem Ausmass von 1.2 Milliarden Login/Passwortkombinationen aufgedeckt worden sein. Die Zugangsdaten sollen von über 420‘000 Webseiten stammen, darunter auch einige von bekannten Firmen. Speziell an diesem Fall war, dass die Firma im gleichen Atemzug auch gerade einen neuen Service ankündigte, der es ermöglichte zu erkennen, ob man von diesem und weiteren Datendiebstählen betroffen ist.[41]

Vielfach stellen Sicherheitsfirmen solche Daten den zuständigen staatlichen Stellen oder den betroffenen Providern zur Verfügung, damit die Opfer informiert werden können. Die Frage nach dem verantwortungsvollen Umgang solcher Informationen wird in Zukunft immer wichtiger werden und wird in Kapitel 5.5 ausführlich behandelt.

4.8 iCloud gehackt – Bilder von Prominenten im Internet

Ende August 2014 wurden gestohlene Nacktbilder von Prominenten veröffentlicht, zuerst auf der Bildveröffentlichungsplattform «4chan», danach auf diversen weiteren Plattformen. Rasch wurde klar, dass die Fotos aus verschiedenen iCloud-Konten stammten. iCloud ist der Cloud-Dienst von Apple. Zur Methode, wie die Diebe an die Fotos gelangten, wurden verschiedene Spekulationen veröffentlicht, wobei die meisten ein Problem in der Software zur Lokalisierung verlorener oder gestohlener Geräte «Find My iPhone» vermuteten. Mehreren Expertenberichten zufolge soll das Programm ungenügend vor Bruteforce-Angriffen geschützt gewesen sein, da eine grosse Anzahl Passwörter für den Zugriff durchprobiert werden konnte, ohne dass die Versuche eingeschränkt wurden. Eine klassische Sicherheitsmassnahme gegen Bruteforce-Attacken besteht darin, den Dienst nach einer bestimmten Anzahl gescheiterter Zugriffsversuche zu sperren. Bei «Find My iPhone» war die Vorkehrung damals nicht integriert, wurde aber kurz nach dem Vorfall implementiert. Verstärkt wurden die Spekulationen durch einen Proof of Concept (PoC) dieser Methode, der auf der Seite GitHub kurz vor dem Vorfall veröffentlicht wurde. Apple hat diese Hypothese einer Schwachstelle auf «Find My iPhone» oder auf einem anderen ihrer Dienste dementiert. In einer offiziellen Erklärung hat das Unternehmen die Ursache einem gezielten Angriff auf Benutzernamen, Passwörter und Sicherheitsfragen der betreffenden Konten zugeschrieben.[42]

Dieser Fall ist nicht der einzige, bei dem im letzten Halbjahr die Sicherheit der Cloud-Speicherdienste diskutiert wurde. Auch der Cloud-Speicherdienst «Dropbox» geriet

[41] http://www.forbes.com/sites/kashmirhill/2014/08/05/huge-password-breach-shady-antics/ (Stand: 28. Februar 2015).

[42] http://www.bbc.com/news/technology-29039294 (Stand: 28. Februar 2015).

beispielsweise ins Visier von Kriminellen, als im Oktober 2014 Zugriffsdaten auf «Pastebin», einer Webanwendung auf der jedermann Texte veröffentlichen kann, gepostet wurden. Diese Fälle rücken einmal mehr die Problematik der Sicherheit von Cloudspeicherdaten in den Mittelpunkt. Ist ein Konto einmal kompromittiert und sind die Zugangsdaten gestohlen, erhalten die Angreifer einen Fernzugriff auf eine Vielzahl persönlicher Daten. In Bezug auf iCloud- oder ähnlichen Diensten ist zudem vielen Nutzern gar nicht bewusst, dass ihre Fotos automatisch mit einem Cloud-Konto synchronisiert werden. Dieser Parameter kann standardmässig aktiviert sein. Die Nutzer sollten deshalb diese Einstellung bei jeder App überprüfen und die automatische Synchronisierung deaktivieren, wenn dieser Dienst nicht erwünscht ist.

Wollen Nutzer die Cloud für Fotos verwenden, gelten die gleichen Sicherheitsregeln wie für alle anderen Online-Konten. Das heisst, dass für jeden Dienst ein eigenes, komplexes Passwort, das Sonderzeichen enthält, verwendet werden muss. MELANI empfiehlt ausserdem, wo möglich die Zweifaktorauthentifizierung zu verwenden.[43] Schliesslich zeigt der Fall der Prominenten-Nacktfotos im Internet einmalmehr sehr deutlich, dass das beste Mittel, um den Diebstahl von kompromittierendem Material zu verhindern, immer noch darin besteht, dieses gar nicht oder zumindest nicht auf einem vernetzten Datenträger zu speichern.

4.9 Wieder gravierende Sicherheitslücken in zentralen Software-Komponenten

Im letzten Halbjahr gab es nebst einer Vielzahl von Lücken in Anwendungen wie Flash, Acrobat, Java und Office auch schwerwiegende Verwundbarkeiten in Betriebssystemen und Basisbibliotheken.

Poodle

Nach der Heartbleed-Lücke war *SSL*, ein Netzwerkprotokoll zur sicheren Datenübertragung, erneut von einer gravierenden Schwachstelle betroffen. Die Poodle[44] benannte Lücke, ist jedoch im Gegensatz zu Heartbleed kein Programmierfehler, sondern eine Lücke im Protokoll selber, genauer in der Version 3 von *SSL*. Die Lücke liegt darin begründet, dass *SSL/TLS* zuerst die Integrität der Daten schützt und erst danach verschlüsselt. Da die Verschlüsselung meist in Blöcken fester Länge vorgenommen wird, werden am Schluss jeder Zeile genau so viel Zeichen angehängt, damit der Block die passende Länge erhält. Das letzte *Byte* enthält dabei die Zahl der Anzahl aufgefüllten Zeichen. Genau in diesem Punkt liegt das Problem. Die Füllzeichen und das letzte Byte werden zwar mitverschlüsselt, jedoch wird deren Integrität nicht überprüft. Ein Angreifer kann daher unbemerkt beliebige Zeichen einfüllen, auch Teile der Zeile, welche man beispielsweise entschlüsselt haben möchte. Voraussetzung dafür ist, dass der Angreifer eine «*Man in the Middle*»-Attacke durchführen kann, sprich in die Mitte einer Verbindung sitzen kann. Dies ist beispielsweise in einem offenen Funknetzwerk möglich.[45]

---

[43] Eine Liste mit Websites, welche eine Zweifaktor Authentifizierung zulassen, ist verfügbar auf: https://twofactorauth.org (Stand: 28. Februar 2015).

[44] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566 (Stand: 28. Februar 2015).

[45] Eine ausführliche Beschreibung der Funktionsweise der Poodle Schwachstelle finden Sie hier: https://nakedsecurity.sophos.com/2014/10/16/poodle-attack-takes-bytes-out-of-your-data-heres-what-to-do/ (Stand: 28. Februar 2015).

Aus diesem Grund empfiehlt MELANI Webseitenbetreibern, SSLv3 komplett zu deaktivieren und soweit möglich nur die Verschlüsselungsprotokolle TLS 1.1 oder TLS 1.2 zu verwenden. In den meisten aktuellen Browsern ist die Unterstützung von SSLv3 mittlerweile entfernt worden.

Shellshock

Von der Shellshock[46]-Lücke waren unter anderem fast alle Unix-artigen Betriebssysteme betroffen. Durch die Sicherheitslücke kann ungeprüft Programmcode ausgeführt werden. Entdeckt wurde diese in der oft verwendeten Software «Bash Shell». Nebst Servern und Clients betrifft dies auch Geräte wie *Router* oder *Sicherheitsgateways*. Es wurden mehrere Lücken gefunden, die laufend korrigiert worden sind. Die Lücke entsteht aufgrund der Tatsache, dass übergebene Umgebungsvariablen nicht korrekt überprüft werden, so dass dieser Variable zusätzlicher Code, und damit auch schädlicher Code, übergeben werden kann.

```
$ env x='() { :;}; echo VULNERABLE' bash -c ""
```

Es gibt verschiedene Angriffsszenarien:

- HTTP / Webserver via CGI Schnittstelle
- SSH
- DHCP
- SIP
- und viele weitere

Nach Bekanntwerden der Lücke hat MELANI einen massiven Anstieg an Scan- und Exploit-Versuchen festgestellt, die mittlerweile zwar etwas zurückgegangen sind, aber nach wie vor anhalten.

Kerberos

Eine weitere Lücke (MS14-068[47]), die insbesondere für Firmen gravierende Folgen haben kann, liegt in der Kerberos-Implementierung in Microsofts *Active Directory,* dem Verzeichnisdienst von Microsoft. Ein Benutzer mit einem nicht-privilegierten Konto kann sich unter Zuhilfenahme dieser Schwachstelle die höchsten Berechtigungen (Administratorenrechte) verschaffen und so ein komplettes *Active Directory* übernehmen. Das bedeutet, dass prinzipiell ein einziger, erfolgreicher Angriff (z. B. mit einer Malware) auf einen Benutzer in einer Firma dazu führen kann, dass das gesamte *Active Directory* und damit sämtliche Windows-Ressourcen vom Angreifer kontrolliert werden können. Nebst dem Schliessen der Lücke empfiehlt MELANI deshalb, Notfallpläne für eine Wiederherstellung des *Active Directories* zu erstellen und regelmässig zu testen. Zusätzlich sollten die hoch privilegierten Accounts speziell abgesichert werden.

[46] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271 sowie die weiteren CVE Nummern 2014-7169, 2014-7186, 2014-7187, 2014-6277, 2014-6278 (Stand: 28. Februar 2015).

[47] https://technet.microsoft.com/en-us/library/security/ms14-068.aspx (Stand: 28. Februar 2015).

SChannel

Eine weitere Sicherheitslücke in Windows (MS14-066)[48] betraf Secure Channel. SChannel ist Microsofts Implementierung der SSL/TLS-Verschlüsselung, welche es ermöglicht, sensitive Kommunikation über ein öffentliches Netzwerk verschlüsselt auszutauschen. Gemäss Angaben von Microsoft konnte ein Angreifer die Sicherheitslücke mit Hilfe speziell präparierter Netzwerkpakete ausnutzen und beliebigen Schadcode auf einem betroffenen System ausführen. Cisco erwähnte in einem Blogeintrag ausserdem mehrere *Pufferüberläufe*.[49] Dieser Patch bereitete Microsoft grosse Schwierigkeiten, so dass mehrmals nachgebessert werden musste, um unerwünschte Nebenwirkungen wie Performance-Probleme wieder in den Griff zu bekommen.

Generell beobachtet MELANI, dass im Internetbereich oft verwendete Software wie Flash, Acrobat und Java stark im Fokus der Angreifer sind. Sofort nach Erscheinen eines Patches werden diese von Angreifern auf die behobene Verwundbarkeit hin analysiert und ein entsprechender Angriff in ihre *Exploit-Kits* eingebaut, mit denen dann die noch nicht gepatchten Geräte angegriffen werden können. Dies geschieht in der Regel innerhalb weniger Tage. Einzelne *Exploit-Kits* verfügen sogar über bisher nicht bekannte Lücken (*0-day Exploits*), die sie für Angriffe auf Endgeräte einsetzen. Aus diesem Grund empfiehlt MELANI Heimbenutzern und KMUs, die Updates automatisch einzuspielen und grösseren Firmen, ein sehr schnelles Patch-Management mit klar definierten und prioritär gehandhabten Prozessen zu implementieren.

4.10 Schwachstelle in Mobilfunkstandard

Experten rund um den Berliner IKT-Spezialisten, Karsten Nohl, machten im Dezember 2014 eine Sicherheitslücke im Mobilfunknetz publik, über die es möglich ist, die als sicher geltende Verschlüsselung im *UMTS*-Netz zu umgehen und so zum Beispiel *SMS* abzufangen. Das von der Sicherheitslücke betroffene SS7 (Signalling System 7)-Protokoll wird dazu verwendet, Informationen zwischen den einzelnen Telekom-Providern auszutauschen, um beispielsweise SMS oder Anrufe über verschiedene Netze hinweg transportieren zu können. Das Protokoll selbst stammt aus den 80er-Jahren und ist somit relativ alt. Obschon das Protokoll zweimal erneuert worden ist, um neue Funktionen einzubauen, ist das Hauptproblem einer fehlenden Authentisierung zwischen den Partnern nie gelöst worden. Als es nur wenige grosse Provider gab, die sich zudem gegenseitig kannten und vertrauten, war dies kein grosses Problem. Heute spielen jedoch im weltweiten Mobilfunkmarkt eine Vielzahl von unterschiedlich vertrauenswürdigen Providern mit, von denen einige den Zugang zu SS7 noch an weitere Firmen weiterverkaufen.

Konkret eröffnen sich mit der Sicherheitslücke einem Angreifer folgende verschiedene Angriffsvektoren:

- Tracking eines Gerätes:
  Jedes Gerät ist bei der nächst gelegenen Funkzelle angemeldet. Um die momentan benutzte Funkzelle einer zu überwachenden Person zu finden, muss der Angreifer lediglich dessen Telefonnummer kennen. Der Ort der verwendeten Funkzelle kann dann in einer Datenbank nachgeschaut werden. In dicht besiedelten Gebieten mit vielen Funkzellen kann ein Benutzer dadurch ziemlich genau lokalisiert werden. Mit der Kenntnis der *International Mobile Subscriber Identity (IMSI)* und des Global Title

[48] https://technet.microsoft.com/en-us/library/security/MS14-066 (Stand: 28. Februar 2015).
[49] http://blogs.cisco.com/security/talos/ms-tuesday-nov-2014 (Stand: 28. Februar 2015).

(Adresse, die für das Routing der Anrufe verwendet wird) gibt es weitere Angriffsvektoren, die auch funktionieren, wenn der Provider gewisse Protokollfunktionen sperrt.

- Abfangen und Abhören von Gesprächen:
  Befindet sich ein Gerät in einem fremden Netz, gibt es bestimmte Ereignisse, bei denen eine Abfrage beim «Heimatprovider» gemacht wird. Überschreibt ein Angreifer nun die Daten, wohin sich das Gerät wenden soll, mit seiner Adresse, wird sich das Gerät in einem solchen Fall im Netz des Angreifers melden. So kann er die Anrufe über sich umleiten und abhören. Er spielt dabei *Man-in-the-Middle*, ohne dass das Opfer dies bemerkt.

- Abfangen von mTANs:
  Die Aktualisierung der Information, wie ein bestimmtes Gerät aktuell zu erreichen ist, wird ebenfalls nicht authentisiert und bietet somit Angriffspunkte. So kann ein Angreifer vorgeben, dass sich sein Opfer in seinem Netzwerk befindet, indem er dies dem Heimprovider meldet. Dieser wird dann Anrufe oder SMS in dieses Netz weiterleiten. So kann ein Angreifer beispielsweise einen mTAN, SMS-Authentisierung beim E-Banking, abfangen.

- Abfangen der IMSI:
  Um einem Gerät mitzuteilen, dass es einen Anruf erhält, wird eine temporär zugeteilte ID verwendet (TIMSI), die unverschlüsselt über das Netz gesendet wird. Wird diese abgefangen, kann mit dieser temporären ID die eigentliche ID des Geräts (IMSI) von der Vermittlungsstelle verlangt werden. Kennt ein Angreifer die IMSI hat dieser weitere Möglichkeiten, wie beispielsweise die tatsächliche Telefonnummer in Erfahrung zu bringen oder den Schlüssel, für die aktuelle Verschlüsselung der Verbindung zu erfragen.

Diese Angriffsszenarien sind relativ einfach durchzuführen und werden mit hoher Wahrscheinlichkeit auch von Akteuren aus dem staatlichen wie auch dem parastaatlichen Umfeld angewendet. Aus diesem Grund sollten sehr heikle Informationen, die beispielsweise Firmengeheimnisse betreffen, nicht via Mobile ausgetauscht werden, insbesondere, wenn sich einer der Gesprächspartner im Ausland befindet und ein Roaming macht. MELANI steht im Gespräch mit den Mobilfunkprovidern in der Schweiz, um diese Schwachstellen soweit als möglich abzusichern.[50]

4.11 Schwachstellen - auch in MacOSX

MELANI stellt fest, dass Lücken im Betriebssystem MacOSX immer stärker ausgenutzt werden, sowohl für gezielte Angriffe als auch für das generelle Verteilen von Schadsoftware. Dabei werden – analog zu Windows – oft Verwundbarkeiten in Java oder in Browser-Plugins wie Acrobat Reader oder Flash ausgenutzt.

In den vergangenen Monaten haben zwei Malware-Familien grössere Aufmerksamkeit erregt:

[50] Quelle: Tobias Engel, http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf (Stand: 28. Februar 2015).

- iWorm[51] ist eine *Backdoor*, die zu verschiedenen Zwecken verwendet werden kann. Interessant ist die Art und Weise wie die Schadsoftware Informationen erhält, mit welchen Steuerungsservern sie kommunizieren soll. Sie verwendet hierzu von den Angreifern veröffentlichte Nachrichten auf der Social News Site «Reddit», um die URL der aktuellen Command and Control Server zu generieren. Die Verteilung von iWorm geschieht primär über kompromittierte Raubkopien, die über die Software Bittorrent verteilt werden.[52]

- Wirelurker[53] ist eine Schadsoftware, welche sowohl eine MacOSX- wie auch eine iOS-Komponente enthält. Ist die Malware auf einem OSX Gerät aktiv, wartet sie, bis ein iOS Gerät (iPhone, iPad) via *USB* verbunden wird. Die Schadsoftware liest dann verschiedene Informationen aus (Telefonnummer, iTunesStore Daten, usw.) und sendet diese an einen Command and Control-Server. Da die USB-Verbindung eine vertrauenswürdige Verbindung ist, kann die Schadsoftware sich so als normale App ausgeben. Dazu benötigt die App ein Enterprise Zertifikat und ein Provisioning-Profil, um die Malware gültig zu signieren. Dieser Vorgang löst eine Nachfrage beim Benutzer aus. Akzeptiert dieser, wird die Malware installiert. Bei Geräten mit einem *Jailbreak* wird dieser Schritt übersprungen. Mit solchen Enterprise-Zertifikaten können Firmen eigene Anwendungen auf ihren iOS Geräten installieren. Die Malware für OSX wird dabei ähnlich wie iWorm über Raubkopien von kommerzieller Software verteilt.

Nebst Angriffen mit Malware stellt MELANI ebenfalls fest, dass iTunes- und iCloud-Accounts immer stärker das Ziel von *Phishing* Angriffen werden. Dabei werden - ganz klassisch - Benutzer mit echt aussehenden E-Mails dazu verleitet, ihre Logindaten auf einem Server der Angreifer einzugeben, die so Zugriff auf die Accounts erhalten.

In der Geräteschnittstelle Thunderbolt gibt es zudem eine insbesondere auch für gezielte Angriffe sehr ernstzunehmende Lücke[54]. Diese Lücke ermöglicht es einem Angreifer, der physischen Zugriff auf ein Gerät hat, direkt die EFI-*Firmware* des Mac zu modifizieren, indem er ein modifiziertes Thunderbolt-Gerät wie z. B. einen Gigabit-Adapter ansteckt. Eine so verteilte Malware ist sehr schwierig zu entdecken, da sie sich vor dem Betriebssystem lädt und sich somit auch komplett vor diesem und einem allfälligen Virenscanner verbergen kann. Apple hat einen Patch veröffentlicht, der die Lücke zumindest für OSX Yosemite (10.10.2) schliesst.

5 Tendenzen / Ausblick

5.1 Informationen sammeln und austauschen im Zeitalter von Big Data

Bereits zu Ende des letzten Jahrtausends, setzte sich der Glaube durch, dass Daten und Informationen das neue Gold seien. Unzählige Internet Start-Ups schossen aus dem Boden, mit Business-Plänen, auf deren Habenseite oftmals einfach lapidar auf eben das Sammeln

51 http://news.drweb.com/show/?i=5977&lng=en (Stand: 28. Februar 2015).

52 http://www.thesafemac.com/iworm-method-of-infection-found/ (Stand: 28. Februar 2015).

53 https://www.paloaltonetworks.com/resources/research/unit42-wirelurker-a-new-era-in-ios-and-os-x-malware.html (Stand: 28. Februar 2015).

54 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4498 (Stand: 28. Februar 2015).

von Daten und Informationen verwiesen wurde. Die Frage, wie genau dies in Geld verwandelt werden soll, wurde dabei geflissentlich übersehen. Entsprechend rüde war denn auch das Erwachen an den Märkten, als neben vielen gehorteten Informationen und Daten in erster Linie rote Zahlen präsentiert wurden. Die Pionierstimmung verwandelte sich in einen veritablen Kater und die Dot-Com-Blase zerplatzte im März 2000 fast so schnell, wie sie sich aufgebaut hatte. Rund fünfzehn Jahre später haben vor allem die Internetunternehmen offensichtlich ihre Hausaufgaben gemacht. Entweder wird nun für Leistungen im Internet bezahlt oder aber kostenlose Angebote lassen sich im Gegenzug für die Angabe persönlicher Daten nutzen. Seien es die in diesem Bereich aktiven Facebook, Google oder Twitter - die Sammlung von Daten und Informationen und deren Auswertung führen unterdessen zu einem ansehnlichen monetären Gegenwert.

Die Ansammlung von Daten und Informationen erlaubt es denn erst, positiv verstanden, Profile auszuwerten, individualisierte Werbung zu schalten und Kunden immer besser zurechtgeschneiderte Dienste anzubieten. In ihrer eigenen Interpretation dieser Tatsache und, als rational zur Erbringung des Produktes Sicherheit, weisen denn auch gewisse Nachrichtendienste gerne darauf hin, dass zum Auffinden einer (meist terroristischen) Nadel am Anfang ein Heuhaufen stehen muss. Selbst auf internationaler und zwischenstaatlicher Ebene werden die Informations- und Datenerhebung sowie der Austausch dieser Sammlungen vermehrt zum Wundermittel beispielsweise im Kampf gegen Auswüchse im Bereich der Steuerhinterziehung oder zum effizienten, internationalen Abgleich von Fahndungslisten eingesetzt. Dabei ist zumindest bei der staatlichen Erhebung und Auswertung von Personendaten, sowie deren Austausch im internationalen Umfeld davon auszugehen, dass der rechtliche Rahmen entsprechend eng gesteckt ist, was bei privaten Sammlungen nicht der Fall sein wird.

In jedem Fall zeigen sich aber bei dieser Entwicklung zwei grundsätzliche Problemfelder. Zum einen sind zentrale Daten- und Informationssammlungen auch ein zentraler Angriffspunkt. Es ist nicht überraschend, dass bei Angriffen auf Unternehmen die Zahl der erbeuteten Daten kontinuierlich steigt. Waren ein paar Tausend gestohlene E-Mail-Adressen vor zehn Jahren noch eine Zeitungsmeldung wert, müssten es heute wahrscheinlich schon ein paar Millionen sein und das zugehörige Passwort ebenfalls gerade beinhalten. Die Tatsache, dass dabei an bestimmten Orten Daten entwendet werden können, die der eigentliche Datenhalter wohl kaum jemals diesem Unternehmen direkt zur Verfügung gestellt hat, sollte dabei nicht erstaunen, da ein reger Handel mit solchen Informationen und Daten geschieht. Dies in den meisten Fällen mit der impliziten Erlaubnis des Datenhalters, der irgendwann einmal einen AGB oder eine Datenschutzbestimmung akzeptierte um endlich sein ersehntes Buch bestellen oder ein Social Media-Konto erstellen zu können. Dabei gilt gerade bei der technischen Sicherheit von Datenhaltungen verstärkt das Prinzip des schwächsten Glieds. Jede noch so genaue Abmachung, jedes noch so strikte Vertragswerk, wie Daten erhoben und technisch ausgetauscht werden, kann letztendlich nicht davor schützen, dass diese am Ende in die falschen Hände geraten. Dies gilt nicht nur für private, sondern auch für staatliche Institutionen, wie beispielsweise der Fall des gehackten Schengener Informationssystems (SIS) in Dänemark zeigt.[55]

Zum anderen stellt sich die Frage nach dem Verwendungszweck dieser immensen Datenflut. Im privatwirtschaftlichen Umfeld kann davon ausgegangen werden, dass in erster Linie marktwirtschaftlichen Überlegungen eine Rolle spielen. Durch die Weitergabe von Daten erhofft sich der Datenhalter einen Vorteil. So kann es absolut Sinn machen, Daten an Dritte zur Verfügung zu stellen, um die besten darauf passenden Angebote zu erhalten. Ein

[55] MELANI Halbjahresbericht 2013/2, Kapitel 3.6: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 28. Februar 2015).

anderer Punkt ist es, wenn diese Daten auch noch gerade den Sicherheitsbehörden eines Landes übergeben werden müssen. Im zwischenstaatlichen Bereich ist die Frage des Verwendungszweckes ebenfalls zu stellen. Die Vereinfachung der Bekämpfung von Steuerhinterziehung durch einen automatisierten Informationsaustausch mag durchaus sinnvoll sein. Wie diese Informationen dann in den Empfängerstaaten genau verwendet werden, muss dringend ebenfalls geregelt sein. Die Schweiz hat sich beispielsweise stark im Rahmen der OECD dafür eingesetzt, dass der Fokus beim automatischen Informationsaustausch nicht nur auf der Art der zu erhebenden Daten liegt, sondern auch auf deren Verwendungsbereich fokussiert wird. Eine Garantie, dass dies vom Partnerstaat auch eingehalten wird, kann es dabei offensichtlich nicht geben, wie ein Entscheid des Bundesverwaltungsgerichtes von 2014 gezeigt hat:[56]

Bei diesem Fall, bei dem es um einen Verdacht auf Insiderhandel eines Schweizer Bürgers ging, ersuchten die pakistanischen Behörden die Schweizerische Finanzmarktaufsicht (FINMA) im Sommer 2012 um Amtshilfe. Die FINMA gab der Amtshilfe statt, worauf der beschuldigte Schweizer beim Bundesverwaltungsgericht eine Beschwerde einreichte, die er im Wesentlichen damit begründete, die zuständige pakistanische Behörde könne die Einhaltung des Spezialitäts- und Vertraulichkeitsprinzips nicht gewährleisten. Interne E-Mails der pakistanischen Behörde sowie die interne Kommunikation zwischen ihr und der FINMA sind dann auch der pakistanischen Presse zugespielt worden und belegten die Amtsgeheimnisverletzung. Die FINMA sistierte darauf umgehend die Amtshilfeverfahren.

Mit der Entwicklung hin zu Big Data und all ihren Vor- und Nachteilen, drängen sich neben Fragen zur technischen Sicherheit und der Verantwortung der Betreiber solcher Datensammlungen auch grundlegende Fragen zur Due Dilligence im Bereich der Verwertung und Verwendung dieser Daten auf. Gefordert sind hier in erster Linie alle, die ihre Daten freiwillig zur Verfügung stellen und sich darüber im Klaren sein müssen, was genau mit ihren Daten passiert. Gefordert sind aber auch staatliche Behörden, gerade wenn es darum geht dafür zu sorgen, dass Daten, die rechtmässig erhoben und weitergeleitet werden, auch wirklich nur dort zur Anwendung gelangen, wofür sie ursprünglich gedacht waren. Die Entwicklung griffiger Audit- und Kontrollprozesse, um dies zu gewährleisten, wird dabei wohl eine der grössten Herausforderungen in naher Zukunft.

5.2 Die totale Vernetzung! Smart und Sicher?

Das Internet – das Netz der Netze – verbindet IKT-Systeme und ermöglicht den Transfer von Informationen und Daten. Es besteht jedoch nicht nur aus dem World Wide Web, das den Menschen Webseiten anzeigt. Über das Internet, diese globale Telekommunikationsinfrastruktur, können Menschen auch mit Maschinen kommunizieren und ihnen Anweisungen geben, welche dann Auswirkungen auf die physische Welt haben. Mittlerweile können das Maschinen auch untereinander – aber natürlich (bislang) nur, sofern sie einmal entsprechend programmiert worden sind. Kommunizierende Kleinstcomputer nehmen in diversen Lebensbereichen zunehmend bedeutende Rollen ein. Die Erfassung von Zuständen durch Sensoren und die Ausführung von Befehlen zur Erzielung eines Effekts durch Aktuatoren ermöglichen weitgehende Automatisierung von Abläufen zur Unterstützung der Menschen nicht mehr nur in der virtuellen, sondern gleichwohl auch in der physischen Welt.

56 http://www.bvger.ch/publiws/download;jsessionid=F01EA73D27D15FF364A9203975D0B648?decisionId=f736b6ed-38ba-4d10-bf8f-c0312d05030f (Stand: 28. Februar 2015).

Im Rahmen dieser Entwicklung entstanden Begriffe wie internet of things (Internet der Dinge oder der «Intelligenten Gegenstände»), pervasive computing (Rechnerdurchdringung), ubiquious computing (Rechnerallgegenwart), wearable computing (tragbare Datenerfassung und –verarbeitung, zum Teil direkt in Kleidungs- oder Schmuckstücke eingearbeitet), und nicht nur das Telefon ist mittlerweile „smart", sondern auch Autos (smart car / smart drive), Wohnräume (smart home) respektive ganze Gebäude (smart building) und nicht zuletzt auch Industrieanlagen (smart factory / smart manufacturing)[57] können Daten erheben, erhalten, verarbeiten, versenden, aus ihnen Befehle ableiten und Aktionen ausführen.

Der Erfolg, der dem Internet zugrunde liegenden Technologie und das Bedürfnis nach Interoperabilität führen dazu, dass immer mehr Anwendungen, welche Datenaustausch bedingen, auf Internet-Protokollen basieren. So werden beispielsweise in Smart Homes die Sensoren und Aktuatoren der Hausautomation in das heimische WLAN eingebunden, da diese Infrastruktur ja bereits besteht und die Bewohner ihr Heim sowieso mit dem Smartphone bedienen können möchten, welches ja ebenfalls schon mit dem Heimnetzwerk verbunden ist. Dies führt zwangsläufig zu Schnittstellen zwischen dem weltweiten Internet, welches auf den globalen Austausch von Daten und Informationen ausgelegt ist, und lokalen Geräten wie dem Temperatursensor der Heizung oder der vernetzten Glühlampe in der heimischen Stube. Mag es noch sinnvoll sein, Heizung und Boiler in der Ferienwohnung vor der Ankunft per Smartphone starten zu können, dürfte das Ein- und Ausschalten von Licht in Abwesenheit bereits bedeutend weniger Anwendung finden und das Hoch- und Runterfahren einer Heimkinoleinwand kaum je benötigt werden. Obwohl die Steuerung der Wohnumgebung über das Internet nur in den seltensten Fällen von den Herstellern dieser Systeme als Feature angeboten wird (sondern auf der Nutzung aus dem Heimnetzwerk heraus basiert), sind entsprechende Möglichkeiten jeweils zumindest hypothetisch ausnutzbar.[58] All diese Systeme sind jedoch nicht nur gegen Angriffe aus dem Internet, sondern auch vor lokalen Bedrohungen zu schützen. Neben dem WLAN können ebenfalls andere drahtlose Schnittstellen (z. B. *Bluetooth* oder *NFC*) als Einfallstor dienen, wenn sie nicht korrekt implementiert und abgesichert sind.

Auf Benutzerseite wird das Smartphone immer mehr zum zentralen Identifikations- und Bediengerät sowie zur Datensammel- und –auswertstelle. Dies lässt sich unter Anderem anhand der aktuell in Mode kommenden Gesundheits-Apps eindrücklich beobachten. Der Sicherheit des Smartphones ist entsprechend aus Datenschutz- und Sicherheitsgründen gebührend Rechnung zu tragen. Daneben sollte auch überlegt werden, wie man im Fall einer Kompromittierung oder bei Verlust des Smartphones vorgehen kann, um Missbrauch durch Unberechtigte verhindern und die gewohnten Funktionen und Daten verlustfrei auf ein Ersatzgerät übertragen kann.

Bei allen Annehmlichkeiten, die uns eine «smarte» Umgebung beschert, darf nicht vergessen werden, die Datenerhebung, -verarbeitung und -speicherung jeweils kritisch zu hinterfragen sowie sich zu überlegen, ob und wie man auch ohne die Unterstützung der kleinen vernetzten Helferlein zurecht kommen würde, respektive ob man zum Beispiel bei einer intelligenten Toilette[59], die nicht mehr spülen will, bis man das WC-Papier nachgefüllt hat oder weil die Internetverbindung unterbrochen ist, auch noch manuell durchgreifen kann. Schliesslich ist die Steuerung von physischen Prozessen durch vernetzte Informatikmittel

---

[57] Die deutsche Bundesregierung spricht in ihrer Hightech-Strategie von „*Industrie 4.0*", gemäss welcher die Informatisierung der Fertigungstechnik vorangetrieben werden soll: http://www.bmbf.de/de/9072.php

[58] Vergleiche hierzu MELANI Halbjahresbericht 2013/2, Kapitel 5.5: Angriffe auf Heimrouter: http://www.melani.admin.ch/dokumentation/00123/00124/01565/index.html?lang=de (Stand: 28. Februar 2015).

[59] http://www.heise.de/newsticker/meldung/31C3-Hacker-nehmen-vernetzte-Toiletten-ins-Visier-2507287.html (Stand: 28. Februar 2015).

auch unter dem Aspekt von böswilligen Manipulationen durch Unberechtigte zu sehen, welche zwar vielleicht nur aus Schadenfreude Unannehmlichkeiten bescheren, jedoch gleichwohl ernsthafte Nachteile zufügen können oder ihre Kontrolle über Geräte und Dienste ausnützen, um die rechtmässigen Nutzer damit zu erpressen.

5.3 Erpressung – verschiedene Formen

Ein Delikt hat in den letzten Jahren im Cyberbereich besonders stark zugenommen: die Erpressung. Immer häufiger versuchen Kriminelle - meist unter zu Hilfenahme von Daten, die dem Opfer gehören - Geld zu erpressen.

Eine der beobachteten Vorgehensweise besteht darin, sensible Daten zu stehlen und mit deren Veröffentlichung zu drohen. Falls das Opfer das verlangte Geld nicht überweist, werden die Daten anschliessend publik gemacht. Im letzten Halbjahr wurden verschiedene solche Fälle gegen Unternehmen bekannt. Dazu gehören insbesondere die Machenschaften der Hackergruppe «Rex Mundi», die auf diese Weise verschiedene Opfer erpresst hat. Bei dieser Erpressungsart wird zuerst über eine *SQL-Injection* auf der Firmenwebseite auf eine Datenbank zugegriffen, welche meist Angaben zu Kunden und deren Korrespondenz enthält. Anschliessend nehmen die Angreifer mit dem jeweiligen Unternehmen Kontakt auf: Wenn dieses nicht die geforderte Summe bezahlt, werden die gestohlenen Daten veröffentlicht. Es wurden noch weitere raffinierte erpresserische Angriffe auf sensible Daten bekannt. Man denke hier vor allem an die Attacke gegen Sony Pictures (siehe Kapitel 4.1). In solchen Fällen hoffen die Täter, dass eine Firma bereit ist aufgrund eines drohenden Imageschadens durch das Bekanntwerden des Falles, ein Lösegeld zu zahlen.

Neben den bereits erwähnten Fällen wird ein weiterer noch stärkerer Trend beobachtet: *Ransomware,* welche es vor allem auf die Datenverfügbarkeit von Privatnutzern abgesehen hat. Während die ersten Fälle erpresserischer Schadsoftware einfach den PC des Opfers blockierten, verschlüsseln Cryptolocker und seine Varianten mittlerweile die Daten auf dem infizierten Gerät. Solche Trojaner erweisen sich als unerschöpfliche Geldquelle für die Erpresser. Viele Experten gehen von einem Anhalten dieses Trends aus. Der Erfolg hängt hauptsächlich von der Bereitschaft der Opfer ab, die geforderte Summe zu bezahlen, um wieder auf ihre Daten oder ihren Rechner zugreifen zu können. Diese Bereitschaft scheint laut einer Studie der Universität Kent[60] gross zu sein. Demnach sollen 40 Prozent der Cryptolocker-Opfer bereit sein, ein Lösegeld zu zahlen. Für die Kriminellen zählt in diesem Fall nicht der Wert der Daten an sich und die Möglichkeit, diese zu verkaufen oder zu verwenden. Es zählt vielmehr der Wert, den die Daten für das Opfer haben und was dieses gewillt ist zu zahlen, um die Daten wiederzubekommen. Es ist deshalb gefährlich, wenn Nutzer den Schutz ihrer persönlichen Daten vernachlässigen, weil sie denken, dass diese wertlos für potenzielle Angreifer sind. Sobald Daten einen (wenn auch nur einen emotionalen) Wert für einen Nutzer haben, sind sie auch wertvoll für potenzielle Erpresser.

Solche Erpressermethoden könnten in Zukunft auch auf weitere Gebiete übergreifen. Ein Beispiel, das kürzlich Schlagzeilen gemacht hat, sind gezielte Angriffe auf schlecht gesicherte Websites. Die Datenbank einer Website wird dabei verschlüsselt und dann vom Administrator Geld verlangt, damit er wieder auf die Datenbanken zugreifen kann.[61] Auch das Internet der Dinge (Internet of Things) und die zunehmende Vernetzung von Geräten könnten Erpressern zahllose weitere Angriffsmöglichkeiten bieten. Jedes Tool oder Gerät, das mit dem Netz verbunden ist, ist ein potenzielles Ziel. Es sind Szenarien denkbar, bei

---

60 http://www.kent.ac.uk/news/science/528/cryptolocker-victims-pay-out (Stand: 28. Februar 2015).

61 https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html (as at 28 February 2015)

denen Haushaltsgeräte gesperrt und für deren Freigabe Geld verlangt wird. Trotz der Möglichkeit, das Gerät selber zu entsperren oder auf manuellen Betrieb umzuschalten, könnten viele Opfer wegen der entstehenden Umstände oder mangelnder Kenntnisse bereit sein zu zahlen, vor allem wenn es sich um kleinere Beträge handelt.

Die bekannten aber auch die denkbaren Beispiele machen deutlich, dass Angriffe unter dem Aspekt der Verfügbarkeit nicht vernachlässigt werden dürfen. Im klassischen Modell «Vertraulichkeit - Integrität - Verfügbarkeit» wird der Schwerpunkt in Bezug auf aktuelle Angriffe und auch der Evaluation neuer Produkte oder Dienste tendenziell auf die Vertraulichkeit gelegt. Es sollte aber nicht vergessen werden, dass Angriffe auf die Verfügbarkeit von Daten oder Diensten für Täter sehr lukrativ sein können. Dieser Aspekt ist mit der sich im Umlauf befindlichen Ransomware bereits heute aktuell und wird mit der zunehmenden Vernetzung von Diensten und Geräten noch an Bedeutung gewinnen.

5.4 Satellitennavigation im Flugverkehr

Das *Global Positioning System (GPS)* ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung. Über einen Empfänger lassen sich somit jederzeit die Längen- und Breitengrade der eigenen Position ermitteln. GPS-Empfänger sind heutzutage nahezu überall zu finden: In Smartphones, Digitalkameras bis hin zu Autos. Zunehmend wird Satellitennavigation aber auch in sicherheitsrelevanten Anwendungen implementiert.

Ein Beispiel, das an dieser Stelle thematisiert werden soll, ist die Zivilluftfahrt. So hat das Bundesamt für Zivilluftfahrt (BAZL) am 17. Februar 2011 auf der Nordpiste 14 des Flughafens Zürich zum ersten Mal in der Schweiz ein Verfahren für einen satellitengestützten Anflug genehmigt.[62] Am 18. Oktober 2012 führte die Flughafenbetreiberin zusammen mit der Flugsicherungsgesellschaft Skyguide einen satellitengestützten Abflug auf der Piste 34 ein. Erstmals wurde damit in der Schweiz ein Abflugverfahren angewendet, bei dem für den Kurvenflug ein Radius definiert wird. Am 14. Oktober 2014 landete die erste Swiss Maschine mittels satellitengestütztem Präzisionsanflugsystems am Flughafen Zürich.[63] Eine entsprechend flächendeckende technische Aufrüstung der Flugzeuge wird aber jedoch wohl erst stattfinden, wenn das satellitengestützte Anflugverfahren an einem Grossteil der angeflogenen Flughäfen angewendet werden kann.

Bei dieser Entwicklung darf nicht vergessen werden, dass die Satellitennavigation nicht spezifisch für den Einsatz in der Zivilluftfahrt entwickelt worden ist und auch absichtlich oder unabsichtlich leicht gestört werden kann. Erinnert sei an die Störungen des GPS-Systems am Flughafen von Newark. Nach mehreren Monaten dauernden Nachforschungen zeigte sich, dass die Störungen durch einen Lastwagenfahrer verursacht wurden. Dieser rastete regelmässig neben dem Flughafen und hatte «*GPS-Jammer*» bei sich.

Die bestehenden GPS-Signale können deshalb nicht alleine verwendet werden. Es ist ein zusätzliches System notwendig, welches die Integrität der Daten überwacht und dazu dient, Ausfälle und Manipulationen zu erkennen. Ausserdem ist die Exaktheit des normalen GPS-Signals mit einer spezifizierten Genauigkeit von 9 bis 17 Meter für Präzisionsanflüge zu

---

62 MELANI Halbjahresbericht 2011/1, Kapitel 5.4: http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de (Stand: 28. Februar 2015).

63 http://www.swiss.com/corporate/de/medien/newsroom/medienmitteilungen/medienmitteilung20141015 (Stand: 28. Februar 2015).

ungenau. Äussere Einflüsse wie ionisierende Strahlung aber auch die Wechsel der GPS-Satelliten können zu Abweichungen führen. Das in Zürich zusätzlich eingesetzte Verfahren nennt sich Ground Based Augmentation System (GBAS) oder zu Deutsch bodengestütztes Ergänzungssystem. Mit vier Referenzstationen bei denen die absolute Position genau bekannt ist, kann eine sogenannte Differential Korrektur zum «normalen GPS» errechnet werden. Dies entspricht dem Fehler des aktuellen GPS-Signals. Diese Abweichung wird anschliessend per Funk an das Flugzeug gesendet.[64] Ein besonderes Augenmerk gilt dabei der Übermittlungssicherheit der Differential Korrektur insbesondere bezüglich deren Integrität.

Ein zusätzliches, in Europa für die Flugnavigation eingesetztes System ist der European Geostationary Navigation Overlay Service (EGNOS).[65] Auch hier wird anhand von in Europa verteilten Referenzpunkten die Genauigkeit erhöht und auch die Integrität des GPS-Signals überprüft. Sollte das GPS Systeme falsche Daten aussenden, wird dies innerhalb von 6 Sekunden erkannt und an den Piloten weitergeleitet. Die Differentialkorrektur wird hierbei über geostationäre Satelliten an die Flugzeuge gesendet. Das Signal wird auch über das Internet verteilt. Bestehende GPS Empfänger können das Signal empfangen und auswerten. Der Fehler beträgt so deutlich unter 10 Metern. EGNOS ist ein gemeinsames Projekt des ESA, der EU und der europäischen Flugsicherung Eurocontrol und dient als Vorstufe des europäischen Satellitennavigationssystems Galileo. Es ist im Gegensatz zu GBAS kostengünstiger, da keine zusätzliche Technik am Boden verbaut werden muss. Neben der höheren Präzision besteht der Unterschied zum GPS, welches durch nicht europäische Staaten betrieben wird, darin, dass dies unter der Kontrolle der oben genannten Betreiber steht und die Qualität des Signals permanent überwacht werden kann.

Bei EGNOS wird das Korrektursignal über einen geostationären Satelliten an die Flugzeuge versendet und ist öffentlich zu empfangen. EGNOS ist nichts anderes als eine Erweiterung und Verfeinerung des bestehenden GPS-Signals. Analog zu dem GPS Signal ist eine Manipulation zwar schwierig aber wie bei jedem technischen System nicht gänzlich ausgeschlossen. Die Sicherheit hängt von den einzelnen Komponenten und deren Produzenten ab. Sicherheit muss gerade in diesem Bereich gross geschrieben werden. Firmen, welche Komponenten für EGNOS liefern, müssen spezielle Sicherheitsanforderungen erfüllen. Schweizer Firmen, welche am Galileo und EGNOS Programm teilnehmen wollen, werden deshalb von Sicherheitsexperten des VBS überprüft.[66]

Moderne IKT-Systeme wecken immer neue Begehrlichkeiten auch in Bereichen, in denen die Sicherheit oberstes Gebot ist. Dabei geht es in vielen Fällen um die Modernisierung aber auch um den Einsatz von Systemen, die effizienter und ressourcenneutraler betrieben werden können. Der erwünschte Effizienzgewinn sollte jedoch in eine Risikobeurteilung einfliessen und mit Sicherheitsüberlegungen abgewogen werden. Im Gegensatz dazu können IKT-Systeme eine wertvolle Ergänzung zu den älteren Sicherheitssystemen bieten. Die Herausforderung für den Einsatz solcher Systeme liegt jedoch nicht nur in der Integrität der übermittelten Daten, sondern auch in der Verfügbarkeit der Systeme. Eine Störung des GPS Signals bedeutet, dass Flugzeuge, die sich im Anflug befinden, die Landung mit alternativ zur Verfügung stehenden Systemen fortsetzen müssen. Dies ist so lange kein

64 http://www.skyguide.ch/fileadmin/user_upload/publications/Factsheets/1201_Factsheet_Satellitennav_System_Verfahren_de.pdf (Stand: 28. Februar 2015).

65 http://www.esa.int/Our_Activities/Navigation/The_present_-_EGNOS/What_is_EGNOS (Stand: 28. Februar 2015).

66 https://www.news.admin.ch/message/index.html?lang=de&msg-id=53264 (Stand: 28. Februar 2015).

Problem, als dass sich die Landeregimes zwischen den zur Verfügung stehenden Systemen nicht unterscheiden oder alternative Systeme wie das Instrumentenlandesystem (ILS) noch zur Verfügung stehen. Bei flughafengebunden Landesystemen, würden sich Störungen analog dem ILS auf den Flughafen beschränken. Der Ausfall von EGNOS hätte allerdings Auswirkungen auf den gesamteuropäischen Flugverkehr.

5.5 Sicherheitslücken – Responsible Disclosure

Direkt oder indirekt sind die Internetnutzer dauernd irgendwelchen Sicherheitslücken ausgesetzt. Dem Durchschnittsnutzer bekannt sind vor allem Lücken in Microsoft-Produkten sowie Acrobat-Reader und Flash-Player. Ebenfalls für Schlagzeilen sorgen jeweils Schwachstellen, welche Sicherheitskomponenten respektive Verschlüsselungskomponenten betreffen. Bekanntestes Beispiel ist hier die Heartbleed *Vulnerability*, welche im letzten Halbjahresbericht thematisiert wurde. In der aktuellen Berichtsperiode sei auf die Poodle und Kerberos Lücke verwiesen (siehe hierzu Kapitel 4.9). Laut der von der Firma MITRE unterhaltenen Datenbank mit allen öffentlich bekannten Schwachstellen in Programmen, wurden im Jahr 2014 weltweit insgesamt 7945 Schwachstellen aufgenommen – so viele wie nie zuvor[67]. Die Palette von Schwachstellen ist aber noch sehr viel grösser und reicht von verwundbaren Webseiten bis hin zu fehlerhaften Konfigurationen, welche nicht in dieser Datenbank aufgeführt sind. Es ist davon auszugehen, dass in praktisch jeder eingesetzten Software irgendeine Lücke zu finden ist. Aufgrund dieser Entwicklung drängt sich zunehmend die Frage nach den Prozessen auf, die den Umgang mit gefundenen Sicherheitslücken regeln.

Beispielsweise wird von den meisten Internetnutzern angenommen, dass der Finder die Informationen den entsprechenden Firmen (kostenlos) zur Verfügung stellt, damit diese so schnell wie möglich ein Update zur Verfügung stellen können. Der Markt im Security Business ist allerdings hart umkämpft und der Umgang mit Informationen, die die Sicherheit betreffen, immer eine Gratwanderung. Da spielen jeweils verschiedene Interessen mit, natürlich auch finanzielle. Das Finden einer Lücke hat einen gewissen Wert, immerhin wird hier vom Finder eine Rolle übernommen, die eigentlich von der Herstellerfirma im Rahmen der Qualitätssicherung wahrgenommen werden sollte. Es ist davon auszugehen, dass diverse Firmen aktiv und gezielt Programme nach Sicherheitslücken absuchen, um daraus Profit zu schlagen. Ein Beispiel, dass diesbezüglich 2012 Schlagzeilen machte, war die maltesische Firma ReVuln, welche sich darauf spezialisiert hat, unbekannte Sicherheitslücken in SCADA-Produkten nicht an die Hersteller zu melden, sondern diese an Regierungen und andere «zahlende Kunden» zu verkaufen.[68] Gerade im Bereich von kritischen Infrastrukturen kann dies ein lohnendes Geschäft sein, da hier der Druck für fehlerloses Funktionieren besonders gross ist und Regierungen gezwungen sind, die Sicherheit dieser kritischen Systeme zu gewährleiten. Diese Kommerzialisierung birgt aber die Gefahr, dass zum Einen Sicherheitslücken aus Kostengründen nicht behoben werden und zum Anderen das Wissen um eine Lücke in die Hände von zahlenden Kriminellen gelangt. Aber auch das Kaufen von Schwachstellen durch Regierungen birgt Gefahren, welche nicht erst seit der Veröffentlichung der Snowden Dokumente bekannt sind. Bereits 2012 sagte Chaouki Bekrarder, CEO und Chefhacker der Firma VUPEN in einem Interview, dass sie gefundene Sicherheitslücken im Google Browser Chrome nicht für 1 Million Dollar

[67] http://cvedetails.com/browse-by-date.php (Stand: 28. Februar 2015).

[68] http://www.computerworld.com/article/2493333/malware-vulnerabilities/security-firm-finds-scada-software-flaws--won-t-report-them-to-vendors.html (Stand: 28. Februar 2015).

an Google verkaufen würden, sondern an dessen Kunden, spezifisch an NATO-Partner und NATO-Regierungen.[69]

Auf der anderen Seite werden gewisse Sicherheitslücken von den Herstellern nicht ernstgenommen, was den Finder der Lücke frustriert. Solange die Lücke nicht öffentlich bekannt ist, sehen gewisse Hersteller keinen Grund, diese zeitnah zu beheben. So gab es immer wieder Fälle, bei denen im Nachhinein bekannt wurde, dass der Hersteller bereits Monate vor ihrem öffentlichen Bekanntwerden von einer Lücke Kenntnis hatte, es jedoch versäumt hatte, sich in dieser Zeit erfolgreich um eine Lösung zu bemühen. Für den Finder bedeutet dies ein gewisses Frustrationspotential. Um den Druck zu erhöhen wird dann mit der Veröffentlichung der Lücke zu einem gewissen Zeitpunkt gedroht, was den Hersteller dann zwingt, schnell zu handeln. Im ungünstigsten Fall wird dann die Sicherheitslücke publiziert, ohne dass ein entsprechendes Update vorhanden ist.

Während das erste Problemfeld, wenn überhaupt, wohl nur mit staatlicher Regulierung beizukommen ist, ist das zweite Problemfeld durchaus lösbar. Das National Cyber Security Center in den Niederlanden hat beispielsweise einen Leitfaden publiziert, wie Melder und Betroffene mit Sicherheitslücken umgehen sollen. Das Security Center fungiert hierzu als Meldestelle, wo gefundene Schwachstellen gemeldet werden können. Der Melder wird dazu angehalten, die Informationen nicht zu veröffentlichen. Dafür wird ihm zugesichert, dass innerhalb von drei Arbeitstagen die Seriosität des Schwachstellenreports evaluiert wird und das erwartete Datum der Problemlösung genannt wird. Der Melder wird zudem über die aktuellen Fortschritte bei der Behebung des Problems informiert und bekommt die Lorbeeren bei der Veröffentlichung und mindestens ein T-Shirt als Dankeschön.[70]

[69] http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/ (Stand: 28. Februar 2015).

[70] https://www.ncsc.nl/english/current-topics/news/responsible-disclosure-guideline.html (Stand: 28. Februar 2015).

5.6 Politische Geschäfte

Geschäft	Nummer	Titel	Eingereicht von	Datum Einreichung	Rat	Amt	Stand Beratung & Link
Po	14.3739	Control by Design. Die Rechte auf Eigentum im Falle von unerwünschten Verbindungen verstärken	Schwaab Jean Christophe	17.09.2014	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143739
Po	14.3782	Richtlinien für den "digitalen Tod"	Schwaab Jean Christophe	24.09.2014	NR	EJPD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143782
Ip	14.3884	Absichten diverser Stromkonzerne, ihre Anteile an Swissgrid zu verkaufen	Killer Hans	25.09.2014	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20143884
Fr	14.5642	Internet-Dienstleistungen. Aufspaltung dominierender Konzerne bei Quasi-Monopolen	Glättli Balthasar	03.12.2014	NR	WBF	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20145642
Ip	14.4138	Beschaffungspraxis bei kritischen IKT-Infrastrukturen der Bundesverwaltung	Noser Ruedi	10.12.2014	NR	EFD	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144138
Ip	14.4123	Ausbau der ICT-Infrastruktur. Rahmenbedingungen für Investitionen verbessern	Guhl Bernhard	10.12.2014	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144123
Ip	14.4194	Big Data. Potenzial und Entwicklungsperspektiven der Datenwirtschaft in der Schweiz	Graf-Litscher Edith	11.12.2014	NR	EDI	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144194
Po	14.4294	Web-Index für ein freies und offenes Internet. Die Schweiz ist nur an 18. Stelle	Glättli Balthasar	12.12.2014	NR	UVEK	http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20144294

6 Glossar

0-day Exploits	Exploit, der am selben Tag erscheint, an dem die Sicherheitslücke öffentlich bekannt wird.
Active Directory	Active Directory (AD) heißt der Verzeichnisdienst von Microsoft Windows Server.
Advanced Persistent Threat	Diese Bedrohung führt zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder auf ein Land wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen.
Anonymisierungsdienst Tor	Tor ist ein Netzwerk zur Anonymisierung von Verbindungsdaten. Tor schützt seine Nutzer vor der Analyse des Datenverkehrs.
Backdoor	Backdoor (deutsch: Hintertür) bezeichnet einen Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
Backup	Backup (deutsch Datensicherung) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.
Black Hat Search Engine Optimization (BHSEO	Suchmaschinenoptimierung oder Englisch „Search Engine Optimization“ bezeichnet Massnahmen, die dazu dienen, dass Webseiten im Suchmaschinenranking auf höheren Plätzen erscheinen. Unerwünschter Methoden seitens der Suchmaschinen werden „Black Hat“ genannt.
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.
Botnetzwerk	Ursprung im slawischen Wort für Arbeit (Robota). Bezeichnet ein Programm, das bestimmte Aktionen nach dem Empfang eines Befehls selbstständig ausführt. So genannte Malicious Bots können

	kompromittierte Systeme fernsteuern und zur Durchführung beliebiger Aktionen veranlassen.
Bruteforce	Die Bruteforce-Methode ist eine Lösungsmethode für Probleme, die auf dem Ausprobieren allermöglichen Fälle beruht.
Byte	Das Byte ist eine Maßeinheit der Digitaltechnik und der Informatik, das meist für eine Folge von 8 Bit steht.
Cloud	Unter Cloud Computing versteht man das Speichern von Daten in einem entfernten Rechenzentrum, aber auch die Ausführung von Programmen, die nicht auf dem lokalen Rechner installiert sind.
Command and Control	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 Systeme (CMS)	Ein Content-Management-System (kurz: CMS, übersetzt: Inhaltsverwaltungssystem) ist ein System, das die gemeinschaftliche Erstellung und Bearbeitung von Inhalt, bestehend aus Text- und Multimedia-Dokumenten, ermöglicht und organisiert, meist für das World Wide Web. Ein Autor kann ein solches System auch ohne Programmier- oder HTML-Kenntnisse bedienen. Der darzustellende Informationsgehalt wird in diesem Zusammenhang als Content (Inhalt) bezeichnet.
Cookie	Kleine Textdateien, die beim Besuch einer Webseite auf dem Rechner des Benutzers abgelegt werden. Mit Hilfe von Cookies lassen sich beispielsweise persönliche Einstellungen einer Internet-Seite speichern. Allerdings können sie auch dazu missbraucht werden, die Surfgewohnheiten des Benutzers zu erfassen und damit ein Nutzerprofil zu erstellen.
DDoS	Distributed-Denial-of-Service Attacke Eine DoS Attacke, bei der das Opfer von vielen verscheiden Systemen aus gleichzeitig angegriffen wird.
Ethernet	Ethernet ist eine Technologie, die Software und Hardware für kabelgebundene Datennetze spezifiziert.

Exploit-Kits	Baukasten mit denen Kriminelle Programme, Scripts oder Codezeilen generieren können, mit denen sich Schwachstellen in Computersystemen ausnutzen lassen.
Firewall	Eine Firewall (engl. für Brandmauer) schützt Computersysteme, indem sie ein- und ausgehende Verbindungen überwacht und gegebenenfalls zurückweist. Im Gegensatz dazu ist eine Personal Firewall (auch Desktop-Firewall) für den Schutz eines einzelnen Rechners ausgelegt und wird direkt auf dem zu schützenden System – das heisst auf ihrem Rechner – installiert.
Firmware	Befehlsdaten zur Steuerung eines Gerätes (z. B. Scanner, Grafikkarten, usw.), die in einem Chip gespeichert sind. Diese Daten können in der Regel über Upgrades geändert werden.
Global Positioning System (GPS)	Global Positioning System (GPS), offiziell NAVSTAR GPS, ist ein globales Navigationssatellitensystem zur Positionsbestimmung und Zeitmessung.
Global System for Mobile Communications (GSM) Netzwerke	Das Global System for Mobile Communications (früher Groupe Spécial Mobile, GSM) ist ein Standard für voll-digitale Mobilfunknetze, der hauptsächlich für Telefonie, aber auch für leitungsvermittelte und paketvermittelte Datenübertragung sowie Kurzmitteilungen (Short Mes-sages) genutzt wird.
GPS-Jammer	Gerät zur Störung von GPS-Daten.
International Mobile Subscriber Identity	Die International Mobile Subscriber Identity dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern.
Jailbreak	Mit Jailbreaking (englisch: Gefängnisausbruch) wird das Überwinden der Nutzungseinschränkungen auf Apple Produkten mittels geeigneter Software bezeichnet.
Keylogger	Geräte oder Programme, die zwischen den Rechner und die Tastatur geschaltet werden, um Tastatureingaben aufzuzeichnen.
Man in the Middle	Man-in-the-Middle Attacke. Attacke, bei der sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner hängt

	und dadurch deren Datenaustausch mitlesen oder verändern kann.
Message Authentication Code (MAC)	Ein Message Authentication Code dient dazu, die Integrität von Daten oder Nachrichten zu überprüfen.
Near Field Communication (NFC)	Die Near Field Communication ist ein Übertragungsstandard nach internationalem Standard zum kontaktlosen Austausch von Daten über kurze Strecken.
Network Attached Storage (NAS)	Network Attached Storage oder zu Deutsch netzgebundener Speicher bezeichnet einfach zu verwaltende Datei-Server.
Netzwerkprotokoll	Ein Netzwerkprotokoll ist ein Kommunikationsprotokoll für den Austausch von Daten zwischen Computern in einem Rechnernetz .
Patch	Eine Software, die den fehlerhaften Teil eines Programms durch einen fehlerfreien ersetzt und dadurch z. B. eine Sicherheitslücke behebt.
Phishing	Mittels Phishing versuchen Betrüger, an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen. Dabei kann es sich beispielsweise um Kontoinformationen von Online-Auktionsanbietern (z. B. eBay) oder Zugangsdaten für das Internet-Banking handeln. Die Betrüger nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.
Plug-in	Eine Zusatzsoftware, welche die Grundfunktionen einer Anwendung erweitert. Beispiel: Acrobat Plug-Ins für Internet Browser erlauben die direkte Anzeige von PDF-Dateien.
Point of Sales	Ein POS-Terminal (in der Schweiz EFT/POS-Terminal) ist ein Online-Terminal zum bargeldlosen Bezahlen an einem Verkaufsort (Point of Sale).
Proof of concept (POC)	Proof of Concept Ein kurzer, nicht zwangsläufig kompletter Beweis, dass eine Idee oder Methode funktioniert. Beispielsweise werden häufig Exploit-Codes als PoC veröffentlicht, um die Auswirkungen einer Schwachstelle zu unterstreichen.

Pufferüberlauf	Pufferüberläufe (englisch buffer overflow) gehören zu den häufigsten Sicherheitslücken in aktueller Software, die sich u. a. über das Internet ausnutzen lassen können.
Quellcode	Der Begriff Quelltext, auch Quellcode (engl. source code) genannt, bezeichnet in der Informatik der für Menschen lesbare, in einer Programmiersprache geschriebene Text eines Computerprogrammes.
Ram Scraper	Diese Malware liest die Daten auf dem Magnetband der Karte direkt nach der Verwendung im Zahlungsterminal, während sie in dessen RAM enthalten sind
Ransomware	Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Typischerweise werden Daten verschlüsselt oder gelöscht und erst nach Lösegeldzahlungen der zur Rettung nötige Schlüssel vom Angreifer zur Verfügung gestellt.
Request	Die Anfrage eines Clients an einen Server im Client-Server-Modell.
Rich Text Format	Das Rich Text Format (RTF) ist ein Dateiformat für Texte.
Roaming	GSM-Roaming ist die Fähigkeit eines Mobilfunknetz-Teilnehmers in einem fremden Netzwerk Zugriff auf Mobilfunknetzdienste zu haben.
Router	Geräte aus dem Bereich Computernetzwerke, Telekommunikation oder auch Internet, die mehrere Rechnernetze koppeln oder trennen. Router werden beispielsweise in Heimnetzwerken eingesetzt und machen die Verbindung zwischen internem Netz und dem Intranet.
SCADA-Systeme	Supervisory Control And Data Acquisition Systeme. Werden zur Überwachung und Steuerung von technischen Prozessen eingesetzt (z. B. Energie- und Wasserversorgung).
Schadsoftware	Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Siehe auch Malware.

Schwachstelle (Vulnerability)	Schwachstelle in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
Session	Eine Session oder zu Deutsch Sitzung bezeichnet eine stehende Verbindung eines Clients mit einem Server.
Session Hijacking	Session Hijacking bezeichnet die Übernahme einer stehende Verbindung eines Clients mit einem Server durch eine unbefugte Drittperson.
Short Message Service (SMS)	Short Message Service Dienst zum Versenden von Kurzmitteilungen (maximal 160 Zeichen) an Mobiltelefonbenutzer.
Sicherheitsgateways	Ein Sicherheitsgateway ist ein Oberbegriff der alle IKT-Systeme umfasst, welche für IKT-Sicherheit in einer Organisation Sorge tragen.
Signierung	Eine Signierung ermöglicht, mit Hilfe des öffentlichen Verifikationsschlüssels (dem Public Key) die Integrität der Nachricht zu prüfen
Smartphones	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.
Social Media	Webseiten auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen. Oft werden persönliche Daten wie Namen, Geburtstage, Bilder, Berufliche Interessen sowie Freizeitaktivitäten bekanntgegeben.
Spam	Unaufgefordert und automatisiert zugesandte Massenwerbung, worunter auch Spam-E-Mails fallen. Als Spammer bezeichnet man den Absender dieser Mitteilungen, während das Versenden selbst als Spamming bezeichnet wird.

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. Der Angreifer versucht dabei eigene Datenbankbefehle einzuschleusen, um Daten in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.
SSL	Secure Sockets Layer Ein Protokoll, um im Internet sicher zu kommunizieren. Der Einsatz von SSL liegt heute beispielsweise im Bereich von Online-Finanz-Transaktionen.
Suchmaschinen-Ranking	Reihenfolge mehrerer vergleichbarer Objekte nach einer Suchmaschinenanfrage, deren Sortierung eine Bewertung festlegt.
Universal Mobile Telecommunications System (UMTS)	Das Universal Mobile Telecommunications System (UMTS) ist ein Mobilfunkstandard der dritten Generation für den Datenaustausch.
Universal Serial Bus Serieller Bus (USB)	Universal Serial Bus Serieller Bus, welcher (mit entsprechender Schnittstelle) den Anschluss von Peripheriegeräten, wie Tastatur, Maus, externe Datenträger, Drucker, usw. erlaubt. Der Rechner muss beim Ein- beziehungsweise Ausstecken eines USB-Gerätes nicht heruntergefahren werden. Die neuen Geräte werden meist (allerdings abhängig vom Betriebssystem) automatisch erkannt und konfiguriert.
Upstream-Provider	Ein Upstream-Provider bietet Internet Service Providern (ISP) Verbindungen zum Internet an, welche der ISP selbst nicht besitzt.
Webseiteninfektionen	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.
Webseitenverunstaltung (Defacement)	Unberechtigtes Verändern einer Website.
Wechseldatenträger	Ein nicht fest eingebauter, austauschbarer, normalerweise tragbarer Datenträger für Computer.
WLAN	WLAN (oder Wireless Local Area Network) steht für drahtloses lokales Netzwerk.
Zwei-Faktor-Authentifizierung	Dafür sind mindestens zwei der drei Authentifikationsfaktoren notwendig: 1. Etwas, das man weiss (z.B. Passwort, PIN, usw.) 2. Etwas, das man besitzt (z.B. Zertifikat, Token, Streichliste, usw.) 3. Etwas, das man ist (z.B. Fingerabdruck, Retina-Scan, Stimmerkennung, usw.)